

THE CRIMINAL USE OF FALSE IDENTIFICATION



NOVEMBER 1976

40865

THE REPORT OF THE FEDERAL ADVISORY
COMMITTEE ON FALSE IDENTIFICATION

UNITED STATES DEPARTMENT OF JUSTICE

THE CRIMINAL USE OF FALSE IDENTIFICATION

**A Summary Report on the Nature, Scope, and
Impact of False ID Use in the United States
with Recommendations to Combat the Problem**

NOVEMBER 1976

**The Report of the Federal Advisory Committee
on False Identification**

**UNITED STATES DEPARTMENT
OF JUSTICE**

NCJRS

APR 27 1977

ACQUISITIONS

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price \$6.30
Stock Number 052-003-00226-4*

Department of Justice
Washington 20530

October 8, 1976

Honorable Edward H. Levi
Attorney General
Department of Justice
Washington, D. C.

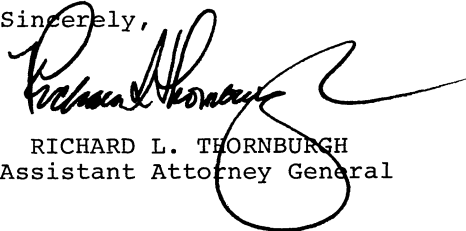
Dear General Levi:

It is a pleasure for me to transmit the Report of the Federal Advisory Committee on False Identification. This Report is the first comprehensive look at the criminal use of false identification: a multibillion dollar Federal, state and local problem.

The Committee recommends that a comprehensive program to combat false identification crimes be adopted at all levels of government, in the private sector, and by the public.

I hope that the Committee's recommendations will provide a starting point for the elimination of false identification as a major tool of crime.

Sincerely,

A handwritten signature in black ink, appearing to read "Richard L. Thornburgh", written over a large, stylized circular flourish.

RICHARD L. THORNBURGH
Assistant Attorney General

ABSTRACT

The criminal use of false identification is a national problem with a multi-billion dollar impact on government, business, and the general public. In November 1974 the U.S. Attorney General established the Federal Advisory Committee on False Identification (FACFI) to assess the problem and recommend solutions. With MITRE support, the FACFI conducted surveys and examined the extent of false ID use in six major problem areas: drug smuggling, illegal immigration, fugitives from justice, fraud against business, fraud against government, and other criminal activity. The Committee ranked potential solutions in these areas by criteria that included not only an assessment of effectiveness but also an evaluation of possible impact on public convenience and privacy. This report contains the findings, background material, recommendations, and plans for implementation of the proposed solutions of the FACFI, and the appendices offer a comprehensive archive of current information available on the problem.

ACKNOWLEDGEMENTS

The Committee Chairman gratefully acknowledges all those who have contributed to this Report, particularly Deputy Attorney General Harold R. Tyler, Jr., Assistant Attorney General Richard L. Thornburgh, Deputy Assistant Attorney General John C. Keeney, General Crimes Section Chief Alfred L. Hantman, Former Section Chief Carl W. Belcher; Douglas H. Westbrook of the Criminal Division, Emil Schroeder, FBI who originally presented the false identification problem to the Criminal Division; Deputy Director William F. Duggan of the Passport Office who spent hundreds of hours working on this project; Staff Director Dr. Thomas P. Kabaservice of the MITRE Corporation whose professionalism produced the final work product; Joseph Kochanski of the Law Enforcement Assistance Administration who coordinated LEAA's contribution to the Committee; and the Committee's 80 members and friends who contributed 18 months of their time and effort as volunteers.

CONTENTS

	Page
EXECUTIVE SUMMARY	ix
BACKGROUND AND MEMBERSHIP OF THE FACFI	xxv
PART I—A LOOK AT THE PROBLEM	
SECTION 1 AN INTRODUCTION	1
SECTION 2 THE SCOPE OF THE PROBLEM	7
Effect on Society	8
Methods of Investigation	11
Definitions	12
A Comment on Collected Data	14
SECTION 3 COMMON IDENTIFICATION DOCUMENTS	17
Birth Certificate	17
Driver's License	20
U.S. Passport	21
U.S. Visa and Alien ID Card	22
Social Security Card	24
Selective Service Draft Card	25
Voter Registration Card	25
Credit Cards	26
Non-Government ID	27
SECTION 4 FRAUDULENT ID USE	29
Drug Smuggling	32
Illegal Immigration	33
Fugitives From Justice	35
Fraud Against Business	36
Fraud Against Government	46
Other Criminal Activity	52

	Page
SECTION 5	FALSE IDENTIFICATION AND THE LAW 55
	Federal Legislation 57
	State Legislation 60
	Legal Change of Identity 65
 PART II—A VIEW TOWARD SOLUTION	
SECTION 6	APPROACH TO FINDING SOLUTIONS 67
SECTION 7	RECOMMENDATIONS APPLIED TO MAJOR PROBLEM AREAS 73
	Rejection of a National Identification Document 73
	Right to Privacy 76
	Federal Legislation 77
	State Legislation 78
	Birth Certificate 79
	Driver's License 82
	Drug Smuggling 83
	Illegal Immigration 84
	Fugitives From Justice 85
	Fraud Against Business 86
	Fraud Against Government 87
	Other Recommendations 88
SECTION 8	DISCUSSION OF THE RECOMMENDATIONS 91
 PART III—A PLAN FOR IMPLEMENTATION	
SECTION 9	GUIDELINES FOR STATE ACTION 95
	State Legislation Against False Identification 96
	Control of Access to Vital Statistics Records 99
	Control of Issuance of Birth Certificates 101
	Standardized Forms for Birth Certificates 103
	Matching of Birth and Death Certificates 106
	Improvements to State Driver Licensing Systems 108

		Page
SECTION 10	GUIDELINES FOR FEDERAL ACTION	113
	Legislation Against False Identification	113
	Action to Combat Fraud Against Government	121
	Cooperation With The States	126
SECTION 11	ACTION BY THE PRIVATE SECTOR	131
	Action By The Business Community	131
	Action By The General Public	134

REFERENCES 137

PART IV—APPENDICES

APPENDIX A	TASK FORCE REPORTS	A-1
	A1 Government Payments	A-3
	A2 Commercial Transactions	A-35
	A3 Fugitives	A-75
	A4 Federal Identification Documents	A-107
	A5 State and Local Identification Documents	A-161
APPENDIX B	PRELIMINARY PROPOSALS FOR SOLUTION	B-1
APPENDIX C	BACKGROUND PAPERS	C-1
	C1 Electronic Funds Transfer Systems (EFTS): An Overview	C-3
	C2 Automated Identification Technology	C-51
	C3 Some Commercially Available Identification Products	C-87
	C4 A Survey of Foreign National Systems for Personal Identification	C-131
APPENDIX D	SPECIAL STUDIES	D-1
	D1 A Plan for Reducing the Abuse of Birth Certification	D-3
	D2 Matching of Birth and Death Records	D-65

	Page
D3 Recommended Federal Guidelines for Improved Driver's License Security	D-105
D4 A Proposal to Upgrade the Security of the State-Issued Driver's License	D-163
APPENDIX E OTHER PERTINENT MATERIAL	E-1
E1 The Paper Trip (Excerpts)	E-3
E2 Letter from Western States Bankcard Association	E-13
E3 Federal Statutes Relating to the Use of False Identification	E-19
APPENDIX F ALTERNATE VIEWS	F-1
F1 Statement to the FACFI in the Matter of a Minority Recommendation	F-3
F2 Letter from the Chairman of The American Committee for Protection of Foreign Born	F-7
F3 Letter from the President of The Association of Immigration and Nationality Lawyers	F-11
F4 Anonymous letter from an employee of a State Drivers License Agency	

LIST OF ILLUSTRATIONS

Figure		Page
1	Cover of Underground Publication The Paper Trip	3
2	Advertisement on Securing a New Identity	4
3	The IDI Method	19
4	Dangerous Fugitives: Customers for False IDs	35
5	A Common Check Cashing Scene	38
6	Example of a Preliminary Proposal	69
7	Format For Evaluation of Preliminary Proposal	70
8	A Model Application Form For Birth Certification	102
9	Sample Form and Format For Certified Copy of Birth Certificate	105

LIST OF TABLES

Table		Page
1	Summary of Responses to Food Stamp Questionnaire	15
2	Summary of Scope and Impact of National False Identification Problem	31
Exhibit		
I	Model State Legislation—The Identity Protection Act	97
II	S.2131, 94th Cong. 2d Sess.—Federal False Identification Crimes	114

EXECUTIVE SUMMARY

The criminal use of false identification is a multibillion dollar national problem. A growing army of criminals and fugitives is using a screen of false credentials in welfare fraud, illegal immigration, drug trafficking, passing bad checks and phony credit cards, and in hundreds of other crimes. These crimes have one thing in common: the taxpayer picks up the tab. Every American man, woman and child pays the price in taxes, the cost of goods, and in the human suffering and tragedy caused by the success of false identification crimes.

False identification is a criminal's best friend. With it, criminals can appear and disappear at will by creating fictitious "paper people." Often victims are not even aware they have been victimized. The exploding use of false identification must be stopped.

The purpose of this report is to unmask false identification crimes and to provide a comprehensive, commonsense plan which Federal, state and local agencies, the commercial sector and the public can use to prevent such crimes. This plan is designed to increase personal privacy while giving law enforcement agencies the necessary tools to fight false ID use. But action must begin now.

I. THE FEDERAL ADVISORY COMMITTEE ON FALSE IDENTIFICATION

The Federal Advisory Committee on False Identification (FACFI) was established by the Attorney General in November, 1974 to: (1) study the nature and scope of the criminal use of false identification; and (2) recommend steps to combat it consistent with every citizen's right to privacy. The Committee consists of some 75 volunteers representing 50 Federal, state and local agencies, the commercial sector and the public. The Committee's 18-month

effort was supported by a \$200,000 grant from the Department of Justice to the MITRE Corporation for staff support to the Committee.

II. HOW FALSE IDs ARE OBTAINED

False identification documents can be obtained readily and inexpensively anywhere in the United States or neighboring countries from a variety of commercial sources or by “do-it-yourself” techniques. In any large city one can find photo studios that provide customers with photo ID cards replete with official-looking signatures and seals in any name, address or birthdate of the customer’s choice—no questions asked. Thriving mail-order businesses, which advertise their services nationally through “underground” newspapers and magazines, supply blank birth certificates and baptismal certificate forms and mount customer-supplied photographs on counterfeit “state ID” cards. Dozens of document vendors south of the U.S. border sell counterfeit U.S. immigration documents and border crossing cards for whatever the traffic will bear. Most of these activities are beyond the reach of current Federal or state laws.

But the enterprising imposter need not risk counterfeit or stolen documents; he can obtain genuine IDs of living or dead persons from the legal issuing offices themselves. This process begins when a criminal obtains a certified copy of another person’s birth certificate by filing a false application at one of 7,000 vital records offices. In the “Infant Death Identity,” or IDI process, the names of deceased infants gleaned from obituary columns or tombstones are frequently used. This “breeder document,” the certified copy, is then used to obtain a driver’s license, Social Security card and other documents until one or more identities are created. With them the criminal can destroy the personal privacy of those living persons whose names he uses and commit virtually any type of crime.

III. THE SCOPE OF THE FALSE ID PROBLEM

Because false identification is a *modus operandi* and not a separate category of crime, firm statistics on it are virtually impossible to obtain. This report reveals only the tip of a vast criminal iceberg of unknown dimensions. False identification impacts nationally in the six major problem areas summarized below.

Problem Area	Scope of Problem	Extent of False ID Use	Sources of Data
Drug Smuggling	> \$1 billion/yr.	80% of hard drugs smuggled	Customs Service, Drug Enforcement Administration, Passport Office
Illegal Immigration	> \$12 billion/yr. *	Unknown; used in entry, employment, welfare application	Immigration & Naturalization Service, independent studies
Fugitives From Justice	> 300,000 fugitives/yr.	~ 100% of Federal cases	FBI, sheriffs and police survey
Fraud Against Business	> \$3 billion/yr. †	> \$1 billion/yr.	American Bankers Assoc., independent studies
Fraud Against Government	Unknown	Unknown	Surveys of Welfare officials, published studies
Other Criminal Activity	Unknown	Very common	FBI, sheriffs and police survey

> More than

* Estimated U.S. tax burden

† Includes out-of-pocket losses and cost of collection attempts

~ Approximately

1. *Drug Smuggling*—Approximately 80% of the hard drugs entering the United States, with an estimated street value of \$1 billion, is smuggled by organized rings that make extensive use of false identification. Passports obtained through false IDs facilitate the flow of drugs and illegal aliens across U.S. borders.

2. *Illegal Immigration*—The tax burden caused by illegal aliens has been estimated by the Immigration and Naturalization Service to be in excess of \$12 billion per year. Many illegal aliens use false identification and obtain welfare and other benefits at taxpayer's expense. Some alien smugglers are so confident of their false IDs that they offer a money back guarantee: if you get caught within five days of entry, you get your money back.

3. *Fugitives From Justice*—Escaped prisoners and other dangerous fugitives almost always obtain false IDs to avoid detection and capture. In a recent FBI survey of 500 names of wanted persons chosen at random, all had active aliases and some had more than 30 identities. James Earl Ray, Patty Hearst and countless other fugitives used false identification.

4. *Fraud Against Business*—The use of false IDs is costing American businesses well over \$1 billion each year through check and credit card fraud, securities fraud, and embezzlement. The average food store is estimated to suffer losses of over \$7,000 per year through false ID fraud. One New Jersey engineer got 1,000 credit cards and \$660,000 in loans by creating 300 phony IDs.

Banks suffer losses primarily through forgery of stolen checks—

estimated by the American Bankers Association at \$50 million for 1974. False IDs play a substantial role in losses on bank credit cards that total approximately \$500 million each year.

5. *Fraud Against Government*—Surveys conducted among state and Federal welfare officials by the FACFI revealed that there are no uniform standards for the identification of welfare recipients. Thus, we have no way to estimate the scope of multiple collection of benefits by individuals using several identities. Losses from false identification are uncontrolled and could well number in the billions of dollars. A New York District Attorney who found several cases of such fraud in a single welfare center concluded that illegal multiple entitlement is “the most serious problem faced in the administration of Public Assistance and one for which there are no present adequate safeguards.”* Significant evidence of the use of false IDs in obtaining illegal benefits was also uncovered in an investigation of the food stamp program in Arkansas. In Chicago, authorities nabbed a “welfare queen” who used 250 aliases in 16 stores to steal more than \$150,000 from social welfare programs. She used 31 different addresses, three Social Security numbers, and records of eight “deceased husbands;” at a preliminary hearing her true name remained a mystery. Further investigation of false identification welfare fraud in many more locations is necessary, however, before the national impact of this problem can be accurately estimated.

In Philadelphia, before a serious effort was made in 1974 to reduce the mailing of welfare checks, an average of 10,000 replacements for checks reported “lost or stolen” were issued each month. About 41% of the lost or stolen checks were subsequently forged, resulting in an annual loss of \$4.8 million. A similar audit of lost or stolen checks conducted in New York City found forgery losses to be in excess of \$8 million during the year ending October 1973. In Federal Social Security programs forgery of stolen benefit checks—amounting to approximately \$10 million during 1975—also appears to be a major source of loss.

6. *Other Criminal Activity*—The usefulness of false IDs has not been lost on the common criminal engaging in crimes from con-

*N. Ferraro, “Report on Investigation of Welfare Fraud for 1974,” Queens County, N.Y., 1975.

fidence games to burglary. In his response to the FACFI survey a Dayton, Ohio sheriff sums it up:

The growing and thriving business in underworld sale of false identification and related items has become so standard that not only does the common thief have ready access to any type of false ID he wishes, but also he finds the going street price within easy reach of his budget.*

IV. RESPONSE TO THE PROBLEM

The FACFI has been charged not only with documenting the problem of criminal use of false identification, but also with developing written proposals for dealing with it at all levels of government as well as informing the public of ways to reduce such crimes. To accomplish these goals, the FACFI has been holding regular sessions in Washington, D.C. since November 1974. All meetings have been announced in advance in the Federal Register and have been open to the public. The FACFI and its staff have examined a large number of potential solutions to false ID problems received from FACFI members, survey respondents, and members of the general public. Other ideas for solutions were gleaned from newspaper and magazine articles, testimony before Congress, and the experience of other democratic societies in dealing with problems of identification. Information was also requested from vendors of fraud-resistant identity verification devices and techniques through a solicitation published in the *Commerce Business Daily*.

Members of the FACFI evaluated potential solutions through a formal procedure and then ranked them with respect to criteria that included an assessment of effectiveness and potential impact on public convenience and privacy. We recognize the legal and implied rights to privacy and the threat to those rights by excessive government interference. Thus, FACFI has attempted to maintain a careful balance in formulating recommendations for dealing with the national false identification problem; we have considered both *protection against crime* and *protection of privacy* to be guarantees provided to all in a free society.

*"Survey of Police Departments and Sheriff's Offices," *Report to Fugitives Task Force of the FACFI*, May 1975.

V. PROPOSED FINDINGS AND RECOMMENDATIONS

1. REJECTION OF A NATIONAL IDENTIFICATION DOCUMENT

The concept of a uniform personal identification document, to be issued and secured by Federal or state government, has occasionally been proposed as a sweeping solution to the problems of false identification. National IDs are in fact used by a number of nations with democratic traditions as well as those under other forms of government. The FACFI considered it necessary and advisable to study the national ID concept as carefully and rationally as possible in order to illuminate the advantages and problems inherent in such an approach.

Three different approaches to a system of uniform personal identification were evaluated by FACFI members. One approach proposed a federally-issued document designed specifically for personal identification within the U.S. This document would be available to citizens on a voluntary basis and would incorporate application procedures and security features similar to those used in the U.S. passport. The second suggestion envisioned a complete national identification system in which citizens would be registered at birth. This proposal included an automated verification system—a data base containing only identity information—that could be accessed only by the registered individual to verify his identity to government agencies. The third proposal suggested the use of present state driver's licenses (and non-driver state IDs) as recognized and required personal identification. Application for such a document would be required of all citizens at age 16. Safeguards against counterfeiting, alteration, and use by imposters would have to be included in all such state documents.

Similar arguments can be brought to bear in favor of and against all these proposals. Arguments in favor of a single standardized ID include the beliefs that:

- a. Such a document could be more easily recognized, controlled and protected against abuse.
- b. Document systems that include everybody would thereby be “foolproof.”
- c. Government has an obligation to provide a reliable means of personal identification for public and private transactions among its citizens.

Arguments against a standardized national ID include the beliefs that such documentation is in opposition to American tradition and would represent an invasion of personal privacy, and that data required for citizen identification could be abused by government or private interests.

It is certain that any new system designed to verify and store identity information on over 200 million people would be extremely expensive and require a major national effort. It is highly probable that proposals for such a system would be opposed politically. If such a system were implemented despite these difficulties, it would be subject to defeat by imposters or counterfeiters taking advantage of careless inspection of documents or through corruption of officials. Occasional errors would also occur in such a system that could adversely affect innocent people. Organized crime would take advantage of any national ID system because of the presumption of validity surrounding such a large system. Criminals could reap benefits far greater than they obtain under the current multifaceted system of identification.

The FACFI therefore strongly opposes any new type of state, or local government-issued ID intended to supersede existing documents. In short, FACFI opposes any so called "National ID card."

*The FACFI instead recommends that the security of existing state document systems be increased, particularly for breeder documents such as the birth certificate and the driver's license. Security must be increased both in the *application phase* (during which documents are issued) and in the *use phase* (when the documents are used).*

Thus, the goals of FACFI's recommended actions are to insure the increased security and privacy of existing state identification documents in state, interstate, and Federal transactions, and to insure swift prosecution of criminals who obtain and use false IDs. The following recommendations are designed to accomplish these goals. Specific steps to implement them are found in Sections 9-11 of this report.

2. RIGHT TO PRIVACY

The FACFI finds that the criminal use of false identification often invades personal privacy; that innocent citizens are victimized when their good names and credit are used in criminal transactions; and that the protection of personal privacy is an essential right, fully

consistent with sound law enforcement efforts to reduce false identification crimes.

The FACFI therefore recommends that individual privacy rights be given the fullest consideration in the formulation and implementation of the following legislative and administrative proposals to counter the criminal use of false identification.

3. BIRTH CERTIFICATES

The FACFI finds that certified copies of birth certificates have frequently been abused by imposters and counterfeiters because:

- a. Unsigned requests by mail for such documents are usually honored.
- b. The birth certificates of deceased persons are not usually so designated and there is almost no correlation of birth and death records.
- c. Records of deaths and births in many states are open for “browsing” by persons seeking false identification.
- d. Minimum standards are not available for issuance security and document security of birth certifications.
- e. Many of the 7,000 local vital records offices are autonomous, which results in a wide variety of formats, seals, and safeguards provided for certifications, making it difficult to confirm or control the validity of local certifications.
- f. Information on the abuse of birth certificates is often not given to the proper state authorities.
- g. Abuse of birth certificates is not sufficiently covered by legislation at either the state or Federal level.

The FACFI therefore recommends that:

- a. Fraudulent application be discouraged by use of state-issued standard application forms requiring the applicant’s signature, justification of request, and items of personal history not generally available to imposters that can be used to detect false applications.
- b. A system be implemented for intrastate and interstate matching of birth and death records to note the fact of death on the

birth certificates of all persons aged 55 years or less at the time of death.

- c. State laws to protect individual privacy by limiting public access to birth and death records be enacted in all states lacking such legislation.
- d. Minimum standards be established for security of certified copies against theft, alteration and counterfeiting for adoption by states. (See Appendix D1.)
- e. Federal agencies that require personal identification in application for privileges or benefits accept as primary evidence of age and place of birth only those U.S. birth certifications issued by a state or state-controlled records office.
- f. Formal notification of the abuse of a birth certification be given by state and Federal law enforcement agencies to the appropriate state registry officials. The information exchange might be facilitated through the establishment of a clearinghouse for false ID information.
- g. Wherever practical, requests for birth certificates be retained by the issuing office to assist in the detection and tracing of fraudulent requests.
- h. Appropriate state and Federal legislation be enacted to prohibit the fraudulent application for, possession, sale, and transfer of birth certifications for the purpose of establishing a false identification.

4. DRIVER'S LICENSES

The FACFI finds that state driver's licenses (and nondriver state ID or age-of-majority cards) are frequently abused by counterfeiting, imposture, or fraudulent application because:

- a. They are used as personal ID for commercial transactions and dealings with government agencies although this use was not intended by issuing authorities.
- b. The security of issuance procedures and of the document itself varies widely among the states.
- c. Driver's licenses and other state identification documents are not sufficiently protected by Federal legislation against interstate abuse.

The FACFI therefore recommends that:

- a. The state-issued driver's license (or state-issued ID) be recognized as the primary form of personal ID for use in commerce and in general transactions between individuals and government.
- b. Guidelines be drafted by the Federal government providing minimum standards for the identification of applicants for original, replacement, or interstate exchange of driver's licenses and state IDs, and for security of those documents against counterfeiting, alteration, and use by imposters.
- c. Voluntary compliance by all states with these guidelines be encouraged by appropriate Federal funding or other incentives and/or sanctions.
- d. An analysis and implementation plan for improvement in the security of state ID systems be developed by the Law Enforcement Assistance Administration (LEAA) for consideration by the states.
- e. Federal legislation be enacted to prohibit counterfeiting in any state of personal IDs issued by any other state, and to prohibit use of the channels of interstate commerce to assist fraudulent application for state IDs.

5. DRUG SMUGGLING

The FACFI finds that smuggling of narcotics and other dangerous drugs by criminal organizations is aided materially by extensive use of false U.S. and foreign passports and other documents.

The FACFI therefore recommends that:

- a. Birth certificates and state-issued IDs, as the primary documents used in U.S. passport application procedures, be secured in accordance with FACFI recommendations.
- b. Federal agencies concerned with the activities of drug smuggling (including the Immigration and Naturalization Service, Drug Enforcement Administration, Customs Service, Passport Office, and Visa Office) provide coordinated training programs for the detection of false IDs used by smugglers and communicate frequently with each other and state and local authorities on the observed patterns of such false ID use.

- c. Interpol be encouraged to coordinate international law enforcement efforts in the detection of passport and other document fraud.

6. ILLEGAL IMMIGRATION

The FACFI finds that illegal aliens routinely use false IDs such as stolen or counterfeit immigration documents and border crossing cards, and U.S. birth certificates and voter registration cards obtained under false pretenses, to enter and remain in the United States. By obtaining Social Security accounts, they are able to secure employment to which they are not entitled, made easier because knowing employment of illegal aliens is not prohibited under Federal law.

The FACFI therefore recommends that:

- a. The Immigration and Naturalization Service (INS) be provided with sufficient funds to develop and implement an improved system for registration of legal aliens that will resist attempts at forgery, counterfeiting, and use of INS documents by imposters.
- b. Birth certificates and secondary evidence of U.S. citizenship be secured in accordance with FACFI recommendations.
- c. Identification and citizenship of applicants for new Social Security accounts be verified by stricter evidentiary requirements or other appropriate means.
- d. Federal legislation be enacted to counteract knowing employment of illegal aliens.

7. FUGITIVES FROM JUSTICE

The FACFI finds that dangerous fugitives are able to avoid apprehension through the use of false identification and that, when arrested, they may be released before their identity and criminal history are confirmed.

The FACFI therefore recommends that:

- a. State and Federal document systems be protected from abuse by fugitives through enactment of FACFI recommendations for birth certificates and driver's licenses.

- b. Laws be enacted requiring verification of the identity of all persons arrested, prior to their release on bond.
- c. To meet such identification requirements without endangering arrestees' rights, appropriate equipment be used for high-speed transmission of fingerprints and other identifying data between local or Federal law enforcement offices and identification bureaus.

8. FRAUD AGAINST BUSINESS

The FACFI finds that American business is subjected to billion-dollar losses each year from false identification fraud through forgery and counterfeiting of personal and corporate checks, impersonation based on stolen credit cards, negotiation of lost or stolen securities, and unauthorized intrusion into data banks and computer facilities.

The FACFI therefore recommends that:

- a. The business community incorporate into its operations measures to prevent false identification crimes; preserve evidence of such crimes; prosecute those who commit them; train employees in preventative measures; and assist the public in understanding the need for these measures.
- b. The business community make use of improved technological safeguards against false ID fraud.
- c. The business community participate in the increasing development and use of electronic funds transfer systems, which have the potential of reducing false ID fraud by reducing the amount of negotiable paper in circulation. The potential for privacy abuses and significant false ID fraud via electronic manipulation must be addressed in the design of such systems.
- d. The security of driver's licenses and other state IDs, which are widely used in commercial transactions, be improved through implementation of FACFI recommendations.
- e. The business community consider unauthorized intrusion into data banks as "white collar crime of the future," and take steps to analyze, detect, and prevent such intrusions.

9. FRAUD AGAINST GOVERNMENT

The FACFI finds that government public assistance programs such as food stamps and Social Security are subjected to outrageous annual losses through false identification fraud and that such fraud results principally from the use of false IDs in applying for welfare IDs, welfare benefits and in the cashing of stolen benefit and payroll checks.

The FACFI therefore recommends that:

- a. The Federal government upgrade existing standards for the identification of applicants for federally-supported or cost-shared public assistance programs.
- b. Mailing of welfare and payroll checks to individual addresses be superseded by mailing or direct deposit to banks and thrift institutions to the extent that such depositing is beneficial to recipients and is practical.
- c. The identity of applicants for new Social Security accounts be verified by stricter evidentiary requirements or other appropriate means and that the Social Security card be made resistant to alteration, counterfeiting and forgery.
- d. Cooperative programs be instituted for the training of welfare and Social Security employees in techniques for detection and reporting of the use of false identification.
- e. The security of birth certificates and driver's licenses, which are frequently used in application for government payments, be improved through implementation of FACFI recommendations.

10. FALSE IDENTIFICATION DATA

The FACFI finds:

- a. That many government agencies and companies who regularly are being defrauded by false identification schemes are not aware that they are being victimized because false identification crimes are often not detected until long after the crime has been committed.
- b. That there is an almost total lack of meaningful statistics concerning false identification crimes both in government agencies and the commercial sector; there is great reluctance by organizations to reveal these crimes even when they are dis-

covered because such losses are embarrassing to the organizations concerned; and that such failure to expose the criminal use of false identification has contributed to the proliferation and success of this criminal technique.

The FACFI therefore recommends that:

- a. Federal, state and local agencies and the commercial sector develop increased awareness of the nature of false identification crimes, compile statistics on those crimes that are committed within their organizations, and affirmatively seek methods of preventing the commission of such crimes both in the application stage and in the use stage.
- b. Federal, state and local law enforcement agencies and firms in the commercial sector establish a statistical base line by which to measure the increase or decrease in false identification crimes; and that other data on false identification be compiled including the type of crime, *modus operandi*, and a profile of the user and victim of false identification. Finally, FACFI recommends that the FBI gather statistics relating to false identification crimes to be published in Uniform Crime Reports. Such statistical base lines can then be used to measure the effectiveness of the countermeasures recommended by the FACFI as they are being implemented.

11. LEGISLATIVE LOOPHOLES

A. Federal Legislation

The FACFI finds that maintaining and upgrading the integrity of state identification documents, particularly the birth certificate and driver's license, is the key to reducing false identification crimes at both the Federal and state level.

There are approximately 350 Federal statutes relating to false identification, false applications and related subjects, but many Federal laws are ineffective in deterring false identification crimes because:

- a. Most identification documents are issued and regulated solely by the states. Federal statutes only come into play when the criminal applies for a federally-issued document such as a passport. By this time the criminal has built up such a variety of state-issued documents that false application is difficult to detect and likely to succeed. Indeed, a criminal's false identification may be more persuasive and complete than an honest person's valid identification.

- b. The Federal government does not collect and maintain information to verify a person's identity; only the states have that information. Therefore, the Federal government is totally dependent on state information and documents such as the birth certificate and driver's license, and those are often weak links in the identification chain.
- c. Federal statutes regulate only those documents issued by the Federal government and states regulate only documents which they issue; thus, there remains a substantial enforcement gap between these jurisdictions. This gap permits nationwide counterfeiting and selling of false identification documents.
- d. There are loopholes in some of the Federal statutes regulating specific documents such as the Social Security card and others.
- e. Even where Federal statutes are specific and well drafted, enforcement and prosecution is often given a low priority. The crime usually appears more innocuous than it actually is.
- f. In some cases, penalties for false statements on applications are sufficient. Other statutes require only revocation of licenses. Civil fines are imposed in other instances. There is little uniformity of treatment for false ID crimes.

The FACFI therefore recommends that:

- a. S.2131, legislation introduced in the 94th Congress, be enacted. S.2131 would close most existing loopholes in Federal legislation dealing with false identification. This bill:
 - 1. Prohibits false applications for Federal documents by prohibiting the knowing use or supplying of false information or falsified documentation when obtaining Federal identification documents;
 - 2. Prohibits the knowing use of the mails or other channels of interstate commerce for transporting any false information or documents for the purpose of obtaining state identification documents;
 - 3. Prohibits the unauthorized making or altering of any Federal identification documents;
 - 4. Prohibits the unauthorized making or altering of any state identification document when there is knowledge that such document will be used to obtain any document issued by the Federal government; and prohibits the sale or delivery of any such state identification document; and

5. Prohibits using the channels of interstate commerce or the mails to transmit any false Federal or state identification document or one intended to be used improperly.
- b. Federal false identification statutes be enforced with renewed vigor by prosecutors; and that judges be made aware of the importance of false identification crimes so that sentences may more accurately reflect the seriousness of these crimes.

B. State Legislation

The FACFI finds that the primary thrust of state statutes dealing with false identification is prohibitive not preventive. Criminal penalties are invoked upon fraudulent use of a false identity rather than the mere possession of fraudulent identification documents. Laws are totally inoperative until the criminal, in his new identity, commits a crime. By this time it is often too late. The criminal may have assumed another identity and disappeared.

In most states there is no comprehensive law against establishing a fraudulent identity. Statutes that purport to deal with the problem only deal with parts of it.

State laws governing the issuance of certified copies of birth and death certificates and access to such records do not adequately protect the public's right to privacy because certified copies of birth certificates are freely (though unknowingly) handed to criminals by all states. In some states it is not even illegal to lie on an application for a certified copy of a birth certificate.

The problem is national in scope, but states are powerless to protect any but their own identification documents. States cannot control the manufacture, counterfeiting and criminal use of their own IDs outside their borders.

The wide variety in document format and authenticating seals encourages the passing of counterfeit state documents.

Laws regulating specific documents, such as the birth certificate, are not comprehensive enough to allow effective enforcement. These laws never make reference to *all* of the following acts involving false identification:

- a. Illegal manufacture
- b. Sale
- c. Possession
- d. Alteration
- e. Transferring

- f. Transporting
- g. Advertising for sale
- h. Obtaining
- i. Receiving
- j. Use or display
- k. Use after expiration, suspension, or revocation
- l. False or misleading statements or use of false documents in an application for such documents.

Without this degree of comprehensiveness, criminals can use and supply others with false identification documents without fear of prosecution.

Many documents which can be used for identification purposes or to obtain other documents are not regulated at all. None of the states investigated by the Committee had laws regulating private ID cards and documents not issued by state agencies. These private ID cards can be used to purchase firearms or dangerous drugs that are not traceable to the real purchaser.

Prosecutors place low priorities on prosecution of false ID crimes because of a lack of awareness of the potential seriousness of the crime. Altering a document does not look nearly as serious as a murder or rape case until one realizes that the use of false IDs prevents many murder, rape and other cases from being solved.

In most states citizens have the common law right to change their name without any formal legal proceedings. In these states it is more difficult for prosecutors to prove fraudulent intent to violate false ID laws.

The FACFI therefore recommends that:

- a. States enact Model State Legislation proposed by the Committee entitled the "Identity Protection Act." This Act:
 - 1. Protects the public health and welfare and the right of privacy and security in one's own identity by penalizing the manufacture, alteration, transfer, sale, possession or use of any false identification document or any document obtained by use of false statements or false identification in the application process.
 - 2. Will specifically protect the integrity of the use and possession of birth certificates and driver's licenses.
 - 3. Establishes stricter criminal penalties for false identification crimes and requires them to be served consecutively with any other sentence arising out of the same crime.

4. Prevents fraud by private ID vendors and prohibits spurious documents issued by criminals in other states.
- b. States enact the most recent amendments to the Model State Vital Statistics Act prepared under the auspices of the National Center for Health Statistics of the Department of Health Education and Welfare (HEW). These are designed to protect the integrity of the birth certificate issuing system. These amendments also upgrade criminal penalties for false identification crimes.
- c. State educational programs be established to facilitate implementation of the Model Identity Protection Act and the Model State Vital Statistics Act and to assist officials in improved methods of document fraud detection.

12. USE OF IDENTIFICATION DOCUMENTS FOR UNDERCOVER PURPOSES

The FACFI finds that a study of the means by which Federal, state and local agencies obtain and use undercover documents for law enforcement and intelligence purposes is outside the charter of the Committee and thus has not been explored; the Committee notes, however, that some people have questioned the adequacy of controls on obtaining and using such documents.

The FACFI therefore recommends that:

- a. Government agencies not obtain or provide “alias identification” in violation of any local, state, or Federal laws.
- b. Agencies review their laws, regulations and procedures for obtaining such credentials to insure that they are lawfully obtained and that their use is adequately controlled.

13. PUBLIC SUPPORT

The FACFI finds it essential to obtain public recognition of the scope and impact of crimes committed with the aid of false IDs and to solicit informed support of measures designed to reduce the use of false IDs in the United States.

The FACFI therefore recommends that the Department of Justice and all other concerned organizations encourage public support for the measures recommended by the FACFI.

BACKGROUND AND MEMBERSHIP OF THE FACFI

The Federal Advisory Committee on False Identification (FACFI) was formed in 1974. Its creation was a product of several converging trends:

- Federal, state and local law enforcement agencies were being deluged with a host of new false identification techniques. Criminals and fugitives were using these techniques to perpetrate crimes and avoid arrest. Underground pamphlets such as the *Paper Trip* detailed steps for defrauding the public, while printing presses cranked out counterfeit “official” documents such as birth certificates and driver’s licenses and advertised them for sale in interstate commerce.
- There was a growing concern on the part of citizens and public interest groups that false identification could be used for unauthorized access to confidential information, and that privacy was being invaded when criminals used innocent persons’ names to commit crimes.
- The growing mobility of Americans required a more secure system of identifying strangers in commercial transactions such as cashing checks and using credit cards.
- The public was becoming more concerned over disclosures that millions of illegal aliens were entering the country, rampant fraud in government social welfare programs was coming to light, and innumerable other crimes involving false identification were increasing in number.

On September 15, 1973 and October 3, 1973, Miss Frances Knight, Director, and Mr. William Duggan, Deputy Director of the Passport Office, U.S. Department of State, testified on false identification before the Internal Security Subcommittee of the Senate Judiciary Committee.* Their testimony called attention to passport

*Hearing Before the Subcommittee to Investigate the Administration of the Internal Security Act of the Committee on the Judiciary, United States Senate, September 15, 1972, 92nd Congress 2d Session.

frauds and forgeries related to illegal narcotics trafficking and other crimes.

In the Fall of 1973, the Passport Office and the Federal Bureau of Investigation exchanged information concerning the increasing problem of false identification. These discussions led to an informal meeting among interested Federal agencies and others concerning the use of false identification. On May 10, 1974, a one-day conference of forty-four representatives from more than fifteen government agencies and other organizations was held at the FBI Academy, Quantico, Virginia. This meeting concluded with the unanimous recommendation that an interagency task force on false identification be formed to combat the problem.

In the Fall of 1974, the Criminal Division of the Department of Justice prepared the necessary charter documents to establish a Federal Advisory Committee on False Identification. On October 14, 1974, Attorney General William B. Saxbe officially announced its creation. In his address, the Attorney General made the following statement:

False identification is a common denominator in a wide range of serious crimes. Let me cite a few examples.

The Weatherman organization has taken credit for a number of terrorist bombings. False identification has been found on some of its members taken into custody. It appears that false identification may be a factor in the success of 23 others who have successfully eluded capture thus far.

But false credentials can touch virtually every aspect of crime. They are frequently used by narcotics peddlers and by persons passing counterfeit checks and securities, by those who take part in bank swindles, and in Social Security and welfare frauds. Car thieves often use false identification, not only to thwart police, but to rent or lease cars which are then driven off and sold.

The list of offenses could go on and on. They include widespread and costly frauds through the use of credit cards. And another growing problem is the use of false identification by illegal aliens who insulate themselves from authorities as they settle into new jobs and new lives . . .*

The announcement of the formation of the Federal Advisory Committee on False Identification and its charter were published in

*Address by William B. Saxbe, Columbus, Ohio, October 14, 1974.

the Federal Register of October 22, 1974.* The charter states the nature and purpose of this Committee are:

1. To identify, with the assistance of Federal, state, and local agencies, as well as representatives from the private sector and the public:
 - (a) the various criminal techniques used to obtain false identification;
 - (b) the types of persons committing such crimes; and
 - (c) the nature and extent of such crimes including their impact upon the criminal justice system and commercial transactions such as check passing, credit card fraud, and the obtaining of fraudulent loans, securities, and other commercial paper.
2. To develop a coordinated Federal plan for meeting the threat which Executive Branch Agencies face from false identification. Such plan will include a discussion of closing any loopholes in existing Federal laws, regulations or procedures, and strengthening the enforcement of such laws, regulations and procedures.
3. To assist state and local law enforcement agencies and bureaus of vital statistics in developing effective measures to prevent the obtaining of false identification and its criminal use.
4. To provide Federal, state and local agencies a forum and mechanism for the exchange of information on false identification.

In its deliberations, the Committee sought not only to aid law enforcement agencies but also to protect personal privacy. As Deputy Attorney General Harold R. Tyler, Jr. stated to the Committee:

. . . this is the very purpose of your Committee: to recommend law enforcement methods which are compatible with every citizen's vital right to reasonable privacy and fair treatment.**

The first meeting of the FACFI was held on November 14, 1974 in the Department of Justice, and monthly meetings were held thereafter. All of its meetings were open to the general public and all voting in the Committee was done by a consensus of those present, including members of the public.

*The Committee was chartered pursuant to the Federal Advisory Committee Act of 1972 (P.L. 92-463, Oct. 6, 1972).

**Address by Harold R. Tyler, Jr., to the Federal Advisory Committee on False Identification, May 8, 1975.

Because of the extensive scope of the problem, the FACFI was divided into five Task Forces, each dealing with a different phase of the false identification problem:

Task Force I—Government Payments

Task Force II—Commercial Transactions

Task Force III—Fugitives

Task Force IV—Federal Identification Documents

Task Force V—State and Local Identification Documents.

FACFI membership consisted of representatives of government agencies at Federal, state and local levels, law enforcement officials, business groups such as the American Bankers Association, and members of the general public. All were volunteers and received no travel funds or remuneration for their assistance. Many independent business firms provided voluntary support to the Committee by sending observers to meetings and by contributing valuable technical background information.

In October 1975, The MITRE Corporation was retained under contract with the Department of Justice to act as technical and editorial staff to the FACFI. MITRE support included: assisting us in gathering additional data covering gaps in the initial FACFI surveys to determine the nature and scope of the false identification problem; surveying the state of the art in technology areas that dealt with potential solutions to the false identification problem; compiling a set of potential solutions to be voted upon and revised by the FACFI; conducting other technical research; and drafting the FACFI final report.

MEMBERSHIP—FEDERAL ADVISORY COMMITTEE ON FALSE IDENTIFICATION

Chairman:	David J. Muchow Criminal Division Department of Justice
Co-Chairman:	Douglas H. Westbrook Criminal Division Department of Justice
Secretary:	Emil L. Schroeder Federal Bureau of Investigation

TASK FORCES

Task Force I—Government Payments

Chairman: Carl B. Williams
Robert B. Carleson & Associates,
Inc.

Co-Chairman: Laurence J. Love
Department of Health,
Education and Welfare

Task Force II—Commercial Transactions

Chairman: Nathaniel E. Kossack
National District Attorneys
Association

Co-Chairman Hollis Bowers
American Bankers Association

Task Force III—Fugitives

Chairman: Emil L. Schroeder
Federal Bureau of Investigation

Task Force IV—Federal Identification Documents

Chairman: William E. Duggan
Passport Office

Task Force V—State and Local Identification Documents

Chairman: Loren Chancellor
Department of Health,
Education and Welfare

Co-Chairmen: Irvin G. Franzen
Am. Assn. for Vital Records and
Public Health Statistics

George A. Gay
Department of Health,
Education and Welfare

STAFF

The MITRE Corporation
Bedford, Massachusetts 01730

Project Leader: Dr. Thomas P. Kabaservice
Group Leader: Special Studies
(617) 271-3179

Project Staff: Maya M. Devi
Technical Assistant
(currently on leave of absence)

Robert J. Ellis
Member of the Technical Staff
(617) 271-2329

Manuel Selvin
Member of the Technical Staff
(617) 271-3217

Writer/Editor: Marjorie A. Lynn
(617) 271-2250

Voting Individual or Organization	Member	Task Force Number
American Association for Vital Records and Public Health Statistics	Mr. Irvin G. Franzen President Forbes Air Force Base Building 740 Topeka, Kansas 66620 (913) 296-3523	5
American Association of Motor Vehicle Administrators	Mr. Arthur A. Tritsch Director Driver's Services Div. 1201 Connecticut Avenue, N.W. Washington, D.C. (202) 296-1955	5
American Bankers Association	Mr. Hollis Bowers Director Insurance and Protection Division 1120 Connecticut Avenue, N.W. Washington, D.C. 20036 (202) 467-4046	2

Voting Individual or Organization	Member	Task Force Number
American Express Company	Mr. Andrew F. Phelan Vice President Corporate Security Inspector's Office 67 Broad Street New York, New York 10004 (212) 797-5080	2
Mr. George Berlinger	(Former Welfare Inspector General, State of N.Y.) 595 Madison Avenue New York, New York 10022 (212) TE 8-1345	1
Bureau of Engraving and Printing	Mr. Charles R. Holmgren Assistant to Chief Office of Research & Technical Services 14th and C Street, S.W. Washington, D.C. 20228 (202) WO 4-7211	4
California Department of Health	Mr. Roger Smith Assistant Chief Vital Statistics Section 410 N Street Sacramento, California 95814 (916) 455-2684	5
Coast Guard	William J. Ward Chief, Technical Security Division (GOIS/74) U.S. Coast Guard Headquarters 400 7th Street, S.W. Washington, D.C. 20590 (202) 427-6361	4
	Lcdr. T. A. Welch Chief, Enlisted Recruiting Branch Washington, D.C. 20590 (202) 426-9542	4
Council of State Governments	Mr. Charles Whitemire Special Assistant 1150 17th Street, N.W. Washington, D.C. 20036 (202) 785-5610	5

Voting Individual or Organization	Member	Task Force Number
Customs Service	Mr. Edward H. Lisle Chief, Special Investigations Office of Investigations 2100 K Street, N.W. Washington, D.C. 20229 (202) 964-2623	4
	Mr. Albert Seeley Special Agent In Charge JFK International Airport 160-19 Rockaway Blvd. Jamaica, N.Y. 11430	4
Department of Agriculture	Mr. Paul D. Lamberth Supervisory Criminal Investigator Office of Investigations Room 27E, Administration Building 14th & Independence Ave., S.W. Washington, D.C. 20250 (202) 447-3923	1
	Mr. Robert E. Magee Assistant Director Performance & Controls Office of Investigations Room 24E, Administration Building 14th & Independence Ave., S.W. Washington, D.C. 20250 (202) 447-3923	1
	Ms. Rebecca Barillari Food Stamp Division 14th and Independence Ave., S.W. Washington, D.C. 20250	1
Department of Commerce	Mr. Norris A. Lynch Director Consumer Goods & Services Division Washington, D.C. (202) 967-4697	2
	Mr. James C. Kingsbury Trade Specialist Bureau of Domestic Commerce Washington, D.C. 20230 (202) 967-3818	2

Voting Individual or Organization	Member	Task Force Number
Department of Defense	Mr. Edgar J. Bethart Defense Investigation Program Office Office of Secretary of Defense Room 5/a/ 670, Pentagon Washington, D.C. 20301 (202) OX 7-9586	4
Department of Justice Criminal Division	Mr. David J. Muchow (Non Voting) Staff Assistant Criminal Division 2112 Main Justice Washington, D.C. (202) 739-5328	
	Mr. Roy Tesler Government Integrity Unit General Crimes Section Criminal Division, Room 507 315 9th Street, N.W. Washington, D.C. 20535 (202) 739-2346	4
	Mr. Stephen M. Weglian Trial Attorney Securities Unit General Crimes Section Criminal Division Washington, D.C. 20530 (202) 739-2670	2
	Mr. Douglas H. Westbrook (Non Voting) Trial Attorney General Crimes Section Washington, D.C. (202) 739-2745	
Department of State Office of Security	Mr. James Dandridge SY/I/PVB — Room 2418 Dept. of State Washington, D.C. 20520 (202) 632-3184	4
	Mr. James K. Moore SY/I/PVB — Room 2418 Dept. of State Washington, D.C. 20520 (202) 632-3184	4

Voting Individual or Organization	Member	Task Force Number
Department of State Passport Office	Mr. William E. Duggan Deputy Director for Legal and Security Affairs Room 600 1425 K Street, N.W. Washington, D.C. 20524 (202) 382-8174	4
	Mr. John O'Dowd U.S. Passport Office 1425 K Street, N.W. Washington, D.C. 20524 (202) 382-1814	5
	Mr. William B. Wharton Chief, Legal Division Passport Office, Room 320 1425 K Street, N.W. Washington, D.C. 20524 (202) 382-1761	4
Department of State Visa Office	Mrs. Dena Cunningham Management Analyst Officer Visa Office, Room 800 515 22nd Street, N.W. Washington, D.C. 20520 (202) 632-2940	4
	Mr. Ernest B. Dane Management Analyst Officer Visa Office, Room 800 515 22nd Street, N.W. Washington, D.C. 20520 (202) 632-1991	4
	Ms. Murrow B. Morris Consular Officer Visa Office, Room 815 515 22nd Street, N.W. Washington, D.C. 20520 (202) 632-1939	4
Department of Transportation	Mr. Frank Altobelli, Chief Licensing & Adjudication Division National Highway Traffic Safety Administration 400 7th St., S.W. Washington, D.C. 20590	5

Voting Individual or Organization	Member	Task Force Number
	Mr. Thomas Campbell U.S. Coast Guard Chief, Security Branch 400 7th St., S.W. Washington, D.C. 20590	4
	Mr. William T. Deeter, Jr. Deputy Director of Investigations and Security Office of the Secretary 400 7th St., S.W. Washington, D.C. 20590	4
	Mr. A. James Latchaw Licensing & Adjudication Division National Highway Traffic Safety Administration 400 7th St., S.W. Washington, D.C. 20590 (202) 426-9692 Ext. 4800	5
	Mr. Wayne J. Tannahill Highway Safety Management Specialist National Highway Traffic Safety Administration 400 7th St., S.W. Washington, D.C. 20590	
	Mr. Donald Wiseman Special Agent Federal Aviation Administration Office of Investigation and Security 800 Independence Ave., S.W. Washington, D.C. 20590	4
Department of Treasury	Mr. James B. Clawson Deputy Assistant Secretary Operations Room 3448 Washington, D.C. 20220 (202) 964-5115	4
	Mr. James J. Featherstone Deputy Assistant Secretary Enforcement Washington, D.C. 20220	4

Voting Individual or Organization	Member	Task Force Number
District of Columbia, Department of Human Resources	Mr. Charles A. Guerin Assistant Chief Counsel Fiscal Service Bureau of the Public Debt Washington, D.C. 20226	4
Drug Enforcement Administration	Mr. John H. Crandall Chief D.C. Dept. of Human Resources 300 Indiana Avenue, N.W. Room 1025 Washington, D.C. 20001 (202) 629-4376	5
Federal Bureau of Investigation	Mr. John W. Starke Special Agent Domestic Investigations Division DEA Headquarters Drug Enforcement Administration 1405 "I" Street, N.W. Washington, D.C. (202) 382-2101	4
Florida Highway Patrol	Mr. Emil L. Schroeder Federal Bureau of Investigation Room 4440, J. Edgar Hoover Building Washington, D.C. 20535 (202) 324-4575	3
Gartlan, Joseph V.	Lt. J. S. McKinnon Assistant Supervisor Investigations Neil Kirkland Bldg. Appalachee Parkway Tallahassee, Florida 32301 (904) 488-6583	5
Giant Food, Inc.	Attorney At Law 1801 K Street, N.W. Washington, D.C. 20006	2
	Mr. Thomas Knighten General Credit Manager P.O. Box 1804 Washington, D.C. 20013 (301) 341-4143	2

Voting Individual or Organization	Member	Task Force Number
Health Education and Welfare Division of Vital Statistics	Mr. Loren Chancellor Registration Methods Branch Chief Room 9A-45 Parklawn Building 5600 Fisher Lane Rockville, Maryland 20852 (301) 443-1820	5
	Mr. George Gay Room 9A-45 Parklawn Building 5600 Fisher Lane Rockville, Maryland 20852 (301) 443-1820	5
Health Education and Welfare Office of Policy Control Social & Rehabilitation Service	Mr. Laurence J. Love Senior Legal Advisor Office of Policy Control Room 5222 South HEW 330 C Street, S.W. Washington, D.C. 20201 (202) 472-3765	1
	Mr. Donald M. Thayer Director, Office of Policy Control Room 5225 330 C Street, S.W. Washington, D.C. 20201 (202) 245-0531	4
Immigration and Naturalization Service	Mr. Ronald J. Grill Chief, Systems Planning Staff Office of Planning & Evaluation 425 I Street, N.W. Washington, D.C. 20536 (202) 376-8430	4
	Tim Horkan 425 I Street, N.W. Washington, D.C. 20536 (202) 376-8561	5
	Matson, John E. 4012 Wexford Drive Kensington, Maryland 20795 (301) 946-5714	4

	Mr. E. G. Webster Program Manager, ADIT System Office of the Deputy Commissioner 425 I Street, N.W. Room 7003 Washington, D.C. 20536 (202) 376-8434	5
	Mr. Kellogg Wittick Staff Investigator Fraud Investigation Unit 425 I Street, N.W. Room 7003 Washington, D.C. 20536 (202) 376-8367	4
Insurance Information Institute	Mr. Frederick D. Watkins Chairman 110 William Street New York, New York 10038	
Internal Revenue Service	Mr. Larry W. Boehm Intelligence Division Room 2530 IRS Building Washington, D.C. 20224	2
International Association of Chiefs of Police	Mr. Robert L. Monroe Technical Consultant Equipment & Technology Center (ETC) Research Division Eleven Firstfield Road Gaithersburg, Maryland 20760 (301) 948-0922	3
Interpol	Louis B. Sims Chief Interpol Room 1116 Main Treasury Building 15th and Pennsylvania Ave., N.W. Washington, D.C. 20220	3
Law Enforcement Assistant Administration	Joseph T. Kochanski Department of Justice Room 811 Indiana Building 633 Indiana Avenue, N.W. Washington, D.C. (202) 386-4425	5

	Warner Jay Merrill Department of Justice Room 809 Indiana Building 633 Indiana Avenue, N.W. Washington, D.C. (202) 386-4425	5
Lea, Douglas	Suite 510 4720 Montgomery Lane Bethesda, Maryland 20014 (301) 395-3122	5
McDonald's Corporation	Mr. Harry T. Mahoney Attorney McDonald's Corporation One McDonald's Plaza Oak Brook, Illinois 60521 (312) 887-6478	3
Metropolitan Board of Trade	Mr. Leonard Kolodny Manager Retail Bureau 1129 20th Street, N.W. Washington, D.C. 20036 (202) 659-6400	2
Metropolitan Police Department Washington, D.C.	Lt. Kenneth V. Moreland Criminal Investigation Division 300 Indiana Avenue, N.W. Room 4071 Washington, D.C. 20001 (202) 626-2211	2
National Association of Securities Dealers Incorporated	Mr. David P. Parina Research Analyst Department of Regulatory Policy and Procedure 1735 K Street, N.W. Washington, D.C. 20006	2
	Mr. Frank J. Wilson Senior Vice President Regulation 1735 K Street, N.W. Washington, D.C. 20006 (202) 833-4830	2

National District Attorneys Association	Mr. Donald Foster Counsel Economic Crime Project 1900 L Street, N.W. # 601 Washington, D.C. 20036 (202) 785-1225	2
	Mr. Nathaniel E. Kossack Principal Consultant Economic Crime Project 1900 L Street, N.W. # 601 Washington, D.C. 20036 (202) 872-9507	2
National Notary Association	Mr. Raymond C. Rothman President 23012 Ventura Blvd. Woodland Hills, California 91364 (213) 347-2035	
National Sheriffs' Association	Mr. Truman H. L. Walrod Director of Public Affairs Suite 320 1250 Connecticut Avenue Washington, D.C. 20036 (202) 872-0422	3
New York Department of Motor Vehicles	Mr. Robert J. Langling Director Department of Investigations Sivan St. Building, South Mall Albany, New York 12228 (518) 474-0955	5
Sears, Roebuck and Company	Mr. Paul B. Chapman National Security Manager Department 731 B.S.C. #42-27 Sears Tower Chicago, Illinois 60684 (312) 875-8431	2
Securities Exchange Commission	Mr. Ira H. Pearch Division of Enforcement 500 N. Capital Street Washington, D.C. 20549 (202) 755-1256	2

Voting Individual or Organization	Member	Task Force Number
Interbank Card Association	Mr. Robert J. Scully Assistant Vice President 110 East 59th Street New York, New York 10022 (212) 486-1100	2
Selective Service System	Mr. Peter T. Straub General Counsel 1724 F Street, N.W. Washington, D.C. 20435 (202) 343-7174	4
Social Security Administration	Mr. Peter A. Di Rito 6401 Security Blvd. Room 4112 West Highrise Bldg. Baltimore, Maryland 21235	1
	Mr. Roy Wallace Supervisor Social Security Administration 6401 Security Blvd. Room 1124 West Low Rise Bldg. Baltimore, Maryland (301) 594-3472	4
U.S. Postal Service	Mr. Allen O. Peffer Postal Inspector Projects Coordinator External Crimes Branch Inspection Service L'Enfant Plaza, Washington, D.C. 20260 (202) 245-5464	2
Virginia State Department of Health	Deane Huxtable State Registrar of Vital Statistics James Madison Building Richmond, Virginia 23208 (804) 770-6202	5
Williams, Carl B.	Robert B. Carleson & Associates, Inc. Suite 510 555 Capitol Mall Sacramento, California 95814 (916) 442-1877	1

Voting Individual or Organization	Member	Task Force Number
West Virginia Bureau of Vital Statistics	Mr. Jack Pawley County Clerk Kanawha County 5305 Noyes Avenue Charleston, West Virginia 25332 (304) 348-6530	5
 Other Participants:		
Cone, Elmer C.	Director of Corporate Security American Bank Note Company Garrison Avenue and Tiffany Street Bronx, New York 10474 (212) 944-6200	
Deadrick, Edward J.	Vice President American Bank Note Company 70 Broad Street New York, New York 10004 (212) 944-6200	
Gadol, William N.	Accounts Systems Supervisor DEK—Electro Group 1530 Progress Road Fort Wayne, Indiana 46808 (219) 484-8611	
Horn, Howard J.	Account Executive Federal Government Services Commercial Tape Division 3M Company 1101 15th Street, N.W. Washington, D.C. 20005 (202) 331-6944	
Kimball, Peter D.	Director of Security Sales American Bank Note Company 70 Broad Street New York, N.W. 10004 (212) 944-6200	
Manos, Theo	Manager Federal Operations Polaroid Corporation 125 South Reynolds Alexandria, Virginia 22305 (703) 524-2806	

Other Participants:

McCullion, Frank E.	New Product Manager American Bank Note Company 70 Broad Street New York, New York 10004 (212) 542-9200
O'Connor, Ronald	Government Sales Manager Polaroid Corporation 549 Technology Square Cambridge, Massachusetts 02139 (617) 864-6000
Sennott, Donald N.	Associate Administrator Safety Systems Department 3M Company 1101 15th Street, N.W. Washington, D.C. 20005 (202) 331-6954
Sharkey, Charles	American Bank Note Company Land Title Building Room 735 Philadelphia, PA. 19110 (215) 563-7366
Morgan, Reese	8630 Buckboard Drive Alexandria, Virginia 22308

PART I



A LOOK AT THE PROBLEM

SECTION 1

AN INTRODUCTION

Around 5,000 years ago, when primitive man began to domesticate animals, he introduced the concept of using possessions such as rings and axes for "exchange" goods. Previously, he bartered what goods he had for those he wanted. Four thousand years later, the Chinese issued the first paper money, and five hundred years ago banking and paper currency were developed further in Europe.

Today, the exchange of goods and money is a sophisticated process of symbol manipulation in computerized transactions on an international scale. American society -- 215 million strong in 1975 -- participates in this increasingly complex socio-economic system in ways that are markedly different than even twenty-five years ago.

In the past when a person gave "goods for goods" or accepted currency in exchange for his goods or services, he depended to a large extent on two safeguards against criminal incursion in these transactions:

- Personal knowledge of the person with whom he transacted, and

- Reliance on the legitimacy of the medium of exchange.

In today's society, both of these safeguards have been disrupted because of the:

- Transient nature of the population, and
- Necessity of relying on paper substitutes (e.g., checks, credit cards, signature on application) whose legitimacy is not guaranteed.

The modern businessman or government employee does not usually know with whom he deals. Unlike his counterpart in earlier days (who personally checked the teeth of his animal purchase, bit the gold coin, or carefully examined the legal tender) he accepts a substitute, the authenticity of which along with its bearer he has limited ability to verify.

Alvin Toffler in Future Shock states that "Between March 1967 and March 1968 -- in a single year -- 36,600,000 Americans (not counting children less than one year) changed their place of residence."^[1] Members of this mobile population do not know each other in the same way that was once common. When we move, we must carry our identity in the papers we have accumulated that "prove" who we are.

This significant shift in our manner of transacting has not eluded the notice of the criminal element, present in all societies, who find ways to use the prevailing system to their own ends. An "underground" press has published a do-it-yourself manual entitled The Paper Trip whose advice confirms how much the paper identities we carry from city to city have become the currency of fraud, proliferating at an alarming rate. If our dollar currency were being counterfeited at an equal rate, the impact would be obvious and startling, both to the economy and to the general public confidence. However, the increase in the use of false ID to "buy" goods, services, entry into the country, and shelter from prosecution is much harder to detect.

From The Paper Trip: [2]

Everywhere one goes, to prove he's 'somebody', he has to present the appropriate document or card which says he actually is that person. His 'identification', or ID makes him that person. Amazing, right? Well not really.American society is no longer a people society, but a PAPER society....

The paper says who you are, not you. Actually, of course, you do know who you are, but you don't want the paper telling you who you are. The solution? The Paper Trip!

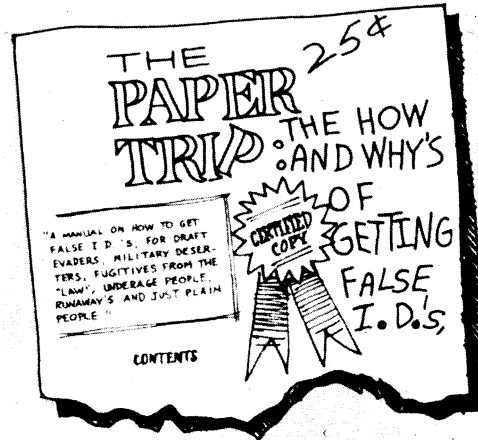


Figure 1. Cover of Underground Publication The Paper Trip

The manual continues with such rhetoric and then outlines, step by step, how one may obtain many false identities and use them for fraudulent purposes. For example, the authors inform their readers that with a false ID:

You can rent a car, never pay more than the initial fee, and drive it all the way across the country and back without paying for more than gas and oil. Use good ID and simply leave the car somewhere after the trip. You disappear. This is not car theft, either.

Such techniques were presented in another underground paper called "Gemini Gallery" in which an article proposed "How to Disappear Completely and Start a New Life with a Brand New Identity." Advertisements such as this also appear:[3]

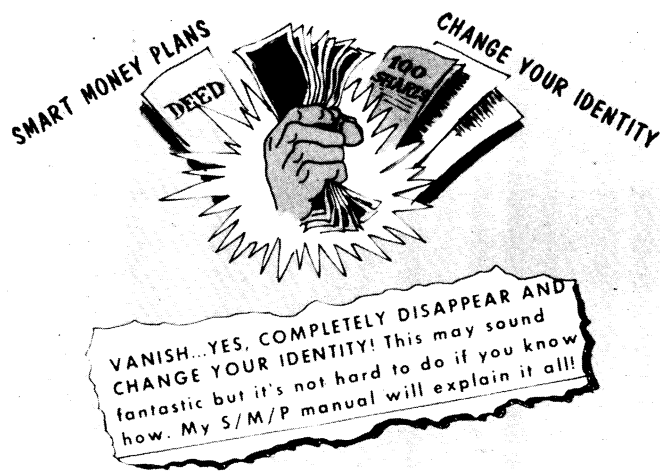


Figure 2. Advertisement on Securing a New Identity

Such disappearing acts are, indeed, not so fantastic. Journalist David Black tried out many of the methods proposed by The Paper Trip and documented the ease with which he established himself in a community under a false identity.^[4] Interviews on the CBS television show "60 Minutes," broadcast on February 1, 1976, provided further documentation of how false ID fraud is perpetrated. A CBS researcher posed on camera as an imposter who successfully obtained and used a complete set of false IDs.

The means do exist to create a false identity in order to commit a crime. Finding out just how big the problem of false identification has become nationwide has been the task of the FACFI. The FACFI has sampled the accumulated experience of officials in Federal and state government, law enforcement, and the business community in order to define the full scope of the problem.

We have found clear evidence of widespread abuses in identification documents commonly used in our society. These abuses not only subject the public to a grievous and illegal "tax" through the fraud committed, they also undermine the trust among individuals upon which our commercial and governmental institutions depend.

CONTENTS OF THIS REPORT

Part I of this report provides a comprehensive picture of the extent to which crimes of violence as well as white collar crimes such as fraud are aided by the use of false identification. We define the scope of the problem as it has emerged from the data collected, define how we have used the data, and categorize the common documents and how they are most frequently used in six major problem areas. False identification and the law is also addressed, both at the state and Federal level.

In Part II, the FACFI proposes some recommended solutions to the problem. We arrived at these solutions after carefully sorting out a myriad of possibilities. Part III contains implementation plans for these solutions, including model state and Federal legislation and guidelines for new regulations.

The Appendices to this report, Part IV, contain a complete collection of all background material, source material, reports, and pertinent data from which the Committee compiled its summary of the problem and its recommendations. The Appendices can serve as a permanent archive of available information on false ID use, which may assist anyone pursuing further the broad problem of false identification in our society.

SECTION 2

THE SCOPE OF THE PROBLEM

The work of the FACFI represents the first serious study of the illegal use of both bona fide and counterfeit documents. We have, therefore, extended our investigation in as much breadth and depth as possible in order to reveal the full impact of the problem in the U.S. Questions of the economic, social and legal effects on the populace were addressed with a view to protecting society from criminal abuse and to making recommendations for safeguards against further abuse. The Committee in this undertaking was dealing with the delicate relationship of Federal and state jurisdictions as well as Privacy Acts [5] and the underlying principle of maintaining the freedoms of an open society. We wished to find answers to such questions as:

- Who is affected by false ID use?
- How big is the problem?
- Where are financial losses incurred as a result of false identification?
- Which are the most significant problem areas?
- Are crimes of violence as well as those of an economic nature aided by false identification?
To what extent?

- What state and Federal laws now exist regarding ID use?
- What state, Federal, or technical safeguards against false ID use already exist? How effective are they?
- What are possible solutions to the problem?
- Which solutions do we recommend?

In finding answers to these questions, the FACFI has begun to uncover a serious problem of considerable import.

EFFECT ON SOCIETY

The criminal use of false identification documents represents a multibillion dollar problem in the United States. False identification is costing American business well over \$1 billion per year. Most of this loss is related to check fraud and counterfeiting, but significant additional losses occur in the areas of credit card fraud and theft of securities and other negotiable instruments. Our estimates of the extent of the effects on business are based on the best available data but should not be considered as complete. The individual citizen pays for the cost of false ID crime against business, primarily in increased cost of goods and services. When small businesses fail because of the particularly severe fraud losses they encounter the consumer also suffers in terms of loss of choice.

The use of a false ID to obtain welfare or other social benefits, to import illegal drugs, or to maintain one's status as an illegal alien or fugitive has a devastating dollar impact on government at

all levels. The success of such activities not only results in direct and indirect costs to taxpayers but also undermines public confidence in government.

Our findings indicate that an individual in our society, in addition to his legal tax burden, pays an additional illegal tax in the form of fraudulent payments and services to users of false IDs committing fraud against government. In New York City, for example, the cost of providing welfare benefits and municipal services has exceeded the resources available from taxpayers. The Immigration and Naturalization Service has estimated that over 10% of New York's population -- about one million persons -- are illegal aliens.^[6] Through the use of false identification, it is probable that these aliens are enjoying either employment or welfare benefits to which they are not entitled. While we cannot yet make accurate estimates of the national impact of these crimes on the individual taxpayer, we would emphasize that the burden of this type of crime is felt by citizens nationwide.

Congress has already been apprised of the false identification problem. The Congressional Record of June 28, 1973, March 5, 1974, and most recently of December 5, 1975 carried warnings of false ID fraud, especially as it is perpetrated in the receipt of welfare benefits and illegal entry into the U.S. Frances Knight, Director of the Passport Office sees investigation of and action on the problem as long overdue. She states that "The Passport Office has been ringing the alarm on passport and identification fraud for 43 years."^[7]

Although false identification has been an area of concern for a long time, current incidents point to growing abuse. Not only have the statistics proven to be extensive in scope, but individual cases have demonstrated blatant and expensive abuse. For example, Miss Knight continues:

Investigators probing Chicago welfare frauds uncovered one case which must be near the top in sheer gall and ingenuity: a thirty-one count fraud indictment charged a welfare recipient with the receipt of illegal welfare benefits, medical assistance, food stamps, in addition to Social Security and Veterans benefits from four non-existent spouses.... The recipient of all these benefits used 80 different names; 30 different addresses and 15 different telephone numbers. The total annual benefits received by this one person was estimated at a minimum of \$150,000 annually in cash assistance alone.^[7]

Added to such losses are those connected with false ID use in other areas. False IDs can be used to:

- Illegally enter institutions of higher learning.
- Collect re-enlistment bonuses from the military services.
- Take entrance exams and tests for unqualified students.
- Escape prosecution or apprehension.
- Gain entry into homes for robbery or crimes of violence.
- Practice a profession under false credentials.

The public is the true victim of the growing menace of false ID use.

METHODS OF INVESTIGATION

The FACFI assembled as much data as possible on the false identification problem in all areas through seventeen surveys developed by its five Task Forces: Government Payments, Commercial Transactions, Fugitives, Federal Identification Documents, and State and Local Identification Documents. The response to these surveys reflects the experience and records of several hundred responsible individuals in business, law enforcement, and government. Additionally, data was obtained from published reports, court records, testimony before Congress, and internal agency records. (See References.) Each Task Force assembled its findings into a report on the scope of the false identification problem in its area of interest. These Task Force reports have served as working documents for discussions of the problem and as primary sources for this report. (See Appendix A.)

As data was reported from the five Task Forces, it was grouped into six general "problem areas" in which there was significant use of false IDs in committing crimes or defrauding business and government. These areas are:

- Drug Smuggling
- Illegal Immigration
- Fugitives from Justice
- Fraud Against Business
- Fraud Against Government
- Other Criminal Activity

Although these areas at times overlap, as in the case of a drug smuggling ring using false IDs as fugitives from justice, the sources of data and an evaluation of their impact were more readily determined by identifying these areas as key parts of the total problem. Section 4 gives a detailed account of each area. The Committee also defined and grouped together the most common identification documents. These documents, their use and abuse, are discussed in Section 3.

DEFINITIONS

Certain definitions were agreed upon for this report. We define false identification fraud as the intentional use by an individual of a document containing a name or personal attributes other than his own for the purpose of assisting in the commission of a crime or in avoiding the legal consequences of a previous crime. This definition is broad enough to encompass the use of a forged check to obtain cash or other benefits, even if no supporting documentation is demanded by the victim of this transaction. However, it does not include simple not-sufficient-funds (NSF) fraud in which an individual presents a check against an existing account in his true name with the knowledge that the check will not clear. Our definition also includes the use of false identification documents for non-criminal transactions by fugitives.

The Committee did consider the non-criminal use of false documents by citizens under certain circumstances, such as the necessity of an individual to establish a "cover" to avoid reprisals from organized crime or a hostile foreign power. Within its charter, however, this was not a primary area of the Committee's investigation. There are adequate legal channels in such cases for obtaining identification documents in a new name.

Included as an identification document (ID) were many types of documents whose intended or major purpose is not identification of the bearer. These include government checks and credit cards, as well as commonly used IDs such as birth certificates, driver's licenses, passports, employee identification badges, and military identification cards. Any of these documents can be used to support a fraudulent claim to an identity. For purposes of classification we have defined three fundamental methods of using an identification document for false purposes.

- Alteration refers to the abuse of a legitimate document by changing significant identification elements, such as the name, photograph, age, or physical description of the legitimate bearer.
- Counterfeiting refers to the unauthorized creation of a complete document by an unauthorized source to support a false identification. For our purposes, counterfeiting includes the unauthorized use of a genuine blank official form to create a false ID.
- Imposture refers to the use of another person's (living or deceased) legal documents as one's own, such as presenting a deceased person's birth certificate to apply for a driver's license.

A COMMENT ON COLLECTED DATA

Sparseness of Data

A common characteristic of responses to the surveys on false identification was the comparative sparseness of quantitative data. In general, the use of false identification is a modus operandi and thus is not recorded as a separate crime. For example, when a suspect is charged with fraud that was assisted by a phony ID, the use of the ID usually does not appear as a separate offense. Thus, when asked about the prevalence of false identification crime, the response of law enforcement officials has been highly qualitative such as, "It happens all the time."

We encountered the same problem while investigating public assistance programs. Although Federal and state statutes require the collection of an immense amount of data on the financial condition of assistance clients, standards for identification of clients or claimed dependents are generally ineffective or non-existent. Thus there are few statistics available nationally on the prevalence and cost of false identification fraud.

Table 1 shows the responses of 24 states to a questionnaire on the use of false identification to obtain food stamps. The majority of respondents were unable to supply us with usable data either because they were not equipped to keep track of such data, or where fraud losses were tabulated, they were not, except in one case, segregated on the basis of false identification. This breakdown is typical of the responses to several other questionnaires; available data on the problem is very sparse:

Table 1

Summary of Responses to Food Stamp Questionnaire

<u>Response</u>	<u>Number</u>
Useful Data Reported	1
Limited Data Reported	6
No System to Collect Data	6
Scope of Problem Unknown	3
Not Aware of False Identification as a Problem	8

Value of Local Data

Although overall figures on the false identification problem were extremely hard to obtain, we observed that excellent data was available covering specific jurisdictions in which careful studies had been performed. These studies were usually performed because of intense local interest (or outrage) over a particular aspect of the false identification problem. In both New York and Pennsylvania, for example, grand jury studies were made covering the fraudulent cashing of welfare checks that had been reported lost or stolen.

In evaluating the financial impact of false identification fraud uncovered in such local studies, it is appropriate to spread costs over the specific locality affected. The cost of forged welfare checks to the City of New York could be expressed as either a fraction of the city's welfare budget or as the cost to the individual New York taxpayer. Where consistent data is obtained from distinct but similar jurisdictions (e.g., different cities of over

50,000 population) reasonable inferences could be made as to the costs in other similar jurisdictions not reporting. We have, however, refrained from large-scale extrapolation of costs based on local data.

Minimization of Fraud Losses

We have observed a tendency on the part of some survey respondents to minimize fraud losses. This minimization may take the form of burying such losses in "the cost of doing business" or in pointing out the relatively small fraction of all transactions that are found to be fraudulent.

Many people also wish to minimize publicity about fraud and its effects and have ostensibly good reasons to do so. These reasons range from the feeling by the average citizen that he is already "hassled" when he attempts to cash a check or obtain benefits from a government agency, to the feeling that publicizing the success of fraud will convince more people to try it. However, these rationales deny the fact that no problem can be dealt with until it is honestly and accurately defined. Such a problem definition at least reveals what might accurately be called "the cost of doing nothing" about the problem. Costs (intangible as well as monetary) of proposed solutions can then be compared with the present situation.

The argument by some that "publicity of fraud increases fraud," is specious since, as we have shown, methods of falsifying and abusing IDs are readily available through underground sources to those willing to locate and pay for the information. Educating the potential innocent victims of ID fraud -- a significant portion of our U.S. populace -- and prosecuting offenders may provide a far greater benefit than any hypothetical danger from exposure of victims to the facts of false ID use.

SECTION 3

COMMON IDENTIFICATION DOCUMENTS

The United States does not have a unique document that can be used to verify the identity of the bearer. Because of the frequent need for such verification in employment and commercial transactions, several types of documents not designed for such use have become de facto identification documents. The birth certificate, which is legal proof of only age, place of birth, parentage and citizenship of the named individual, is extensively used in employment and in applications for benefits or for obtaining other documents. The state-issued driver's license has become indispensable as an identification document for many commercial transactions; for this reason, many states now issue special "licenses" to non-drivers and blind persons. Several other documents issued by government agencies and private sources also serve as de facto identification documents.

This section summarizes the various types of common identification documents that are used either as primary IDs to defraud or gain access or benefits, or as breeder documents for obtaining further identification to use or falsify.

BIRTH CERTIFICATE

Birth certificates^[8] in the United States are generally kept in local vital records offices, over 7,000 of which are authorized to issue certified copies of birth certificates. (Only in a few states are birth certificates issued exclusively at the state level.) Approximately 10 million certified copies of birth certificates

are issued each year, and over 80 percent of those requested are received and processed by mail. The name and return address of the requestor are usually the only indications of the requestor's identity.

There are no uniform standards for either the form of the document or for processing requests for certified copies. A request may legally be made for a copy of another person's birth certificate if the requester is related to the individual or has legitimate need for the document. Some states and Washington, D.C. regard all vital records as public documents, a copy of which must be supplied to any interested person. We have found no state law that authorizes a registry official to refuse to honor an unsigned request for a birth certificate.

Under these conditions, an imposter can quite easily acquire a certified copy of the birth certificate of a person, and this certificate can then be used to obtain additional IDs in the name of the person whose identity the imposter assumes. Frequently an imposter will choose to assume the identity of a person born about the same time as himself but who died in early childhood. This way of obtaining false identification -- called the Infant Death Identity (IDI) method -- is difficult to detect because state birth and death records are largely uncorrelated and an imposter's identity is unlikely to be challenged. To apply for a copy of a birth certificate an imposter needs only the date, place of birth and names of the parents of a deceased person. This information can be obtained either from a death certificate (found by browsing in a local vital records office) or from newspaper accounts of a person's death. The process of obtaining and using false identification by the IDI method is illustrated in Figure 3.

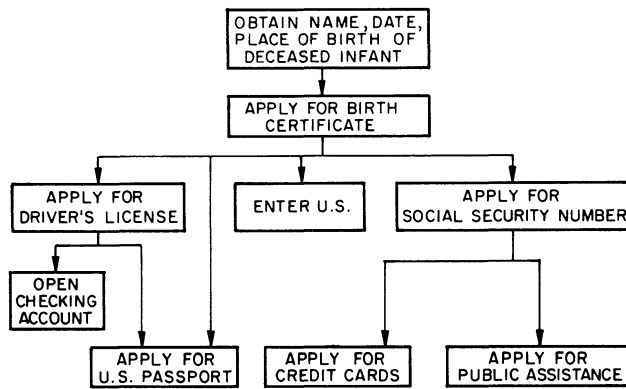


Figure 3. The IDI Method

Immigration and Naturalization officials have documented many false claims to citizenship, many of which used the IDI method of obtaining false documents. They relate, for example, the case of an illegal alien wanted for homicide in the Phillipines who created several new identities for himself in California using the records of deceased U.S. citizens. He also used the IDI method to obtain fraudulent birth certificates and U.S. passports for at least 12 other illegal aliens, charging fees of up to \$2000 for this service before being apprehended.

Although application for certified copies by imposters appears to be the most significant abuse of the birth certificate, counterfeit and altered certificates have also been used in false identification frauds. Counterfeiting is aided by the fact that forms

of birth certificates and authenticating seals vary widely in the U.S.; over 1,000 different forms may be found of presently issued certified copies. Counterfeit documents can be obtained from underground printers and are difficult to detect if the corresponding legitimate document is not secure against photocopying. Documents altered to change date of birth or to invent an additional "dependent" for tax or welfare purposes are less common. Erasure and inexpensive photocopying are the methods usually attempted. Genuine blank forms and even official seals are sometimes used to create counterfeit certificates. Theft of blank forms or misuse by dishonest employees is made easy in some states by the lack of strict security and accounting procedures for blank forms.

DRIVER'S LICENSE

Driver's licenses^[9] are issued by all 50 states and the District of Columbia. The popularity of the license as a credential for business transactions is due in part to the fact that a driver's license always carries the bearer's signature, address, birth date, and some type of physical description. A photograph of the legal bearer is used on 36 of the 51 types of U.S. license; 46 carry the bearer's height, 40 weight, 36 color of eyes, and 18 color of hair. The bearer's Social Security number (SSN) is collected and maintained in the Motor Vehicle Administration's record system in 31 states. In eleven jurisdictions the SSN serves as the license number; however, under the provisions of the Privacy Act this use of the Social Security number cannot be extended to record systems not using the SSN prior to January 1, 1975.

Forty-four jurisdictions claim to seek positive proof of full name, date, and birthplace of an applicant prior to issuance of an initial driver's license; however, such proof may be waived if the

applicant presents a valid license from another state. A birth certificate is always accepted as proof; some states, however, accept school records, military ID, or a baptismal certificate as well. Thirty-three states presently issue an identification card (usually in the same form as a driver's license) to non-drivers; in four of these states, a birth certificate or similar proof of age and birthplace is not required to obtain such a card.

Since the birth certificate is accepted as "proof" of identity in applying for a driver's license, a false birth certificate can be used to obtain a license in the same false name. Counterfeit documents that are often good enough to pass close visual inspection are also legally available from "underground" sources. Because the form and content of a driver's license varies, detection of a counterfeit out-of-state license by merchants or local police is extremely difficult. False application and counterfeiting appear to be the most common forms of abuse of driver's licenses. Twenty-nine types of driver's licenses incorporate measures that resist attempts at alteration; however, none are foolproof and some are still too easily altered.

U.S. PASSPORT

Passports^[10], which are essential for international travel, can be used for either legitimate purposes or such illegal purposes as drug smuggling. By definition, a passport attests to the identity and citizenship of its bearer; therefore, specific evidence of identity and citizenship is required from a passport applicant. A birth certificate is usually the accepted proof of citizenship; identity can be established either by a government-issued photo ID (such as a driver's license) or by affidavit of a witness who knows the applicant personally. Applications must be submitted in person

before a passport agent or other authorized official. After a waiting period of several days, the completed passport is delivered by mail or may be picked up in person by the applicant.

Because in almost all cases of passport fraud there is false ID use, the Passport Office has been concentrating on alleviating this problem. When in 1972 the number of passport frauds detected in the United States rose sharply, from 174 in 1971 to 288 in 1972, the Passport Office initiated a fraud detection program. As a result of this program, the Passport Office increased its ability to detect fraud in the application stage (as opposed to detection upon arrest) from 28% of reported cases in 1973 to 53% in 1975. The number of domestic passport frauds detected by all methods for fiscal year 1971 through 1975 increased: from 174 in 1971; 288 in 1972; 449 in 1973; 553 in 1974; to 617 in 1975. Detecting these frauds upon application has helped keep down those criminal activities, especially drug trafficking and illegal alien entry, that are perpetrated through passport fraud.

U.S. VISA AND ALIEN ID CARD

A visa^[11] is a document issued by a host nation granting permission to an alien to enter the host nation. A U.S. immigrant visa permits the bearer to settle and work in the U.S. and eventually to apply for citizenship. An immigrant visa is generally issued to an alien who has either a close family relationship with a U.S. citizen or resident alien, or a profession or job skill that is in short supply in the U.S. The number of these visas granted each year is limited by law. Aliens who have neither family ties nor job skills sometimes participate in sham marriages or obtain fraudulent documents to get immigrant visas.

A U.S. nonimmigrant visa permits a temporary or limited stay (1) by a visitor on business or pleasure; (2) by a student; or (3) by any alien who has a residence abroad (that he does not intend to abandon) and who has sufficient funds to pay for the trip. Some nonimmigrant visa categories permit specific employment to aliens who are, for example, journalists, foreign government officials, trainees or artists; however, the validity of this type of visa depends on the alien's continuing the same work. An alien who is unable to obtain an immigrant visa often attempts to get a nonimmigrant visa by using fraudulent documents to misrepresent his reasons for visiting the U.S., his financial status or his employment. He also can buy a counterfeit visa or an altered passport that already contains a valid visa. Once in the U.S. he overstays his visa and becomes an illegal alien.

Both immigrant and nonimmigrant visas are issued by consular officers abroad; an immigration officer examines each entering alien's visa at the port of entry. Each immigrant is then given a Form I-151 ^[12] a photo ID card which serves to identify him as a legal resident alien. When traveling outside the U.S. he uses this as evidence of his right to re-enter the U.S. An alien set on illegally entering the U.S. might use a stolen or counterfeited I-151, while an illegal alien already in the U.S. might use an I-151 to establish his identity as a legal resident alien.

Immigration officers also issue border crossing cards ^[12] to permit Mexicans to visit the U.S. border area without a visa. Like the I-151, these photo ID cards are subject to counterfeiting and alteration to gain illegal entry into the U.S.

SOCIAL SECURITY CARD

Although never intended by the Social Security Administration to be used for personal identification, the Social Security card^[13] has become an important document in maintaining employment records and in obtaining other identification documents. Although the Social Security number is widely used for tax records and as a driver's license number, it is neither unique nor protected against imposter use. The Social Security Administration estimates that over 4.2 million people have more than one SSN.^[14]

Prior to 1974, SSNs were issued in the name of any individual upon submission of an application form, in person or by mail, without any other evidence of identity. Evidence of identity, age, and citizenship of the applicant is now required. In recent testimony before Congress,^[15] an official of the Social Security Administration listed the kinds of documents that are acceptable in applying for an SSN. The list included several documents that are easily forged or obtained under false pretenses, i.e., baptismal certificate, library card, and voter registration card.

The Social Security card in its present form has no safeguards against counterfeiting. Unofficial "cards" are also available by mail from commercial suppliers. Ostensibly the reproductions are intended only to remind the cardholder of his SSN; however, the suppliers do not check the authenticity of SSNs provided by their customers, so the unofficial cards can be used to support a false identity.

SELECTIVE SERVICE DRAFT CARD

It is estimated that as many as thirty million draft cards were issued before the last one was sent out in 1975. Although they were issued only as a means of informing the individual of his classification or Selective Service number, they have been used as identification cards to prove age as well as for other uses for which they were not designed. The draft card is notoriously unsecure: it is merely a typed postcard; is unserialized; the background information at the application stage is largely unverified; it is easily forged; it contains no photograph; and its uses rarely, if ever, cause it to be scrutinized by the issuer.

VOTER REGISTRATION CARD

Voter registration cards [16] are issued by local Boards of Election and are used by their holders as evidence of age and citizenship for limited purposes. For example, these cards are frequently presented by persons to support their claim of U.S. residence for re-entry from Canada and Mexico. However, they are not accepted as evidence of age and citizenship when applying for a U.S. passport, and are not usually accepted as part of a driver's license application. Limited investigation into voter registration procedures by FACFI staff suggests that these cards are very easy to obtain under false pretenses. Registration by mail is permitted in many jurisdictions, and even where a personal appearance is required, the only evidence of age, citizenship, residence, and identity of the registrant that can be demanded by local officials is a verbal declaration given under penalty of perjury. The ability of the local Board of Election to check any of the entitling data is typically very limited.

Since the voter registration card contains no physical description of the legitimate bearer, it can be used with relative ease by imposters. Voter registration cards are commonly used by aliens attempting illegal entry into the U.S. and have been sold to illegal aliens for this purpose at prices ranging up to \$350.

CREDIT CARDS

Although a credit card^[17] contains certain printed and embossed information which, when checked by a merchant, may confirm the validity of the card, the primary means of cardholder authentication is the signature on the card. Normally no other ID is required to charge goods or services at a wide variety of retail outlets unless a question arises as to the validity of the card or the authenticity of the cardholder. Bank cards such as Master Charge and Bank Americard can even be used to obtain cash.

Credit cards are obtained by mailing an application form that requests credit information, but not information about identity; a credit and reference check is then made before issuing the card. Cards in a false name can be obtained by false application or by theft of legitimate cards from the mail or from cardholders. One article reported:

Credit card thieves sometimes use the cards they steal but more often they peddle them in underworld circles. When the black market was at its height in New York, a thief would sell a card to a dealer for \$25; the dealer in turn would dispose of it for as much as \$150 if the card were 'clean' -- i.e., without a signature.^[18]

Although use by an imposter of a stolen credit card appears to be the most common form of abuse, obtaining credit cards in many

identities is an equally serious abuse. One recent newspaper account told of a credit card fraud committed by one person who had obtained 1,000 credit cards using 300 different false identities.^[19]

NON-GOVERNMENT IDs

When a person applies for benefits or is establishing identity for other purposes, he sometimes uses privately-issued identification to reinforce other documentation. Privately-issued documents include baptismal certificates, student ID cards, employee badges, business cards and membership cards of all types. Baptismal certificates are sometimes accepted in lieu of birth certificates to establish age, e.g., of a dependent child. Such documents, however, are easily obtained or constructed fraudulently. Blank baptismal certificates are sometimes available at religious-goods or stationery stores, or can be obtained by mail. Commercial photo IDs can be made to order by photographic studios in every large city.

This non-government, unofficial ID was found to be the type most frequently used in the cashing of checks stolen from the mails.^[20] Business and membership cards can usually be obtained from job printers, and many employee badges, courtesy cards, and other types of unofficial ID can be easily counterfeited.

SECTION 4

FRAUDULENT ID USE

Crimes assisted by the use of one or several false IDs represent a significant national problem. Directly or indirectly, this problem affects every American household in terms of the cost of government benefits paid to imposters, the cost of fraud against business that is passed on to consumers, and the threat to public health and safety from drug smugglers and fugitives.

Possession of false identification documents gives a criminal, or someone intent on committing a crime, the means to appear and disappear almost at will and without a trace. Attempts in FAFI surveys to profile the typical user of false IDs were largely unsuccessful. As in the case of many types of fraud, successful perpetrators of false identification fraud are quite indistinguishable from the groups they pretend to represent. Thus, a request for a profile of the typical suspect of welfare fraud using false identification yielded the description of a young, unmarried, unemployed woman resident of a metropolitan area, which is in fact a description of a typical legitimate welfare mother as well. Similarly, the typical check forger^[21] can be described as a middle-aged male, which also describes a large percentage of legitimate check users.

The only exception we have found to the "invisibility" of false identification suspects occurs in passport fraud.^[10] Here the typical offender is usually an international traveler, 18 to 40 years of age, who does not travel with a family group or on government-related

business. Since this description fits only 40% of the passport holders, the possibility exists of decreasing passport fraud to some degree by screening for user type in review of passport applications.

One further distinguishing characteristic has emerged of those involved in false identification fraud; suspects are more likely to be repeat offenders than is the average for criminals apprehended. For example, 76% of those arrested for forgery and counterfeiting in 1971 had previously been arrested for the same crime at least once;^[21] this compares with a recidivism rate of only 68% for overall crime.

The universality of the use of false IDs by criminals is unquestionable. A random sampling^[22] of 500 cases in which a fugitive was being sought by the FBI showed that in every case the fugitive was known to have used at least one alias. In 75 of these cases, the fugitives had previously been identified under five or more aliases, and in one case the subject is known to have used more than 30 different false identities.

Besides aiding drug smuggling, illegal immigration and fugitives from justice, the use of false IDs materially assists fraud involving stolen checks, credit cards, securities, and welfare and Social Security benefit checks. Although we cannot provide firm figures on the scope of government benefit checks stolen from the mails and subsequently cashed by forgery, the experience of state and local welfare departments suggests that such losses are in the order of hundreds of millions of dollars annually.

The U.S. Postal Inspection Service during FY 1974 received reports of 140,864 checks with a total face value of over \$22 million stolen from the mails and subsequently cashed. A sampling of almost 6,000 of these checks was undertaken by postal inspectors

to determine the type of false ID used to cash the checks.^[20] About 25% of the sampled cases were definitely determined to involve the use of a false ID other than the forged check itself (which becomes a false ID upon forgery). When cashing of a stolen check was supported by another ID, the one most commonly used was the commercial photo ID, followed in frequency by a stolen welfare ID and state driver's license.

This section presents data on the significant fraudulent uses nationally of false IDs. These findings are probably conservative because our studies are based only on those cases of false identification that have been detected. The crimes we illustrate would be much more difficult to commit if criminals did not have such easy access to false identification documents. Table 2 summarizes the extent of the problem in the six problem areas, discussed in more detail below, and lists the sources of information for this estimate.

Table 2
Summary of Scope and Impact of
National False Identification Problem

Problem Area	Scope of Problem	Extent of False ID Use	Sources of Data
Drug Smuggling	> \$1 billion/yr.	80% of hard drugs smuggled	Customs Service, Drug Enforcement Administration, Passport Office
Illegal Immigration	> \$12 billion/yr. *	Unknown; used in entry, employment, welfare application	Immigration & Naturalization Service, independent studies
Fugitives From Justice	> 300,000 fugitives/yr.	~ 100% of Federal cases	FBI, sheriffs and police survey
Fraud Against Business	> \$3 billion/yr. †	> \$1 billion/yr.	American Bankers Assoc., independent studies
Fraud Against Government	Unknown	Unknown	Surveys of Welfare officials, published studies
Other Criminal Activity	Unknown	Very common	FBI, sheriffs and police survey

> More than

* Estimated U.S. tax burden

† Includes out-of-pocket losses and cost of collection attempts

DRUG SMUGGLING

False identification is indispensable to the well-organized smuggling rings that carry in the bulk of the hard drugs supplied to U.S. addicts. Statistics compiled by the U.S. Customs Service and the Drug Enforcement Administration^[23] show that 80% of all hard drugs are imported by rings making extensive use of false IDs. One such group whose smuggling activities have been carefully studied is the Brotherhood of Eternal Love.^[24] Between 1968 and 1973, this group alone is estimated to have smuggled 24 tons of hashish into the U.S. The principal means by which this group avoided detection was by securing documents, such as U.S. passports, under false names.

The activities of the Brotherhood of Eternal Love indicate the extensiveness of false ID use for a solitary smuggling group. As of October 1973, 130 separate passport frauds had been attributed to members of this group; fifty-one of these frauds were accomplished with counterfeit birth certificates. Indictments were obtained against 25 individuals. The individual who was considered to be the leader of the LSD operation was arrested on four separate occasions under four different false identities; on each occasion he escaped by posting and forfeiting relatively small bonds before his true identity was discovered.

Accurate records of seizures of dangerous drugs by the U.S. Customs Service were obtained for fiscal years 1967 through 1973.^[23] In FY 1973, seizures involving well-organized rings using false IDs totalled \$100 million ("street value" at time of seizure). From statements obtained by captured members of these rings, the value of drugs successfully smuggled by these groups was estimated as \$1 billion

in FY 1973, which does not include estimates of drugs smuggled by unknown individuals or by individuals not using false IDs. Assuming the level of smuggling as constant (though, in fact, its increase is more likely), we conclude that a minimum of \$1 billion each year is being lost in illegal purchases of narcotics made available through false identification. Such an estimate does not include the indirect costs to society, such as the value of goods stolen by addicts to purchase the drugs, the cost of programs to treat the addicts, or their movement through the criminal justice system.

ILLEGAL IMMIGRATION

The most recent estimate^[25] of the number of illegal aliens presently living in the U.S. is about 8 million, 6 million of whom are adults. The U.S. Immigration and Naturalization Service believes that the number of such illegal aliens is increasing at the rate of more than 250,000 per year. The net tax burden on the U.S. for each adult illegal alien is estimated in a recent study^[26] to be \$2,000 per year. This estimate considers direct costs such as public services and welfare benefits to the extent they are not supported by taxes paid by the aliens and indirect costs related to the job displacement of U.S. citizens by illegal aliens. The tax burden does not include losses from tax evasion by aliens or balance of payments losses from funds sent out of the U.S. by illegal aliens. The total estimated tax burden from the presence of illegal aliens is thus estimated at over \$12 billion for 1976. (A dissenting opinion on these tax burden figures is expressed in Appendix F2.)

The extent to which this staggering burden can be attributed to the use of false documents by illegal aliens is unknown but believed to be substantial and increasing.^[27] Over 15,000 illicit INS

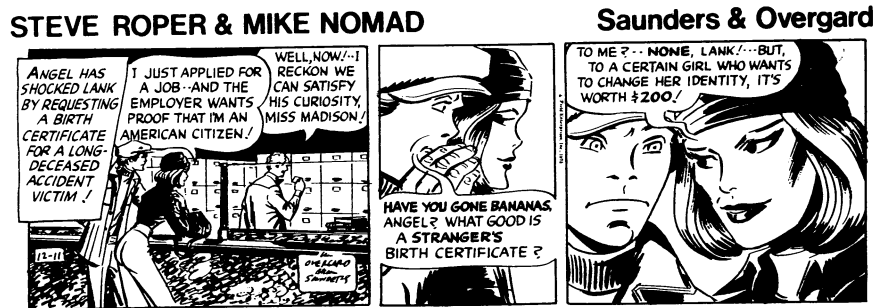
documents (border-crossing and alien registration cards) were encountered by INS personnel during fiscal 1975; these documents had been purchased in Mexico from document vendors and smuggling rings at a total cost of \$1.7 million. The number of illicit documents seized is believed to be only a small fraction of those in use by illegal aliens. This belief has been supported by occasional large seizures of counterfeit forms and the fact that the black market price of such documents is declining steadily.

A study on the subject, the Fraudulent Entrants Study, which is part of the Major Illegal Alien Study being undertaken by INS during 1976, was recently completed by INS. This study indicated that in FY 1975 at least 14 times the routinely detected number of aliens with fraudulent alien documents successfully entered through Southwest border ports. Additionally, at least 10 times the routinely detected number of aliens falsely claiming U.S. citizenship along the Southwest border were successful in gaining admission. Together, these groups account for at least a quarter of a million illegal entries by the use of fraudulent documents or false verbal claims to U.S. citizenship^[28]

It is reasonable to assume that false claims to legal status or citizenship are used by illegal aliens in obtaining employment and welfare benefits to which they are not entitled, which contributes heavily to the estimated tax burden previously cited. The use of false documentation by illegal aliens is probably increasing because of the recent requirements for evidence of age, identity, and citizenship in applying for a Social Security number, and new state legislation restricting payment of welfare benefits to illegal aliens.

FUGITIVES FROM JUSTICE

Escaped prisoners and other dangerous fugitives almost always obtain false identification documents to avoid detection and capture. [29] Members of militant groups such as the Black Liberation Army, Weather Underground, and Symbionese Liberation Army, [30] who have gone underground to carry on their activities, make extensive use of false IDs. They have been able to escape arrest for violent crimes for considerable periods of time because of effective false identification. Figure 4 shows that false ID use, including the specific use of the IDI method previously mentioned, is common enough knowledge to be included in the public's comic strip lexicon.



STEVE ROPER by Allen Saunders and William Overgard, Courtesy of Field Newspaper Syndicate.

Figure 4. Dangerous Fugitives: Customers for False IDs

The number of fugitives from justice is considerable. Between 1973 and 1975 an average of approximately 160,000 "criminal wanted" records each year were entered into the National Crime Information Center (NCIC), but not all persons sought under fugitive warrants are entered into the NCIC. The Federal Bureau of Investigation in fiscal 1974 located 37,891 fugitives indicted on Federal offenses or for crimes involving interstate travel. [31]

The major impact of the use of false identification by criminal fugitives cannot, however, be measured in the number of offenders or dollar losses. Its impact is felt more in the loss of public confidence in law enforcement caused by the success of notorious fugitives in maintaining their covert status and in the danger such fugitives pose to society. We have found that their success is critically dependent on the availability of false IDs. While we cannot estimate the cost of the use of false IDs by fugitives, we emphasize that the ability of dangerous criminals to move freely and undetected in society is a serious threat to public safety and police morale.

FRAUD AGAINST BUSINESS

Check Forgery and Fraud

In a nationwide survey of police and sheriff's departments fraudulent cashing of checks, either stolen from the mails or drawn on accounts bearing false names, was cited as the most common criminal use of false IDs. Bad checks have become a major cause of financial loss to banks, far exceeding the loss from robbery and burglary combined. [32] This loss is due in great measure to the successful use of one or more complete sets of false IDs that are part of the

usual working equipment of the experienced forger or check fraud artist. See Figure 5. A recently arrested check forger had in his possession 30 different birth certificates with which he had already obtained 15 driver's licenses, 17 Social Security cards, 11 checking accounts, 4 credit cards, and 10 miscellaneous IDs.^[30]

In 1973, about 25 billion checks were written in the United States; of these, approximately 0.65% (one out of 150) failed to clear and were returned to the depositor. These "return items" amounted to 169 million checks returned in 1973,^[33] 25 million of which proved to be counterfeit or forged, representing false identification fraud. Since the average dollar amount of all bad checks is estimated to be around \$30, total out-of-pocket losses from counterfeit or forged checks amounts to over \$750 million.^[21] The cost of attempting to collect on these checks, which averages about \$10 per check, must be added to this total. Thus, we estimate that the losses due to counterfeit and forged checks totalled approximately \$1 billion in 1973. Since the number of checks written is increasing rapidly from year to year, these losses may be expected to increase, even if the rate of forgery and counterfeiting does not.

Check fraud hits particularly hard at retail food stores and small businesses. The U.S. Department of Commerce estimates that bad check losses for food transactions exceeded \$450 million in 1974.^[34] The typical food store receives checks for 85% to 90% of its total sales and in addition often acts as a "bank" to cash payroll and government checks for customers. Bad check losses have been reported by members of the National Association of Food Chains and the Super Market Institute^[35] at about 0.04% of total sales; therefore, a single average food store, with an estimated sales volume of \$60,000 per week, puts \$240 per week or \$12,500 per year in the hands



Figure 5. A Common Check Cashing Scene Could Really Be a "Bank Robbery"
Aided By A False ID "Disguise".

of check thieves. About 60% of these losses appear to involve false identification fraud (forgery and counterfeiting), while 40% are uncollectible "not-sufficient-funds" cases. We do not count as losses the much larger number of returned checks on which collection is ultimately made.

According to a study conducted by the Small Business Administration,^[36] bad checks accounted for about 13% of all crime-related losses to business in 1967-1968. The small business suffers a loss rate (in percentage of profits) over 3 times the average of business in general and 35 times that reported for large businesses.

Banks take the loss on only about 5% to 7% of all bad checks; however, the dollar losses tend to average considerably higher than in other businesses. The principal form of fraud affecting banks is forgery of stolen checks, with counterfeit checks contributing significantly also.^[37] The American Bankers Association estimates bank losses due to forgeries in 1974 at \$50 million. Even though the direct loss is suffered by the first acceptor of the check rather than the bank, banks and their depositors suffer indirect losses as the result of bad checks, such as the cost of investigating incidents.

A survey conducted of 1974 losses to banks resulting from individuals presenting false identification for various bank activities revealed significant losses per crime. The average loss to the banks from checks cashed through the use of false IDs was \$216, while the average for cashing savings bonds was \$643. However, banks were much harder hit by the use of false IDs in opening new checking and/or savings accounts; total funds lost in this activity were \$3,734,521 with an average per crime of \$6,586. Most of these crimes were committed with falsified driver's licenses, the form of identification

most often used in bank transactions. The Insurance and Protection Division of the American Bankers Association believes this survey "has verified the long-held belief of bankers and law enforcement officials that phony driver's licenses are the most prevalent means of false identification used to defraud banks."^[38]

Credit Card Fraud

Credit card transactions have continued to grow in volume; the gross billings of the two largest bank credit card associations (Bank Americard and Master Charge) reached \$17.6 billion in 1974.^[37] Losses to business can occur as a result of three types of false identification fraud using such cards: misuse of a lost or stolen card by an imposter, use of a counterfeit card, or application for a card by a person with criminal intent. These losses may affect either the issuer of the card or the merchant accepting it, depending on circumstances.

A 1974 U.S. Department of Commerce publication placed losses on bank credit cards from all sources at approximately \$500 million per year.^[36] Sources of specific estimates on credit card fraud losses have been limited, but the Committee has received helpful information in the application area from the Fraud Application Section of the Western States Bankcard Association. (Their letter to the FACFI is included as Appendix E2 of this report.) Formed in January 1975, the Association's unit may be the only investigative one of its kind devoted exclusively to identifying and combatting fraudulent applications in the credit card industry.

G. Pat Bland, Agent in Charge of the Section, describes the numerous well-organized groups they found operating in California with ties to other states (Appendix E2):

These organizations are involved in the establishment of phoney credit files, loan fraud of all types and phoney businesses, some of which go so far as to file articles of incorporation to further their devious ends. Most of the better organized groups utilize fraudulent identification to insure success in their ventures. One such business averaged in excess of \$5,000 per month in deposits on Master Charge Cards that were all obtained in fraud applications.

Individual cases investigated by the Fraud Application Section included one suspect, wanted for murder, who had used 37 identities, and another who victimized a California bank for \$26,000 in four months with only two cards. The examples uncovered by the Association seem to be only a part of a much larger incidence level. Bland continues:

Our statistics show an increase in caseload during this first year of 673% over 1974. Initially, our average loss per case was approximately \$2,800. After our first year of operation, we had reduced this average loss to \$405 per identified fraud application.

He notes that the most measureable results are obtained when they have total participation by the credit industry.

The experience and information being accumulated by this group verifies the FACFI's estimation of the vast amounts of fraud that have yet to be uncovered, especially in areas such as credit card fraud,

where virtually no reliable data has been forthcoming until now. The Association feels that "there are literally thousands of fraud applicants in California alone, and in their opinion, the same situation exists in every major metropolitan area in the nation."

Securities Fraud

False identification fraud makes up only a portion of the actual or potential fraud losses in the securities industry; many reports on securities fraud do not distinguish between potential and actual losses, much less between false identification fraud and other types of crime. It is therefore necessary to define carefully terms used to describe securities losses in order to eliminate confusion introduced by widely differing loss estimates contained in various reports.

The FACFI is specifically concerned with the value of lost, stolen or counterfeited securities that are negotiated through the use of false IDs. Because they represent ownership of value, securities certificates are of interest to criminal elements as much as cash or checks. If the securities are "bearer documents," that is certificates which are not registered and imprinted with the name of a specific owner, they are negotiable by anyone and the bearer is assumed to be the legal owner. Bearer certificates do not require the use of an ID for negotiation; therefore, false identification would not be necessary for their negotiation by a criminal. Registered certificates bear upon their face the name of the owner of record, are legally negotiable only by the owner of record, and are therefore similar to checks, in that some measure of fraud is necessary to transfer ownership without consent of the rightful owner. This fraud may take the form of alteration of the

certificate or use of false ID in an attempt to impersonate the owner of record.

A "risk of loss" to the financial industry arises when securities are lost or stolen; the risk equals the value of those securities. An "actual loss" occurs only when lost or stolen securities are converted to cash. Although an owner of securities incurs a loss when bearer certificates are lost or stolen, he can replace registered certificates. Loss may still be suffered by the financial industry if registered certificates are fraudulently negotiated. Negotiation may be accomplished by direct conversion to cash through sale or use of the certificates as collateral to secure a loan. We are concerned only with the cases of actual loss resulting from securities which are lost, stolen, or counterfeited and subsequently negotiated through the use of false ID; data collected from the sources mentioned below were evaluated in the light of this concern.

In 1973, testimony before the Permanent Subcommittee on Investigations, the Committee on Government Operations, of the U.S. Senate included the statement by Mr. W. Henry duPont that "...it is our considered judgment that the dollar value of lost, missing and stolen Government, state, municipal and corporate securities could be as high as \$50 billion".^[39] This figure was based on information from an estimated 1% of the total number of handlers of securities. No basis was established to validate the extrapolation, to define the risk of loss, actual loss, or applicability of false ID to this figure.

The U.S. Marshals' Service, on the basis of a 1974-1975 survey of 287 banking institutions, stated that during the three-year period 1971-1973, 11 incidents of stolen or fraudulent securities

representing a dollar loss of \$5,136,554 were reported.^[40] Loss in that report was equated only to risk of loss as defined above. Neither actual loss nor false ID involvement were addressed specifically.

In a report of a survey conducted by The New York Stock Exchange entitled the "Magnitude of Lost and Stolen Securities in N.Y.S.E. Member Firms 1969-1972," the market value of lost or stolen securities reported to the N.Y.S.E. Stock Clearing Corporation ranged from a low of \$4.6 million in 1973 to a high of \$14.7 million in 1970. Data from all reporting organizations to the N.Y.S.E. Stock Clearing Corporation ranged from a low of \$24.1 million in 1972 to \$104 million in 1973.^[41] Since these figures do not specifically address actual loss or the extent to which false identification may have been involved, they are of little direct value to FACFI.

The National Association of Securities Dealers (NASD), Inc., conducted a survey of its membership covering the period 1972-1974 that attempted to cover the specific area of false identification. Replies from 2,734 respondents, representing an almost 90% response, reported 44 distinct cases of loss "...incurred vis-a-vis counterfeit securities and/or a return to the marketplace of securities previously obtained through some forms of misappropriation". The value of this loss was reported as \$563,412.^[42]

Since the NASD survey specifically addressed the area of concern to the FACFI, the information reported therein appears to be the best indication of the scope of the false ID problem in securities fraud.

Embezzlement

Embezzlement is another area in which fraud against business may be perpetrated. While the majority of embezzlers operate under their true name, the potential of infiltration of business firms by employees hired under false identities should not be overlooked. In 1974, the Washington, D.C. Metropolitan Police Department investigated twenty-two cases of embezzlement in which the suspect was found to be using a false ID.^[43] These cases represented 15% of all complaints for embezzlement handled by the Department in 1974. The average loss to business from each reported incident was about \$3,000.

Banks and other credit grantors are also subjected to large losses through embezzlement by persons making loans with false identification. Typically, this type of fraud involves a dishonest bank officer who processes loans for a confederate posing as a legitimate borrower. However, the "borrower" cannot be located when the loan falls due.

Another type of loan fraud is accomplished by a criminal's creating excellent credit ratings in the names of fictitious persons through the internal manipulation of the data banks of credit-reporting services. Participants in these loan fraud schemes acquire complete sets of false IDs to match their bogus credit ratings. A single bank victimized by one such scheme lost \$200,000 in loans on nonexistent cars made to borrowers with false identification.^[44]

These "nonexistent borrower" schemes have been blamed for a major part of the \$188 million fraud and embezzlement losses reported by financial institutions in fiscal year 1975.^[45] Total losses to all credit grantors from false ID credit swindles may never be known

because such losses can be unwittingly written off as simple bad debts. The effectiveness of false identification in removing all traces of the perpetrator often makes it difficult for victimized businesses or prosecutors to sustain a fraud complaint.

FRAUD AGAINST GOVERNMENT

We have found that most state and national social welfare programs are very vulnerable to false identification fraud. Such fraud may take various forms -- applying for benefits under several identities, claiming nonexistent dependents, or in the case of Social Security programs, claiming to be a dependent of a covered wage earner. No uniform standards exist for verifying the identity of claimants for benefits; in fact, some states do not require any identification.

In a recent case of welfare fraud in Denver, a woman was accused of using four different names to collect almost \$50,000 in welfare money and food stamps over a four-year period. According to Orlando Romero, Director of the Denver Department of Social Services, it is difficult to know if fraud on this large a scale is happening more often than the Department is able to detect with present procedures and limited personnel. Romero admits, "I'm scared to death this is happening in other cases."^[46]

Misappropriation of benefits by imposters, usually with stolen welfare or Social Security checks or stolen food stamps, is another way in which fraud is committed with the aid of a false ID. The studies in New York City and Philadelphia, mentioned previously, revealed that 30% to 40% of all welfare checks reported "lost or

stolen" were subsequently cashed by forgers. The annual loss in both cities from this kind of fraud reaches multimillion dollar proportions.

Welfare Fraud

Our surveys have shown that, due to the lack of identification standards for welfare recipients, neither Federal nor state agencies have a very good idea who is receiving almost \$37 billion per year in public assistance and Social Security payments. (See Appendix A1.) We have, therefore, no way to accurately estimate the scope of multiple collection of benefits by individuals using several identities. In fact, several welfare officials have admitted that there is no organized procedure for detecting such fraud; however, we have noted that institution of a photo ID program for welfare recipients in New York City in 1973 resulted in the closing of about 3,000 cases of ineligibility.^[47] These closings produced a saving of \$7.2 million per year, which represented about 0.6% of all New York City assistance payments for FY 1974. It seems likely that a large portion of these cases represented multiple payments, since the only major change in procedure was the issuance of a photo ID to recipients.

Although many attempts at false identification fraud may have been discouraged by the photo ID program, the problem has not been eliminated. For example, after the Queens County (New York City) District Attorney found several cases of multiple applications for benefits under false names in a single welfare center, he declared in early 1975 that this type of fraud is "...the most serious problem faced in the administration of Public Assistance and one for which there are no present adequate safeguards...".^[48]

Cashing stolen or forged welfare checks is a major problem for which the FACFI has also received data from the Philadelphia and New York City studies. Before a determined effort was made in 1974 to reduce mailing of welfare checks, an average of 10,000 replacements for checks reported lost or stolen were issued each month in Philadelphia alone.^[49] About 41% of the checks reported lost or stolen were subsequently forged, resulting in an annual loss of approximately \$4.8 million. This figure represents about 16% of the total public welfare budget in Philadelphia for the year 1972.^[50]

In New York City, over 30% of checks for which replacements were issued were subsequently cashed fraudulently.^[51] The total value of checks replaced in the year ending October 1973 was \$28 million; therefore, losses through fraud amounted to at least \$8.4 million for the year, which represents approximately 0.7% of total welfare payments in New York City for FY 1974. The acceptor of a forged check, rather than the issuer, is legally responsible for the loss; in practice, however, the process of recovery for welfare check losses is so slow and uncertain that the taxpayers, in fact, absorb most of the losses.

The food stamp program has expanded from modest beginnings to the point now where it encompasses 19.1 million recipients and a payment level of \$5.2 billion per year. This program as presently structured provides a disincentive to investigation and prosecution of fraud in that such costs must be covered by the participating state, while all funds recovered must be returned to the Federal government. Not surprisingly, then, our data on false identification fraud in the food stamp program has been sparse. However, where local investigations have been pursued, significant evidence of false identification fraud has been uncovered. In North Pulaski

County, Arkansas, which includes only 2.5% of all Arkansas food stamp cases, 57 cases of false identification fraud were recorded in one year.^[52] These cases carried a loss of nearly \$19,000 in Federal funds, or about 2% of all food stamp funds expended in the county.

The sparseness of the data that has been received on false identification fraud in the area of welfare does not permit an accurate assessment of the national impact of this crime; however, the paucity of data does not mean that the problem is insignificant. False identification fraud has been discovered in significant proportions (1% to 2% of the total payments) in every jurisdiction where it has been seriously investigated. Even these percentage estimates may be quite low, since only the least sophisticated methods of false ID fraud were uncovered in the investigations. The only characteristic unique to those localities that have reported a significant incidence of false identification fraud in welfare programs is the existence of an investigation of such fraud. We conclude, therefore, that the primary reason for the lack of data on false identification fraud in welfare programs nationwide is that this fraud has been generally unrecognized or ignored.

Periodic audits of federally-sponsored welfare programs by state agencies and the Federal government are required by law. These audits are based on actual cases selected at random and in sufficient numbers to be a statistically valid sample of the total caseload. The audits involve a careful review and investigation of the selected cases. One would suppose, therefore, that these audits would be a fertile and valid source of data on the prevalence of all types of welfare fraud, including false ID fraud. Unfortunately, this is not the case; the audit data is virtually useless in determining the

extent of fraud against government. Suspected fraud is not even mentioned in these audits. The objective of the audits according to instructions of the U.S. Department of Health, Education and Welfare (and Department of Agriculture for the food stamp program) is merely to determine "error rates" in the broad categories of ineligibility, overpayment and underpayment. Ineligibility, which means that the audited case should not have received any benefits, could be caused by outright fraud on the part of the recipient or of agency personnel, or simply a procedural error or an innocent mistake. Federal auditors are required to report cases of suspected fraud to state authorities for investigation and possible action; however, the audit reports contain no data on the number of such referrals or any assurance that they are made.

Action to recover public funds from welfare recipients who have committed fraud is the sole responsibility of the state; however, reports of such actions must be made to the Federal government. Those reports show that states which have the highest numbers of ineligible recipients are not necessarily trying to recover the lost funds; in fact, the contrary is true. For example, a recent Federal audit of the food stamp program ^[53] showed that 50% of the cases audited in Massachusetts were ineligible; this was the highest ineligibility rate in the nation. Yet Massachusetts made no claims against food stamp recipients in fiscal years 1973-1975! In contrast, Utah which had one of the nation's lowest food stamp ineligibility rates at 3.1%, took action in 378 cases over the 1973-1975 period to recover over \$103,000 in overpayments from food stamp recipients.

We can only conclude that false identification fraud in welfare programs, like other types of program abuse, is most prevalent where there is the least effort to discover and punish it. We also find

that such laxness is encouraged by the failure of Federal agencies to provide effective ID standards for welfare recipients, and failure to enumerate instances of suspected fraud uncovered in audits of state welfare programs and to take action against states which make no effort to deter such abuse.

Social Security Fraud

Social Security programs are responsible for the issuance of over 100 million benefit checks each year, with a total value of \$13.7 billion in fiscal 1975. These programs include Retirement and Survivors Insurance (RSI), Disability Income (DI), and Supplemental Security Income (SSI), which provide monthly payments to beneficiaries. An additional \$9.2 billion in annual benefits, in the form of reimbursement of medical expenses, is provided under the Health Insurance (HI) program, which includes Medicare. The reported instances of fraud in all these programs has been remarkably low compared to the immense level of payments and number of potential beneficiaries. In 1973, the latest year for which Social Security Administration figures^[54] are available, a total of 3,762 potential fraud cases of all types were detected in both RSI and DI programs. Of these cases, 743 or 20% involved falsification of identity, age, or relationship to a covered wage earner, or illegal multiple entitlement. Since documentary evidence must be presented to establish entitlement to benefits, we would classify these as false identification fraud cases. A majority of the suspected fraud cases were cleared following investigation or by agreement to repay the government for any overpayment.

The very low incidence of fraud detected in RSI and DI programs may be explained by several factors. First, coverage under these programs is established by prior payment into the system; in the

case of RSI, coverage requires at least 10 years of prior payments. Second, firm documentary evidence and an adjudication period are required to establish entitlement. Third, the Social Security Administration's Bureau of Data Processing has advanced capabilities for record search and retrieval that make successful false ID fraud more difficult.

The SSI program was instituted in 1973 to replace state welfare programs for the elderly, blind and disabled. This program does not require prior payment to establish entitlement, and thus might be somewhat more attractive than the RSI or DI programs to persons intent on fraud. However, no data on the incidence of suspected fraud in the SSI program is yet available.

The largest source of fraud loss in Social Security benefit programs appears to result from the forgery of stolen benefit checks. Social Security checks are stolen more frequently than any other type of check issued by the U.S. Treasury.^[55] The probable reason for this fact is that they are regularly mailed to recipients each month. Approximately 47,000 or 65% of the 72,500 forged Treasury checks investigated by the Secret Service during 1975 were Social Security checks. These forgeries of Social Security checks involved a loss to the government of approximately \$10 million.

OTHER CRIMINAL ACTIVITY

The foregoing examples illustrate major categories of crimes where the criminal's success is dependent in large measure on the ease with which he can obtain false identification documents; however, the usefulness of false IDs has not been lost on the common criminal engaging in crimes of a lesser scope.

A citizen is most often victimized by the use of false credentials when a criminal tries to gain access to his home, business, or confidence. In large cities, legitimate servicemen and utility company employees often find it difficult to do their job because of the widespread fear of imposters gaining access to homes and apartments using a false ID. Police departments are particularly concerned about the growing use of false police IDs by criminals. Incidents involving police impersonators in New York City totalled 1,358 in 1974, an increase of 88% over 1973,^[29] while arrests (268) for this crime increased by only 23% over the same period.

Individuals may also be victimized directly by "confidence men." Investigations conducted in 1974 by the Washington, D.C. Metropolitan Police showed that a false ID was a factor in 50% of the 876 fraud complaints handled. The average fraud complaint involved a loss of about \$380.^[43]

SECTION 5

FALSE IDENTIFICATION AND THE LAW

Most identification documents are issued and regulated solely by the states. Federal statutes come into effect only when the criminal applies for a passport or draft card. By this time, the criminal often has built up such a variety of state-issued documents that false identification is hard to detect. Because Federal statutes regulate only those documents issued by the Federal government, and states regulate only documents that they issue, there remains a substantial gap between these jurisdictions, a gap that permits interstate commerce in these documents.

Although the problems inherent in regulating false identification are different at the state and Federal levels, and are discussed separately below, there are some general problem areas that are common to both. At either level, even where statutes are specific and well-written, prosecutors usually place a low priority on prosecution of false ID cases. This is due to a great extent to a lack of awareness of the potential seriousness of the crime; altering a document does not look nearly as serious as a murder or rape case -- until one realizes that the use of false IDs is what keeps many major crimes unsolved and their perpetrators free and "hidden."

In those cases where prosecution does take place, penalties for false statement often only requires revocation of the license, and simple civil fines are imposed in others. Yet in some cases, penalties are sufficient or even excessive. This lack of uniformity in sentencing decreases any deterrent effect that could be possible if more consistent penalties were provided.

On the other hand, many documents that are used for identification purposes and to obtain other documents are not regulated at all. Neither the Federal government nor any of the states investigated in the FACFI survey have laws regulating privately-issued documents. Such private ID cards can be used to purchase firearms or dangerous drugs that are not traceable to the real purchaser.

The FACFI has investigated Federal and state legislation on false identification and evaluated the strengths and weaknesses of both. Using a computer, the legal staff of the Committee, conducted a survey of all applicable Federal statutes and annotations (included as Appendix E3). This survey uncovered about 400 relevant citations and annotations. A manual review of the citations eliminated about half because they dealt with subjects outside the scope of the Committee. Additional manual research using indexes and cross references revealed several other citations that had not been found in the computer run but which were related to the work of the FACFI. Even with both the computer and manual search for relevant statutes, there is no assurance that all the statutes were uncovered; however, it is safe to assume that the research uncovered all major statutes and at least a representative sampling of the rest. We did not attempt to review the Code of Federal Regulations (C.F.R.) or any internal agency regulations.

At the state level, the staff took a sampling of five states selected from different geographical regions with different densities of population. New York, California, Illinois, Mississippi, and Nebraska were chosen to assist us in determining the range and effectiveness of state laws on false identification. In addition, we examined legislation recently passed in Nevada and North Carolina that deals comprehensively with the possession and use of false IDs.

At the local level, some counties and cities have ordinances dealing with various facets of the problem; however, these ordinances vary to such a degree that a general survey would not be practical at this time. In areas where both local ordinances and state statutes exist, the state statutes generally take precedence. In other areas, it is doubtful that local statutes could fill the gaps in state legislation.

FEDERAL LEGISLATION

The Federal government does not collect and maintain the kind of information that is necessary to verify a person's identity from birth. Only the states have that information. The government is, therefore, totally dependent on state documents and information over which it has no control in any verification process for federally-issued documents. When Federal statutes do regulate specific documents such as the Social Security card, loopholes render the statutes ineffective. The difficulty of establishing effective legislation at the Federal level can be categorized into four general areas:

- Federal dependence on state identification documents and information.
- Problems with the statutes themselves.
- Jurisdictional gaps between Federal and state statutes.
- Enforcement and prosecution problems.

These problems are interrelated; a solution in one area will not be totally effective without corresponding improvements in all areas.

Federal Dependence on State Identification Documents and Information

Most documents that are commonly used for identification are issued by the state (except for such documents as the passport, draft card, Social Security card, and alien registration card). If a criminal wants to establish a false identity he starts with state-issued documents (birth certificate, driver's license, etc.) and moves on to obtain federally-issued documents only if they are necessary. (Usually the Social Security card is the only federally-issued document needed to establish an identity, unless it is necessary to leave the country.) These state documents are relatively easy to obtain in a false name and are beyond the reach of Federal regulations, which makes enforcement of Federal laws difficult. Many times when a criminal first applies for a Federal document other than the Social Security number, he has more proof of his false identity than the average citizen has of his true identity. Even if the Federal government were to put stringent identity verification standards into effect for all Federal documents, this verification must eventually be based on a state document or state information over which the Federal government has no control.

Weaknesses in the Federal Statutes

Generally, Federal statutes that regulate the fraudulent obtaining, producing, transferring, or using of specific federally-issued documents are comprehensive and potentially effective. However, if the possession of these documents were also included as a crime, the statutes would, by impacting on the criminal at an earlier stage of his establishing a false identity, be strengthened.

There are no laws at all in the one area where the Federal government has jurisdiction and control over a document of fundamental importance in establishing a false identity. There are no penalties for the false application for or use or counterfeiting of the Social Security card or number, except in an application for Social Security benefits. The Social Security card is the only Federal document that is issued early in an individual's life that is required in the application phase for many state identification documents. Currently, though application procedures have been tightened somewhat, there are no effective safeguards or penalties in this area.

Coordination Between State and Federal Statutes

Current Federal legislation deals with the subject of false IDs only as it applies directly to Federal documents. The law forbids the counterfeit reproduction of government documents, seals, official signatures; impersonation of Federal employees, officers, or other officials or agents of the government; and making false statements on any application form or making other false use of any federally-issued document. State legislation covers about the same areas except their laws only cover documents issued at the state level.

There are no Federal laws dealing with interstate commerce in false identification documents, the use of the mails to transfer these documents, the counterfeit reproduction of the official documents of one state in another state, or out-of-state application by mail for another person's birth certificate for fraudulent purposes. Such lack of regulation allows the criminal use of false IDs to prosper and the suppliers of such IDs to go unpunished.

Problems of Enforcement and Prosecution

Federal laws on false identification as written are difficult to enforce, and unenforced laws are virtually useless. Because in most cases the possession of a fraudulent identification document is not a crime, there must be evidence of a false application or fraudulent use before a successful prosecution is possible. Often a false identification charge is dropped in favor of prosecution of the substantive crime involving the fraudulent use, such as bank robbery. As we stated previously, the main problem with enforcement is not only with the laws themselves, but also with the priorities prosecutors assign. There is a lack of awareness by investigators and prosecutors of the seriousness of the false ID problem.

STATE LEGISLATION

The primary thrust of state legislation is prohibitive not preventive. Criminal penalties are invoked upon fraudulent use of a false ID not the mere possession of fraudulent identification documents. Laws are totally inoperative until the criminal, in his new identity, commits a crime. By this time it is often too late. The criminal has assumed another identity and disappeared.

In most states there is no comprehensive law against establishing a fraudulent identity.

Laws that regulate specific documents, such as the birth certificate, are not comprehensive enough to allow effective enforcement. They do not, for example, make reference to all of the following:

- Illegal manufacture
- Sale
- Possession
- Alteration
- Transferring
- Transporting
- Advertising for sale
- Obtaining
- Receiving
- Use or display
- Use after expiration, suspension, or revocation
- False or misleading statements or use of false documents in an application for such documents.

Without this degree of comprehensiveness, criminals can use and supply others with false IDs without fear of prosecution.

State legislation on false ID use falls into three general areas, legislation dealing with:

- Specific documents,
- False personation, or
- Commercial fraud.

Each of these areas has different loopholes and different strengths.

Specific Documents

The most fundamental ID is the birth certificate. Possession of this document is the starting point for building a new identity. Most states have some laws regulating access to and fraudulent use of birth certificates and certified copies of them; however, these laws are full of loopholes. Though it is illegal in many states to fraudulently alter or use a birth certificate in another person's name, it is not illegal in any of the five states surveyed to possess an altered, forged or counterfeit birth certificate or to apply for a genuine birth certificate in another person's name.

Although the laws regulating the application for and use of the driver's license as an identification document are generally adequate in all five survey states, verification of the applicant's identity at the time of application is either inadequate or nonexistent.

Other state-issued identification documents include: fishing and gaming licenses, professional licenses, identification cards for state employees and charitable fund raisers, and in some states welfare recipient or food stamp identification cards. Statutes relating to their use vary considerably in form and content, but none are totally effective. In fact, the regulations for these documents are generally limited to preventing fraudulent use for the purpose for which they were issued. Furthermore, many of these statutes only require revocation of the license for false statements on the application form. Other penalties are usually misdemeanors.

False Personation

In some states there are no laws making it illegal to impersonate a private citizen, even for fraudulent purposes. In other states it is illegal to impersonate private citizens with the intent to defraud that person or a third party. This still does not eliminate the use of false personation for other purposes such as to elude law enforcement officers, to enter the country illegally, or to apply for another ID.

All of the states surveyed have statutes that make it illegal to impersonate certain public officials and professional people in their public or professional capacity. This protection does not carry over into their private lives. Policemen, firemen, and other public officials, attorneys, doctors, and architects are all protected from impersonation in their public or professional capacity only.

Commercial Fraud

There are two types of statutes in this category that are or could be related to the use or possession of false identification. These are:

- The counterfeiting-forgery statutes, which are primarily designed to prevent a person from making or altering instruments which transfer money, property or some other right or obligation. They have not been specifically directed at the fraudulent making or altering of identification documents.

- Deceptive practices or fraud statutes, which are concerned with the fraudulent use of credit cards and checks. Although these statutes may be effective in these limited areas, there is a definite need for credit card and check issuers and receivers to make more extensive identity verification prior to issuing or accepting a card or check. These statutes also neglect to penalize the use of false identification or financial documents in applications.

Preventive Legislation in Nevada and North Carolina

On March 26, 1975, Nevada enacted legislation* that outlawed the possession, sale, or transfer of any document "for the purpose of establishing a false status, occupation, membership, license or identity for himself or any other person." The penalties for the sale or transfer of such documents are felonies, while possession is a misdemeanor.

On the same date Nevada passed strict laws preventing the obtaining, possession or fraudulent use of another person's birth certificate. Possession without lawful authority is a misdemeanor. Use of a birth certificate in the commission of a felony is a separate felony. Unlawful possession is a separate offense from unlawful use of a birth certificate.

North Carolina has recently enacted legislation that deals only with fraudulent use or application for birth certificates. It does contain a provision that Nevada's law does not -- forbidding the use of birth certificates obtained in other states from being used fraudulently in the State of North Carolina.

* Appendix A, p. 159.

LEGAL CHANGE OF IDENTITY

Many states recognize the common law right of any person to change his name without formal legal proceedings. The tradition is an old and venerable one. As early as 1811 a Massachusetts Court said:

As to the fact of this parish having used several names in its public proceedings, we know not why corporations may not be known by several names, as well as individuals. [56]

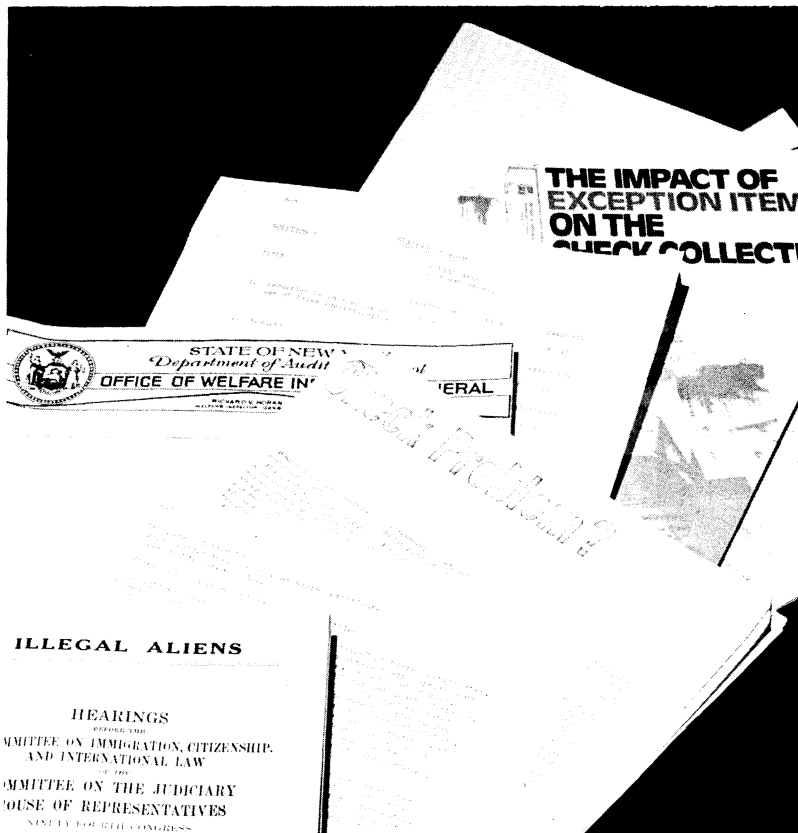
A joint decision of the Attorney General and the Secretary of State of Massachusetts dated December 5, 1975, is even more explicit:

It has always been the law of this Commonwealth that any individual, male or female, has the right to choose and from time to time change his or her name. This right is not contained in any statute or other codified form. Rather it is a common law right which the courts have consistently recognized so long as he or she has no intent to defraud anyone by the use of such name. Although it is common practice for a person wishing to change his or her name to present a Petition for Change of Name to a court and obtain a court order changing his or her name, such a court order is not required by law. A person may change his or her name simply by using another name. (emphasis added) [57]

Some jurisdictions, however, while permitting the use of a new name, do not give that name legal effect until the proper forms are filed in a court of law. This implies that in some jurisdictions other than Massachusetts which recognize the right of a person to change his name, there still may be grounds for refusing him or her state-issued documents in the new name without a court order. Other

states, including California, provide a form by which a person can inform the state of intent to change his name. By filling out this form (under penalty of perjury for a false statement), the individual can obtain a new name on any official state document.

PART II



A VIEW TOWARD SOLUTION

SECTION 6

APPROACH TO FINDING SOLUTIONS

In adopting a formal procedure for evaluating and publicly reviewing proposed solutions to false identification problems, we considered three major criteria:

- 1) The national problem of false identification demands a set of imaginative solutions that can be applied cooperatively and comprehensively at local, state and Federal levels and in the commercial and private sectors.
- 2) Personal identification is a sensitive area in which restrictions and regulations should be proposed with great care, and should increase, not decrease, personal privacy.
- 3) Any set of proposals having an impact on the general public should be subjected to public examination and comment at all stages of their formulation.

Ideas for potential solutions were obtained principally from suggestions contained in Task Force reports prepared by the Committee's five Task Forces. These suggestions were supplemented with proposals described in testimony before Congress, and with suggestions made by individual FACFI members, staff representatives, and public observers. The FACFI staff then identified and considered approximately 150 such suggestions. After consolidation of related suggestions and the elimination of those ideas that were clearly ineffective, technically infeasible, or only marginally related to problems of false identification, more than 50 preliminary proposals still remained for consideration by

the FACFI membership and public observers. (Preliminary proposals considered by the FACFI, together with evaluations and comments, are further discussed in Appendix B of this report.

In order to provide a uniform basis for discussion of these proposals, we devised standard formats for presentation and evaluation of preliminary solutions. Illustrations of these formats are given in Figure 6 and Figure 7, respectively. The presentation of each proposal included a title, the major problem areas affected by the proposed solution, necessary background information, a description of how the solution would work and a rough indication of cost and impact on the public. Also included in the solution presentation were sample arguments that could be raised in favor of the proposal and against it, the measures that would be required to implement the proposal, and possible legal questions raised by the proposal. The standard evaluation format listed a set of evaluation criteria and called for comments and suggested revisions.

Respondents were asked to rate each proposed solution on its effectiveness in reducing the use of false identification and also in combating the illegal activity in which false IDs are used. For example, a respondent could decide that a certain proposal might be quite effective in reducing the use of false ID by illegal aliens but would have little effect on the general problem of illegal immigration. This evaluation might ultimately result in the respondent's decision that the proposal should not be recommended. Other criteria against which all proposals were rated included the potential impact on the structure and procedures of public and private organizations affected by the proposal, and the effect on public and private convenience and privacy. They also evaluated the cost effectiveness of each proposal.

Proposed Solution No. 1
Major Problem Area: Misuse of Birth Certificate
Minor Problem Areas: None

Title: Limit access to vital statistics files

Description: Certain states maintain "open files" of birth certificates, in which unauthorized individuals are able to obtain birth certificates of any person they choose. This is not only an invasion of privacy, but also gives rise to an offense known as "IDI" (infant death identity), in which the birth certificate of a dead infant is obtained and later used to apply for driver's licenses and other documents in the assumed false identity, with or without alteration of certain vital information. The IDI method has been a problem in Florida where over a hundred cases of this offense have been documented. Florida recently closed all its files to persons other than those having a specific need to obtain their birth certificate (or someone else's, for a legitimate purpose). This appears to have cut down the problem of IDI.

At this time, over 40 states restrict access to their vital statistics files, prohibiting browsing through files except by authorized officials who are seeking a specific birth certificate for a requestor. The suggestion is that the few remaining states be requested to adopt similar restrictions in the interest of citizen privacy and crime prevention.

Arguments For:

1. Limits the possibility of IDI.
2. Conforms to the Model Vital Statistics Act. Section 26A of the Model State Vital Statistics Act states, "It shall be unlawful for any person to permit inspection of, or to disclose information contained in vital statistics records, or to copy or issue a copy of all or part of any such record except as authorized by regulation."
3. Cost is low.
4. Impact on public and current procedures is low.

Arguments Against:

1. Mail applications are not addressed specifically by this solution.
2. Information required for perpetration of IDI can still be obtained from old newspaper records.

Action Required: State pass regulations conforming to the Model Vital Statistics Act, such as Florida has done.

Legal Questions: None, since Model Vital Statistics Act is accepted as the guideline for such state legislation.

Figure 6. Example of Presentation of a Preliminary Proposal

EVALUATION FORM

SOLUTION #	PRIMARY AREA:										
	SECONDARY AREAS:										
TITLE:											
	INEFFECTIVE			FAIR				EFFECTIVE			
1. Reduction in incidences of use of false identification	0	1	2	3	4	5	6	7	8	9	10
	INEFFECTIVE			FAIR				EFFECTIVE			
2. Reduction in (specific to problem area)	0	1	2	3	4	5	6	7	8	9	10
	POOR			MODERATE				EXCELLENT			
3. Increased ability to detect use of false identification	0	1	2	3	4	5	6	7	8	9	10
	POOR			MODERATE				EXCELLENT			
4. Increased ability to (specific to problem area)	0	1	2	3	4	5	6	7	8	9	10
	UNDERSIRABLE			NEUTRAL				DESIRABLE			
5. Impact on structure of agencies and organizations	0	1	2	3	4	5	6	7	8	9	10
	HINDRANCE			NEUTRAL				HELP			
6. Effect on normal procedures of these organizations	0	1	2	3	4	5	6	7	8	9	10
	ANNOYING			NEUTRAL				DESIRABLE			
7. Effect on Public Convenience	0	1	2	3	4	5	6	7	8	9	10
	INVASION			NEUTRAL				ENHANCEMENT			
8. Effect on Public Privacy/Rights	0	1	2	3	4	5	6	7	8	9	10
	LOW			MODERATE				HIGH			
9. Cost Effectiveness	0	1	2	3	4	5	6	7	8	9	10
	POOR			FAIR				EXCELLENT			
0. Overall Evaluation of Solution	0	1	2	3	4	5	6	7	8	9	10
<u>Comments:</u>											

Figure 7. Format For Evaluation of Preliminary Proposal

Respondents rated the attributes of each solution with respect to each criterion on a zero-to-ten scale. For example, the zero end of the scale for the "public privacy" rating represented a serious invasion of privacy, while a "10" indicated a significant improvement of privacy protection over the present situation; a "5" rating in this case indicated no impact on privacy in either direction. In addition to these numerical ratings, the Committee asked respondents to give an overall evaluation of each proposal, indicating their individual decision on whether the proposal should be "recommended", "revised" in accordance with comments, or "rejected" as an unacceptable

Proposed solutions included a broad range of suggestions involving legislative, technical, and procedural changes. Also included in every problem area was the option not to recommend any official action, on the grounds that the problem does not justify additional action or that actions being taken independent of FACFI will deal adequately with the problem.

The FACFI distributed all proposals for solutions at their monthly public meetings, which were announced in advanced in the Federal Register and by mail to FACFI members, representatives of the press, and privacy advocates. We solicited additional suggestions for solutions at all public meetings; a number of proposals were received as a result of these solicitations and were drawn up and evaluated in the same manner as the original set of proposals.

The recommendations of the FACFI grew from these individual evaluations of the proposed solutions. The evaluations were given no official status, but we used them to compile comments, suggestions for modification, and to identify strong and weak points of each

proposal. The formal evaluation procedure also permitted the identification of proposals that were generally favored, universally disliked, highly controversial, or seriously in need of modification.

Actions on proposed solutions were taken only at the public meetings of the FACFI. Proposals that appeared to have a special impact on government payments, commercial transactions, fugitives, Federal government documents, or state and local government documents were referred to the appropriate Task Force for a recommendation to the Plenary Session. Action on each proposal was then taken in the Plenary Session by consensus of everyone present (including visitors). The FACFI leadership preferred consensus actions to voting by organizations represented on the Committee. We considered that the public and governmental consensus required to implement FACFI recommendations would be difficult to obtain if consensus could not be reached within the FACFI itself.

The Committee ultimately approved or rejected all proposals for solution of false identification problems (some solutions were retained for a time to permit further study by Task Forces or staff). The approved solutions were included in draft recommendations that we released through the Federal Register^[58] for public distribution and comment prior to final approval by the Committee. The decision to reject a given proposal did not necessarily imply FACFI disapproval of the suggested solution. In many cases, the decision to reject a proposal simply reflected a belief that a FACFI recommendation was inappropriate because the relation of the proposal to false ID problems was too tenuous. In other cases, it was determined that a potential solution was already being implemented on a sufficient enough scale that a FACFI recommendation would be superfluous.

SECTION 7

RECOMMENDATIONS APPLIED TO MAJOR PROBLEM AREAS

In our summary of the scope of the national problem of false identification, we identified several areas in which the use of false IDs has significant impact. These major problem areas include drug smuggling, illegal immigration, fugitives from justice, fraud against business, and fraud against government. In many cases, false ID use in such crimes begins with the abuse of a birth certificate, then a state driver's license, which are then used as "breeder" documents to obtain other IDs. In this section we present the recommendations of the FACFI with respect to Federal and state legislation, the issuance of birth certificates and driver's licenses, as well as recommendations with respect to each of the major problem areas. At the end of each recommendation, when applicable, we have given the designated number of the committee's preliminary proposal in that area (see Figure 6 and Appendix B).

Before these recommendations are considered, however, we wish to capsule our thinking on a broader, more all-encompassing solution -- adoption of a national identification document. We discuss the concept of a national ID in order to present the reasons why such a document (or system) is not recommended by the FACFI as a solution to false identification problems.

REJECTION OF A NATIONAL IDENTIFICATION DOCUMENT

The concept of a uniform personal identification document, to be issued and secured by Federal or state government, has occasionally

been proposed as a sweeping solution to the problems of false identification. National IDs are in fact used by a number of nations with democratic traditions as well as those under other forms of government. (See "A Survey of Foreign National Systems for Personal Identification," Appendix C4.) The FACFI considered it necessary and advisable to study the national ID concept as carefully and rationally as possible in order to illuminate the advantages and problems inherent in such an approach.

Three different approaches to a system of uniform personal identification were described in preliminary proposals submitted for evaluation by FACFI members. (Listed in Appendix B as Preliminary Proposals 54, 3, and 11.) One such approach proposed a federally-issued document designed specifically for personal identification within the U.S. This document would be available to citizens on a voluntary basis and would incorporate application procedures and security features similar to those used in the U.S. passport. The second suggestion envisioned a complete national identification system in which citizens would be registered at birth. This proposal included an automated verification system -- a data base containing only identity information -- that could be accessed only by the registered individual to verify his identity to government agencies. The third proposal suggested the use of present state driver's licenses (and "non-driver" state IDs) as recognized and required personal identification. Application for such a document would be required of all citizens at age 16. Safeguards against counterfeiting, alteration, and use by imposters would have to be included in all such state documents.

Arguments can be brought to bear in favor of and against all these proposals. Arguments in favor of a single standardized type of ID include beliefs that:

- Such a document could be more easily recognized, controlled and protected against abuse.
- Document systems that include everybody would thereby be "foolproof".
- Government has an obligation to provide a reliable means of personal identification for public and private transactions among its citizens.

Arguments against a standardized national ID included beliefs that such documentation is in opposition to American tradition and would represent an invasion of personal privacy, and that data required for citizen identification could be abused by government or private interests.

It is certain that any new system designed to verify and store identity information on over 200 million people would be extremely expensive and require a major national effort. It is highly probable that proposals for such a system would be opposed politically. If such a system were implemented despite these difficulties, it would be subject to defeat by imposters or counterfeiters taking advantage of careless inspection of documents or through corruption of officials. Occasional errors would also occur in such a system that could adversely affect innocent people. Organized crime would take advantage of any national ID system because of the presumption of validity surrounding such a large system. Criminals could reap benefits far greater than they obtain under the current multi-faceted system of identification.

The FACFI therefore strongly opposes any new type of state, or local government-issued ID intended to supersede existing documents. In short, FACFI opposes any so called "National ID card."

The FACFI instead recommends that the security of existing state document systems be increased, particularly for breeder documents such as the birth certificate and the driver's license. Security must be increased both in the application phase (during which documents are issued) and in the use phase (when the documents are used).

Thus, the goals of FACFI's recommended Federal actions are to insure the increased security and privacy of existing state identification documents in state, interstate, and Federal transactions, and to insure swift prosecution of criminals who obtain and use false IDs. The following recommendations are designed to accomplish these goals.

RIGHT TO PRIVACY

The FACFI finds that the criminal use of false identification often invades personal privacy; that innocent citizens are victimized when their good names and credit are used in criminal transactions; and that the protection of personal privacy is an essential right, fully consistent with sound law enforcement efforts to reduce false identification crimes.

The FACFI therefore recommends that individual privacy rights be given the fullest consideration in the formulation and implementation of the following legislative and administrative proposals to counter the criminal use of false identification.

FEDERAL LEGISLATION

The FACFI finds that although there are approximately 350 Federal statutes relating to false identification, false application and related subjects (see Appendix E3), Federal laws are ineffective in deterring false identification crimes because:

- Most identification documents are issued and regulated solely by the states; Federal statutes only come into play when the criminal applies for a federally-issued document such as a passport.
- The Federal government does not collect and maintain information to verify a person's identity; only the states have that information.
- There are loopholes in some of the Federal statutes regulating specific documents such as the Social Security card.
- Even where Federal statutes are specific and well drafted, enforcement and prosecution are often given low priority.
- In some cases, penalties for false statements on applications are sufficient. Other statutes require only revocation of licenses.

The FACFI therefore recommends that:

- a. S. 2131 (see Section 10) Introduced in the 94th Congress be enacted. S.2131 would close most existing loopholes in Federal legislation dealing with false identification.

- b. Federal false identification statutes be enforced with renewed vigor by prosecutors, and that judges be made aware of the importance of false identification crimes so that sentences may more accurately reflect the seriousness of these crimes.

STATE LEGISLATION

The FACFI finds that the primary thrust of state statutes dealing with false identification is prohibitive, not preventive, and are ineffective because:

- In most states there is no comprehensive law against establishing a fraudulent identity.
- State laws governing the issuance of certified copies of birth certificates and access to such records do not adequately protect the public's right to privacy because certified copies are freely (though unknowingly) handed to criminals.
- The problem is national in scope, yet states are powerless to protect any but their own identification documents.
- The wide variety in document format and authenticating seals encourages the passing of counterfeit documents.
- Laws regulating specific documents, such as the birth certificate, are not comprehensive enough to allow effective enforcement.

- Many documents that can be used for identification purposes or to obtain other documents are not regulated at all.
- In most states, a citizen has the common law right to change his or her name without any formal legal proceedings; in these states it is more difficult for prosecutors to prove fraudulent intent to violate false ID laws.

The FACFI therefore recommends that:

- a. States enact Model State Legislation proposed by the Committee entitled The Identity Protection Act. (See Section 9)
- b. States enact the most recent amendments to the Model State Vital Statistics Act that are designed to protect the integrity of the birth certificate issuing systems. These amendments also upgrade criminal penalties for false identification crimes. (See Section 9 and Appendix C1)
- c. State educational programs be established to facilitate implementation of the Model Identity Protection Act and the Model State Vital Statistics Act and to assist officials in improving methods of document fraud detection.

BIRTH CERTIFICATE

The FACFI finds that certified copies of birth certificates have frequently been abused by imposters and counterfeiters because:

- Unsigned requests by mail for such documents are usually honored.

- The birth certificates of deceased persons are not usually so designated.
- Records of deaths and births in many states are open for "browsing" by persons seeking false identification.
- Minimum standards are not available for issuance security and document security of birth certifications.
- Many vital records offices are autonomous, which results in a wide variety of the formats, seals, and safeguards provided for certifications.
- Information on the abuse of birth certificates is often not given to the proper state authorities.
- Abuse of birth certificates is not sufficiently covered by legislation at either the state or Federal level.

The FACFI therefore recommends that:

- a. Fraudulent application be discouraged by use of state-issued standard application forms requiring the applicant's signature, justification for request, and items of personal history not generally available to imposters. (Solution #58)
- b. A system be implemented for intrastate and interstate matching of birth and death records, such that the fact of death is noted on the birth certificates of

all persons aged 55 years or less at the time of death. (Solution #5)

- c. State laws to protect individual privacy by limiting public access to birth and death records be enacted in all states lacking such legislation. (Solution #1)
- d. Minimum standards for identification of applicants for birth certification, and for security of certified copies against theft, alteration and counterfeiting be drafted for adoption by state legislatures. (Solution #2)
- e. Federal agencies that require personal identification in application for privileges or benefits accept as primary evidence of age and place of birth only those U.S. birth certifications issued by a state or state-controlled records office. (Solution #47)
- f. Formal notification of the abuse of a birth certification be given by state and Federal law enforcement agencies to the appropriate state registry officials. The information exchange might be facilitated through the establishment of a national clearinghouse for false ID information. (Solution #10)
- g. Wherever practical, requests for birth certificates be retained by the issuing office to assist in the detection and tracing of fraudulent requests. (Solution #7)
- h. Appropriate state and Federal legislation be enacted to prohibit the possession, sale, and transfer of

birth certifications for the purpose of establishing a false identification. (Solution #4)

DRIVER'S LICENSE

The FACFI finds that state driver's licenses (and "non-driver" state ID or "age-of-majority" cards) are frequently abused by counterfeiting, imposture, or fraudulent application because:

- They are used as personal ID for commercial transactions and dealings with government agencies although this use was not intended by issuing authorities.
- The security of issuance procedures and of the document itself varies widely among the states.
- State documents are not sufficiently protected by Federal legislation against interstate abuse.

The FACFI therefore recommends that:

- a. The state-issued driver's license (or state-issued ID) be recognized under law as the primary form of personal ID for use in commerce and in general transactions between individuals and government. (Solution #11 Revised)
- b. Guidelines be drafted by the Federal government providing minimum standards for identification of applicants for original, replacement, or interstate exchange of state IDs, and for security of state IDs

against counterfeiting, alteration, and use by imposters. (Solution #11 Revised)

- c. Voluntary compliance by all states with these guidelines be encouraged by appropriate awards and/or sanctions. (Solution #11 Revised)
- d. An analysis and implementation plan for improvement in the security of state ID systems (see Appendices D1 through D3) be developed by the Law Enforcement Assistance Administration (LEAA) for consideration by the states. (Solution #12)
- e. Federal legislation be enacted to prohibit counterfeiting in any state of personal IDs issued by any other state, and to prohibit use of the mails to assist fraudulent application for state IDs. (Solution #4)
- f. Federal legislation be enacted to allow all states to use the Social Security number on their driver's licenses in other records.

DRUG SMUGGLING

The FACFI finds that smuggling of narcotics and other dangerous drugs by criminal organizations is aided materially by extensive use of false U.S. and foreign passports and other false documents.

The FACFI therefore recommends that:

- a. Birth certificates and state-issued IDs, as the primary documents used in U.S. passport application procedures, be secured in accordance with FACFI recommendations.

b. Federal agencies concerned with the activities of drug smugglers (including the Immigration and Naturalization Service, Drug Enforcement Administration, Customs Service, Passport Office, and Visa Office) provide coordinated training programs for the detection of false IDs used by smugglers and communicate frequently with each other and state and local authorities on the observed patterns of such false ID use.

(Solution #49)

c. Interpol be encouraged to coordinate international law enforcement efforts in the detection of passport and other document fraud.

ILLEGAL IMMIGRATION

The FACFI finds that illegal aliens frequently use false IDs such as stolen or counterfeit immigration documents and border crossing cards, and U.S. birth certificates and voter registration cards obtained under false pretenses to enter and remain in the United States. By obtaining Social Security accounts, they are able to secure employment to which they are not entitled, made easier because knowing employment of illegal aliens is not prohibited under Federal law.

The FACFI therefore recommends that:

a. The Immigration and Naturalization Service (INS) be provided with sufficient funds to develop and implement an improved system for registration of legal aliens that will resist attempts at forgery, counterfeiting, and use of INS documents by imposters.

(Solution #20)

- b. Birth certificates and secondary evidence of U.S. citizenship be secured in accordance with the foregoing FACFI recommendations.
- c. Identification and citizenship of applicants for new Social Security accounts be verified by stricter evidentiary requirements or other appropriate means. (Solution #43)
- d. Federal legislation be enacted to counteract knowing employment of illegal aliens. (Solution #17)

FUGITIVES FROM JUSTICE

The FACFI finds that dangerous fugitives are able to avoid apprehension through the use of false identification, and that, when arrested, they may be released before their identity and criminal history is confirmed.

The FACFI therefore recommends that:

- a. State and Federal document systems be protected from abuse by fugitives through enactment of FACFI recommendations for birth certificates and driver's licenses.
- b. Laws be enacted requiring verification of the identity of all persons arrested, prior to their release on bond. (Solution #22)
- c. To meet such identification requirements without endangering arrestees' rights, appropriate equipment

be used for high-speed transmission of fingerprints and other identifying data between local law enforcement offices and state identification bureaus. (Solution #22)

FRAUD AGAINST BUSINESS

The FACFI finds that American business is subjected to billion-dollar losses each year from false identification fraud through forgery and counterfeiting of personal and corporate checks, impersonation based on false or stolen credit cards, and negotiation of lost or stolen securities.

The FACFI therefore recommends that:

- a. The business community incorporate into its operations measures to prevent false identification crimes; preserve evidence of such crimes; prosecute those who commit them; train employees in preventative measures; and assist the public in understanding the need for these measures.
- b. The business community make use of improved technological safeguards against false ID fraud. (The general characteristics of some of these safeguards are described in the FACFI Staff Paper, "Automated Identification Technology," Appendix C2.) (Solution #24)
- c. The business community participate in the increasing development and use of electronic funds transfer systems, which have the potential of reducing false ID fraud by reducing the amount of negotiable paper in circulation. The potential for privacy abuses and significant false ID fraud via electronic manipulation must be addressed in the design of such systems. (These systems and their relationship to false ID fraud are described in the FACFI Staff Paper, "Electronic Funds Transfer Systems (EETS) - An overview," Appendix C1.) (Solution #27)

- d. The security of driver's licenses and other state IDs, which are widely used in commercial transactions, be improved through implementation of FACFI recommendations.

FRAUD AGAINST GOVERNMENT

The FACFI finds that government programs such as public assistance, food stamps, and Social Security are subjected to large annual losses through false identification fraud, and that such fraud results principally from the use of false IDs at application for benefits, in welfare ID cards, and in the cashing of stolen benefit and payroll checks.

The FACFI therefore recommends that:

- a. The Federal government draft stricter uniform standards for the identification of applicants for federally-supported or cost-shared public assistance programs.
(See Section 9 for this and following recommendations;
Solution #36)
- b. Mailing of welfare and payroll checks to individuals be superseded by mailing or direct deposit to banks and thrift institutions, to the extent that such depositing is beneficial and practical.
(Solution #25)
- c. The identity of applicants for new Social Security accounts be verified by stricter evidentiary requirements or other appropriate means. (Solution #43) And that the Social Security card be made resistant to counterfeiting, alteration and forgery.
- d. Cooperative Federal programs be instituted for the training of welfare and Social Security employees in

techniques for detection and reporting of the use of false identification. (Solution #49)

- e. The security of birth certificates and driver's licenses, which are frequently used in application for government payments, be improved through implementation of FACFI recommendations.

OTHER RECOMMENDATIONS

The FACFI finds that because false identification crimes are often not detected until long after the crime has been committed, many government agencies and commercial establishments are being defrauded without their even being aware of the fact.

The FACFI therefore recommends that Federal, state and local agencies and the commercial sector develop increased awareness of the nature of false identification crimes, compile statistics on those crimes that are committed within their organizations, and affirmatively seek methods of preventing the commission of such crimes both in the application state, when fraudulent applications are made, and in the use stage, when false documents are used.

The FACFI finds that there is an almost total lack of meaningful statistics concerning false identification crimes; there is great reluctance by organizations to reveal these crimes even when they are discovered; and that such failure to expose the criminal use of false identification has contributed to the proliferation and success of this criminal technique.

The FACFI therefore recommends that Federal, state and local law enforcement agencies together with commercial firms establish a statistical base line by which to measure the increase or decrease in false identification crimes and that other data on false identification be compiled, including the type of crime, modus operandi, and a profile of the user and the victim. The FACFI also recommends that the FBI gather statistics relating to false identification crimes and publish them in Uniform Crime Reports. Such statistical base lines can then be used to measure the effectiveness of the countermeasures recommended by the FACFI as they are being implemented.

The FACFI finds that a study of the means by which Federal, state and local agencies obtain and use undercover documents for law enforcement and intelligence purposes is outside of the charter of the Committee and thus has not been explored; the Committee notes, however, that some have questioned the adequacy of controls on obtaining and using such documents.

The FACFI therefore recommends that: (1) government agencies should not obtain or provide "alias identification" in violation of any local, state, or Federal laws; and (2) recommends that agencies review their laws, regulations and procedures for obtaining such credentials to insure that they are lawfully obtained and that their use is adequately controlled.

The FACFI finds it essential to obtain increased public recognition of the scope and impact of crime committed with the aid of false IDs and to solicit informed support of measures designed to reduce the use of false IDs in the United states.

The FACFI therefore recommends that the Department of Justice and all other concerned organizations encourage public support for the measures recommended by the FACFI. (Solution #46)

SECTION 8

DISCUSSION OF RECOMMENDATIONS

The recommendations outlined by the Committee provide a comprehensive and coordinated program for action by Federal and state government and by business and the general public to combat the criminal use of false identification. We believe this set of recommendations is the minimum response that will be effective in improving the security and privacy of personal identification documents, which at present are abused by criminals with great profit, little difficulty, and minimal risk. Effective legislation at both the state and Federal level can maintain and upgrade the integrity of state identification documents, close loopholes in existing Federal legislation, and insure swift prosecution of false ID crimes.

Birth records that originate in state and local offices serve as legal proof of U.S. citizenship and should be protected from criminal misuse. FACFI recommendations would provide greatly increased security for these important documents and provide assurance to the honest citizen that his or her identity cannot be usurped easily by a criminal. The recommendation for a standard application form, requesting information probably not known to an imposter, has its precedents in the actions of several states.

Under FACFI recommendations, "over-the-counter" service for birth certification would still be retained where such service is presently

available; however, we recommend that all local issuing offices be made subject to state control with respect to document format, application requirements, and document security. Matching of birth and death records would effectively deny the use of birth certifications of deceased persons to imposters. The recommended limitation of such matching to the records of persons aged 55 or less is intended to reduce the cost of such matching while covering most of the records subject to abuse. Finally, state and Federal legislation is essential to counter the activities of purveyors and users of false IDs who flourish under present conditions and who might otherwise benefit from improved protection for legitimate documents.

We believe that government has an obligation to protect the integrity of government-issued documents used in any legitimate transaction; for this reason, we recommend improved security for state driver's licenses in recognition of their wide use as personal IDs. Lax standards for the identification of license applicants jeopardize even the presently recognized function of the license as evidence of the right to drive. It is perfectly possible for a driver whose privileges have been revoked (e.g., for drunken driving) to apply immediately for a new license under a false name. He need remain sober only long enough to pass the road test.

Most states issue to residents, upon request, documents that are intended solely as personal identification. The side use of such documents in interstate commerce and in applications for Federal benefits and U.S. passports makes their integrity an object of national concern. This concern is the basis of FACFI recommendations for Federal guidelines to protect the security of driver's licenses and other state IDs. Such guidelines will ultimately prove effective only if subscribed to by all states; therefore, we recommend the use of appropriate incentives to insure cooperation by all states. In

addition, Federal legislation is clearly required to prevent the interstate abuse of state IDs.

The recommendations to improve the security of birth certificates and state-issued IDs form an integral part of FACFI recommendations dealing with drug smuggling, illegal immigration, fugitives from justice, fraud against business, and fraud against government. However, we have made additional suggestions in each area to deal with special problems involving false identification. For example, drug smuggling is primarily a well-organized activity carried on by resourceful international conspirators. Therefore, solutions to the use of false IDs by these conspirators should stress cooperative actions on domestic and international levels. Personal interviews by well-trained inspectors have proven effective in detecting passport fraud; we therefore recommend wider use of such training by all government agencies concerned with drug smuggling.

The FACFI endorses current plans of the Immigration and Naturalization Service to improve the security of documents issued to legal aliens. As a means of discouraging illegal entry, we also endorse the concept of Federal legislation against knowing employment of illegal aliens. And, we recommend stricter enforcement of existing Congressional action denying Social Security accounts to illegal aliens.

The special recommendations dealing with fugitives from justice call for legal action and technical improvements to the procedures of state and Federal identification bureaus. The principal requirement for such improvements is the provision of facsimile equipment for the transmission of fingerprints and other information between local law enforcement offices and state identification bureaus. A system of this type has been in use in New York State since 1971

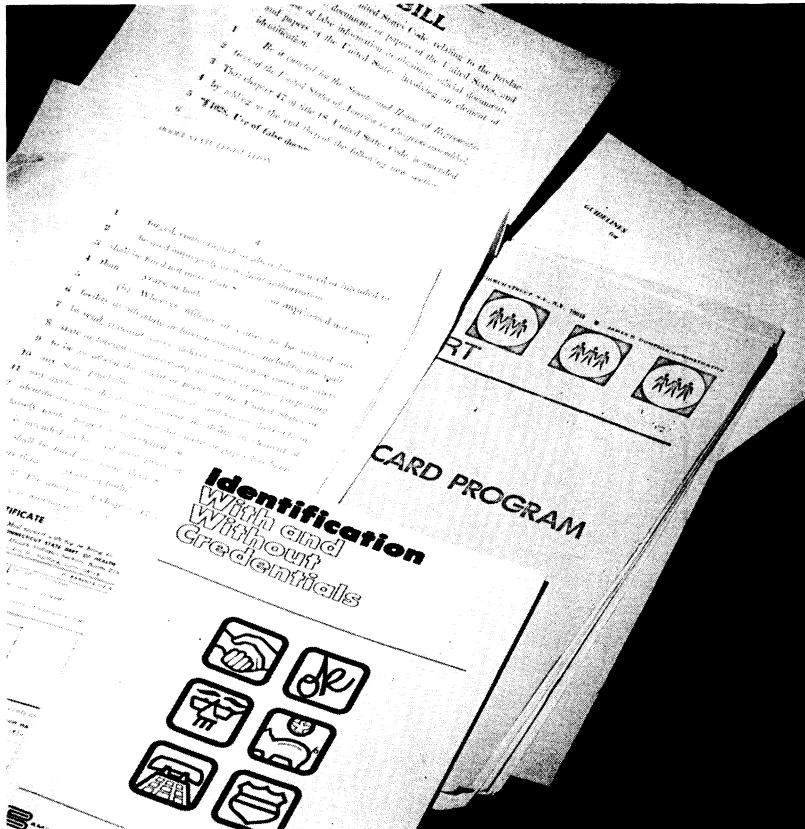
and has decreased the average response time of the state bureau for post-arrest identity checks from several days to three hours or less. By giving judges a firm identity and criminal history of a suspect at arraignment, this system permits careful assessment of the risk to society posed by release of the suspect on bond.

The Committee believes that fraud against business will be reduced by improving the security of state IDs. We endorse wider use of electronic systems that reduce the amount of negotiable paper in circulation and thereby reduce the potential for forgery and counterfeiting of such instruments. At the same time, we point out that such systems are vulnerable to a different type of false identification fraud, involving manipulation of computer files or use of fraudulent credit/debit cards. This threat must be addressed in the design and operation of these systems.

To combat fraud against government, the FACFI recommends that uniform standards be drafted for identification of applicants for public assistance, training of employees in the detection of false IDs, and reduction in the number of government checks mailed to individual addressees.

Finally, we recognize the need for strong public support for these badly needed improvements in personal identification documents. In studying the effects of false identification on our society, we conclude that the present situation is intolerable and justifies a strong and comprehensive effort toward its correction. We are confident that the Congress and the American people, given the same information, will reach the same conclusions.

PART III



A PLAN FOR IMPLEMENTATION

SECTION 9

GUIDELINES FOR STATE ACTION

There are many concrete steps that can be taken by the states, the Federal government and the private sector to implement the FACFI's recommendations. These steps are found in Section 10, Guidelines for Federal Action; and Section 11, Action by the Private Sector.

This Section deals with steps that states can take to deal with the criminal use of false identification. The Committee believes that these steps are feasible and can be implemented with a minimum of disruption to state operations. All of them are designed to safeguard personal records from abuse and improve the reliability of state-issued identification documents.

State actions include:

- Legislation Against False Identification
- Control of Access to Vital Records
- Control of Issuance of Birth Certifications
- Standardized Forms for Birth Certifications
- Matching of Birth and Death Certificates
- Improvements to State Driver Licensing Systems

Detailed proposals for implementing FACFI recommendations dealing with the issuance and protection of birth certifications and driver's licenses appear as special studies in Appendix D of this report.

STATE LEGISLATION AGAINST FALSE IDENTIFICATION

(Implements FACFI Proposed Solution No. 4)

The Committee proposes that the states enact legislation that will protect the public health and welfare and the right of privacy and security for one's own identity by penalizing the manufacture, alteration, transfer, sale, possession or use of any false identification document or any document obtained by use of false statements or ID in the application process.

There are two alternatives states may take in implementing this recommendation:

Alternative I: Enact the Proposed Revision to the Model State Vital Statistics Act and its accompanying Regulations which have been prepared by the National Center for Health Statistics of the Department of Health, Education and Welfare (Text of the Act is found at the end of Appendix D1; Regulations may be obtained from HEW). This will insure adequate protection of application for and possession and use of birth, death and marriage certificates and copies of these documents.

Then, enact only Section 3 of the Proposed FACFI Model State Legislation entitled the "Identity Protection Act" (Exhibit I). This legislation will protect all other identification documents from abuse within the state's jurisdiction.

Alternative II: Enact the full text of the Identity Protection Act (Exhibit I).

Alternative I is preferred because HEW's Model State Vital Statistics Act and its accompanying Regulations set forth a comprehensive program for sound management of vital statistics information while providing many safeguards against false identification abuses (Sections one and two of the Identity Protection Act duplicate penal provisions of the HEW's Model Vital Statistics Act).

The Committee also recommends that both the Proposed Model State Vital Statistics Act and the Identity Protection Act be presented to the Council of State Governments to be included in their annual package of "Suggested State Legislation." The Committee recommends that the Proposed Revisions to the Model State Vital Statistics Act also be formally approved by the Department of Health Education and Welfare as soon as is practicable and sent to the appropriate state offices through established channels, as well as through the Council of State Governments.

The Identity Protection Act, which follows as Exhibit I, specifically protects the integrity of the use and possession of birth certificates, driver's licenses, and all other IDs used within the state, and establishes stricter criminal penalties for false identification crimes, requiring sentences for them to be served consecutively with any other sentence arising out of the same crime.

EXHIBIT I

MODEL STATE LEGISLATION

TEXT

Identity Protection Act

(Title, enacting clause, etc.)

Section 1. [Short Title.] This act may be cited as the [State] Identity Protection Act.

Section 2. [Fraudulent Use of Birth Certificates.]

(a) It is unlawful for any person to obtain, possess or use a birth certificate of another or a copy thereof for the purpose of establishing a false identity for himself or any other person.

(b) Any person who has in his possession the birth certificate of another person without lawful reason for such possession or who uses a birth certificate of another in the commission of a misdemeanor, is guilty of a misdemeanor and shall be fined not more than \$ or imprisoned for not more than years or both.

(c) Any person who has in his possession birth certificates of 2 or more persons without lawful reason for such possession or who uses the birth certificate of another person to aid in the commission of a felony shall be punished by a fine or not more than \$ or imprisonment for not more than years or both.

(d) Any person who applies for or obtains a birth certificate of another person without lawful reason shall be fined not more than \$ or imprisoned for not more than years or both.

(e) As used in this section:1. "lawful reason" means any reason as determined by [the appropriate section of the State Vital Statistics Code] for which a person may lawfully apply for or receive a certified copy of a birth certificate. 2. "Birth certificate" means birth certificates and copies and facsimilies thereof.

Section 3. [Other False Identification Documents]

(a) Any unauthorized person who manufactures, advertises for sale, sells or alters any document knowing or having reason to know that such document establishes or may be used to establish a false status, occupation, membership, license, privilege, or identity for himself or any other person shall be fined not more than \$ or imprisoned for not more than years, or both.

(b) Any person who obtains, transfers, transports, applies for, possess or uses any document or other thing for the purpose of establishing a false status, occupation, membership, license, privilege, or identity for himself or another person shall be fined not more than \$ or imprisoned not more than years, or both.

(c) Any person who uses any such document to commit a crime shall be punished by fine or imprisonment or both equal to that required by statute for the accompanying offense. Such sentence shall be served consecutively with that of the accompanying offense.

Section 4. [Severability.] [Insert severability clause.]

Section 5. [Repeal.] [Insert repealer clause.]

Section 6. [Effective Date.] [Insert effective date.]

CONTROL OF ACCESS TO VITAL STATISTICS RECORDS

(Implements FACFI Proposed Solution No. 1)

Vital statistics are a peculiar form of record; they are neither completely public nor completely private. In a sense, they are public records of private events. They do not share the inherent personal privacy of, for example, a medical record although they include medical data; at the same time, they are not a record of "public business" to which the public is clearly entitled. Furthermore, the status of the birth certificate in particular is complicated by its common use as a personal identification document. The FACFI believes that the potential for abuse of vital records, and the right to privacy of the individuals whose vital events are detailed in such records, justify requiring a "need to know" from individuals seeking the use of these records. It should be clear, and emphasized, that the potential for misuse lies not only in the use of birth certification for establishing a false identity, but also in the use of other vital statistics data to gather information to assist fraudulent application for birth certification. For example, death certificates can be scanned for data on dead infants, and marriage records can be used to establish false entitlement to Social Security and other benefits. For this reason, access to all vital statistics records should be controlled if misuse is to be minimized. (Details of the proposed control program are contained in Appendix D1, "A Plan for Reducing the Abuse of Birth Certification.")

Section 26(a) of the Model Vital Statistics Act,^[59] (Section 22 of the proposed Revisions to that act; see Appendix D1) which has been approved and recommended by the U.S. Public Health Service and the American Association for Vital Records and Public Health Statistics, proposes the following language with respect to disclosure of records:

To protect the integrity of vital statistics records, to insure their proper use, and to insure the efficient and proper administration of the vital statistics system, it shall be unlawful for any person to permit inspection of, or to disclose information contained in vital statistics records, or to copy or issue a copy of all or part of any such record except as authorized by regulation [or by order of (a court of competent jurisdiction)].

Certain individuals and groups (i.e., researchers, investigators, and genealogists) may require access to vital records in the course of their work. The rights of such individuals to inspect vital records should be established and controlled by state regulations. It should be recognized that persons having a legitimate interest in vital records are generally able to specify their needs and purposes before inspecting the records and do not require access to even a significant part of the general vital statistics files. We recommend that language similar to that of Regulation 13, Model State Vital Statistics regulations,^[60] be used as a guide in preparing such state regulations. (See Appendix D1.) These model regulations require that research organizations agree to conditions established by the registrar prior to use of vital statistics data for research purposes. Business firms or agencies seeking listings of names and addresses are specifically barred from obtaining such information under these regulations.

CONTROL OF ISSUANCE OF BIRTH CERTIFICATIONS
(Implements FACFI Proposed Solution No. 58)

FACFI recommends that standard state-issued application forms be used to apply for certified copies of birth certificates. The purpose of the application form is to solicit information about the applicant that would not be available to an imposter seeking to establish a false identity; information requested on the form would also assist state registrars in filling the requests of lawful applicants.

A prototype for such an application form is shown in Figure 8. Personal information requested in Part I and Part II of the application would probably be known by a person entitled to receive birth certification (i.e., the registrant, his parents or guardians, or attorney) but not by an imposter who had obtained the registrant's name and birth date through an obituary column. Besides providing assurance that the applicant for certification is not an imposter, this data assists the registrar's office in ensuring that the correct certificate will be located and supplied to the applicant.

The model application form also calls for the name, address, and signature of the applicant, and requires justification for the request. This justification is consistent with the model state regulations recommended by the FACFI and the Public Health Service which restrict birth certification to those with a "direct and tangible interest" in such certification (Model Regulation 13). A separate schedule of fees and addresses of records offices would be supplied with the application form for all states. The form also carries a clear warning of the legal penalties for willful seeking of false certification. The Committee recommends that the penalty be a felony rather than a misdemeanor.

REQUEST FOR COPY OF BIRTH CERTIFICATE

Mail request with fee or bring to:
 (name) _____ STATE DEPT. OF HEALTH
 Public Health Statistics Section, Room _____
 _____ (address)


PLEASE PRINT

I. BIRTH CERTIFICATE OF:		II. PARENTS OF PERSON NAMED IN BIRTH CERTIFICATE	
FULL NAME AT BIRTH		FATHER'S FULL NAME	FATHER'S BIRTHPLACE (Town)
DATE OF BIRTH	SEX	MOTHER'S MAIDEN NAME	MOTHER'S BIRTHPLACE (Town)
PLACE OF BIRTH (City, County, State, Hospital)			
III. PERSON MAKING THIS REQUEST		NUMBER OF COPIES WANTED	
Your Name	(No. and Street)	FEE ENCLOSED	\$
Your Address	(Town, State)	(See Fee Schedule)	

For the protection of the individual, certificates of vital events are not open to public inspection.

The following must be completed in order to permit this office to comply with the request.

RELATIONSHIP TO PERSON NAMED IN CERTIFICATE (e.g., parents, attorney)	FOR WHAT PURPOSE DO YOU NEED THIS COPY?
---	---

Your Signature 

Warning: False application for a birth certificate is punishable by up to five years in prison and/or \$10,000 fine.

Figure 8. A Model Application Form for Birth Certification

We recommend that a form of this type, applicable to all states, be made available nationwide at local vital records offices, town halls, or other locations designated by individual states. This service would insure that mail requests for birth certificates contain information known only to bona fide applicants and would provide a source of information and assistance to citizens on the infrequent occasions when a birth certificate must be obtained.

Laws restricting public access to vital statistics records and requiring justification for issuance of certified copies of birth certificates have been challenged in some states on the basis of provisions in state "freedom of information" laws. We believe that public rights to vital statistics information can be met without wholesale distribution of certified copies that can easily be abused by impersonators. We suggest that "freedom of information" requests be met using forms that do not resemble certified copies and are marked "Void For Identification Purposes." The information released should contain sufficient information to locate and verify the birth certificate, but should not provide details that are superfluous as public information and that would provide an imposter with the data needed to apply falsely for a certified copy. We suggest that the information be limited to the following: file number, name of registrant, sex, date of birth, and town or county of birth.

STANDARDIZED FORMS FOR BIRTH CERTIFICATES

We anticipate that when false application for birth certificates is curtailed through the precautions detailed above, more frequent attempts will be made to produce counterfeit certificates for use as false IDs. To counter this threat, we recommend that states adopt a standard format for certified copies of birth certificates, that such

certificates be issued in a form that is highly resistant to counterfeit and alteration, and that blank forms be properly secured and accounted for.

Figure 9 shows a sample of one type of secure birth certificate, which is based on a prototype prepared by American Bank Note Company for the Commonwealth of Virginia. The certificate is edged with fine-line intaglio printing, the details of which cannot be reproduced, either in this report or by a counterfeiter. The raised intaglio features on the original can easily be verified by touch as well as appearance; the rosettes in the upper left and right corners contain hidden letters which (on the original) can be made legible by viewing the document obliquely. The stock of the certificate is a safety paper that reveals clearly any attempt to alter information by erasure, bleaching, or "whiting out." The control number pre-printed on the certificate provides a basis for accounting and inventory of blank forms. Validation of the document can be accomplished either with the traditional raised seal or with a modern multicolor fine-line dry stamp, which offers at least equal protection against counterfeit and is more convenient to use. The cost of the improved form is estimated to be between nine and fifty cents per copy, depending on such factors as the size of the document and the number of copies ordered from the vendor.

In addition to full certified copies of birth certificates, most states offer "short form" copies or "birth registration cards." State regulations with respect to the issuance of such documents vary widely. In some states, short forms and birth cards are regarded as equivalents of the certified copy and are regulated accordingly; in other states, these forms are regarded merely as verification of the existence of a birth record and are made available rather freely. Both short forms and birth cards are wallet-size documents

COMMONWEALTH OF VIRGINIA

— CERTIFICATE OF LIVE BIRTH —
DEPARTMENT OF HEALTH — BUREAU OF VITAL RECORDS AND HEALTH STATISTICS

(Address)

ABNCO TEST

1. SEX: MALE FEMALE

2. RACE: WHITE BLACK OTHER

3. BIRTH: SINGLE FIRST BORN TWIN OR BORN

4. NAME OF HOSPITAL OR INSTITUTION OF BIRTH

5. COUNTY OF BIRTH (If independent city, leave blank)

6. CITY OR TOWN OR BIRTH

7. STREET ADDRESS OF BIRTH

8. STATE OF BIRTH (If foreign country, use mother's residence)

9. COUNTY OF RESIDENCE

10. CITY OR TOWN OF RESIDENCE

11. STREET ADDRESS OF HOME OF RESIDENCE

12. FULL NAME OF MOTHER

13. FULL NAME OF FATHER

SPECIMEN

14. AGE AT BIRTH

15. PLACE OF BIRTH

16. DATE AND HOUR OF BIRTH

17. SIGNATURE OF ATTENDANT

18. DATE RECORD FILED

19. REGISTRAR'S SIGNATURE

20. DATE RECORD FILED

*On Abbreviated Certified Copy, Not Applicable Must Be Typed In

This is to certify that this is a true and correct reproduction of the original record filed with the Bureau of Vital Statistics, Virginia Department of Health, Richmond, Virginia.

DATE ISSUED

Deane 2/9/2008
DEANE HUXTABLE, State Registrar

ANY REPRODUCTION OF THIS DOCUMENT IS PROHIBITED BY STATUTE. DO NOT ACCEPT UNLESS ON SECURITY PAPER WITH SEAL OF THE BUREAU OF VITAL STATISTICS CLEARLY AFFIXED. Section 32-353.27, Code of Virginia, as Amended.

DEPARTMENT OF HEALTH — BUREAU OF VITAL RECORDS AND HEALTH STATISTICS

Figure 9. Sample Form And Format For Certified Copy of Birth Certificate (derived from form used by Commonwealth of Virginia).

that are often used as "proof" of age or identity. In view of their ambiguous status and low resistance to abuse, we recommend that these documents not be accepted generally as identification of the bearer. The driver's license or state-issued "age-of-majority" ID card, personalized with a photograph and protected against counterfeit and alteration, should supplant the short form or card birth certificate as proof of age. We recommend that a certified copy of the birth certificate plus other identification be required in the initial application for either a driver's license or state ID.

The implementation of improvements in control of birth certificate issuance will generally require modification of existing state Vital Statistics Acts and regulations. FACFI recommendations are incorporated in the proposed amendments to the Model State Vital Statistics Act and Model State Vital Statistics Regulations found in Appendix D1.

MATCHING OF BIRTH AND DEATH CERTIFICATES (Implements FACFI Proposed Solution No. 5)

The purpose of matching birth certificates and death certificates is to block the popular "Infant Death" method, described in Section 3 of this report, of initiating a false identity by application for a copy of a birth certificate of a deceased person. The proposal recommends that notification of the fact of death be supplied to the registrar of vital statistics in the state of the decedent's birth, and provides for the marking of the birth certificate so that it can not be used as an ID by an imposter.

The correlation of all birth and death records that could be abused by imposters may appear to be a gigantic task; more than 100 million Americans have died just in the last 50 years, and most of

these deaths have not been matched with birth records. However, a recent study by The MITRE Corporation for the Law Enforcement Assistance Administration (See "Matching of Birth and Death Records," for full details of such matching, Appendix D2.) has indicated that matching is feasible and relatively inexpensive, provided some restrictions are placed on the process. The major restriction is limiting the correlation to those records most likely to be abused by imposters, i.e., those which pertain to people who would be 55 years of age or less. Such a restriction avoids the effort of correlating about 84% of past deaths while frustrating the great majority of those seeking a false identity. The bulk of those deaths that remain to be correlated are infant deaths which can be matched with birth records in the same state. The remainder of the records to be matched may require the transmission of information from the vital records office in the state where the person died to the state registrar in the state where he was born.

Interstate transfer of death certificate data could be accomplished by either of two methods: direct exchange of information between states, or interstate exchange through an appropriate Federal clearinghouse such as the National Center for Health Statistics of the U.S. Department of Health, Education and Welfare. We recommend the latter approach since most states presently supply microfilm copies of death and birth information to the National Center on a monthly basis. Thus, the sorting of this data by birth state at the National Center would be a relatively minor modification of an established flow of information and would save each state the cost of reproducing, sorting, and transmitting this data to every other state. Transmission of data in this fashion is also likely to be more accurate and easier to implement than state-to-state transfer.

Based on the stated restrictions and recommended method of interstate information exchange, we estimate the labor of screening and correlating old death records would average about seven man-years per state, with less than one person's full time effort per state required to correlate current records of persons dying at age 55 or less. The costs (in millions) of dollars of such a system are: one time correlation of old records: search of state registrar's files to identify deceased persons 55 or less at the time of birth: \$1; copying of relevant death: \$.5; sorting of records by HEW: \$1; locating and marking birth certificates at State offices: \$3.5; locating and matching birth certificates at local offices: \$2.5; software development: \$.1; administrative costs: \$.5. Total one-time matching of old records: \$9.1 million. Annual costs for matching birth and death records at state and local offices: \$.5 million.

Correlation of birth and death records will require some modifications to existing state laws. Accordingly, the Committee recommends that the National Center take the necessary measures to implement a nationwide system of birth/death matching; urges the Department of Justice to work with the Center to determine whether or not further authorizing legislation might be needed for such a matching program; and recommends that both agencies fully consider all privacy aspects of such matching in their deliberations. Should legislation be required, it should be drafted and submitted to the Congress without delay. As a part of this study the matter of a national death index containing the names of all deceased persons should also be discussed; and access to such an index should be limited to federal and state agencies including law enforcement agencies.

IMPROVEMENTS TO STATE DRIVER'S LICENSING SYSTEMS

The recommendations of the FACFI have noted the widespread voluntary use of the state driver's license as a personal ID and have called for improvements to protect this document from abuse by counterfeiters and impostors. Steps that should be taken to provide this protection have been described in studies by The MITRE Corporation under sponsorship of the Law Enforcement Assistance Administration ("Recommended Federal Guidelines for Improved Driver's License Security," Appendix D3) and by the Polaroid Corporation (A Proposal to Upgrade the Security of the State-Issued Driver's License," Appendix D4). All the recommendations directed toward improvement of the driver's license apply with equal force to the state ID or age-of-majority cards now issued by 34 states at the request of their citizens. The latter document is specifically intended for use as a personal ID.

The plan to improve the reliability of the driver's license as an identification document identifies three areas of concern: application procedures, resistance of documents to counterfeit and alteration, and interstate communication among motor vehicle registries. Methods to reduce fraudulent application for driver's licenses and state IDs include:

- Requiring independent identification in addition to a certified copy of a birth certificate for new license applicants.
- Filing a few items of information that do not appear on the license in order to discourage fraudulent application for renewal and duplicate licenses.
- Completing a check of license validity with the former state of residence before issuing a transfer license.

Identification required in addition to the birth certificate, which of course does not contain any personalizing information, should be of a type that could not easily be obtained with a recently acquired birth certificate; examples include school records, military IDs, or local references that can be cross-checked by telephone and directory. File information that does not appear on the license and can be used to check applications for duplicate licenses might include such data as mother's maiden name and the name of the high school or grade school attended by the original registrant. Applications for transfer of a valid license to a new state of residence should not be granted until a check of data with the former state of residence confirms that the license is valid and has not been reported lost or stolen.

We believe that these elementary precautions would significantly reduce the probability that fraudulent applications for licenses will be honored. The proposals involve little inconvenience to the public, which has a right to expect the state to support the integrity of its licenses and ID cards.

Our principal recommendation in the area of document security is that all states adopt the use of a photo-personalized driver's license and state ID card that incorporate significant resistance to counterfeit and alteration. Only 15 states (Alabama, Arkansas, Connecticut, Illinois, Indiana, Idaho, Maine, Maryland, Nebraska, Nevada, New York, Oklahoma, Tennessee, West Virginia, and Wisconsin) do not presently offer such a license. A stolen photo license is much more difficult for an impersonator to use than a license not containing a photograph. While no license is totally counterfeit-proof, we estimate that a photo license would cost a counterfeiter at least 20 times more to manufacture than a plausible counterfeit of a non-photo license. The need to retake photographs at renewal intervals of two to four years can provide the opportunity for increasing highway safety by requiring

eye examinations or written examinations on traffic laws at the same time. Finally, the additional cost of a photo license to the issuing state can be covered by a very modest increase in the license fee; a study performed for the State of Florida showed that all additional costs of adopting a color photo license could be recovered in four years with an average fee increase of 12.5 cents per year. Because of the vulnerability of non-photo licenses to false ID fraud, we recommend that such licenses not be accepted as sole evidence of identity for interstate transfer of the driving privilege.

Finally, we observe that the present method of interstate exchange of licensing information by mail is too slow and inefficient to provide an effective counter to license fraud. We recommend that a study be undertaken to determine the costs and impact of automating such information exchange through the National Driver Register and an existing communication network, such as the National Law Enforcement Telecommunications System.

The Committee strongly urges the department of Transportation and the Department of Justice to take further steps to examine these recommendations; implement those which can be implemented under current legislative and regulatory authority; and draft further legislation and regulations as necessary to accomplish these recommendations without delay.

SECTION 10

GUIDELINES FOR FEDERAL ACTION

The Federal government has a clear and direct interest in assisting the states in implementing FACFI proposals to counter the criminal use of false identification. Federal responsibilities are particularly clear-cut in the area of benefits programs in which false ID fraud causes direct loss of Federal principal or matching funds. The Federal government also has a direct interest in safeguarding the integrity of state IDs that serve as source documents for the issuance of U.S. passports and Social Security accounts. Finally, as part of its obligation to safeguard interstate commerce, the U.S. government should take vigorous steps to curtail the activities of the highly mobile individuals and groups practicing credit card and check fraud, and interstate dealing in false credentials. Some of the required Federal actions involve new legislation, while other steps can be accomplished through regulations affecting Federal agencies. This section outlines our program for action against false identification by the Congress and other segments of the Federal government.

LEGISLATION AGAINST FALSE IDENTIFICATION

(Implements FACFI Proposed Solution No. 4)

Federal Jurisdiction Over Interstate False ID Crimes

The FACFI's primary recommendation for legislation against false identification is enactment of S.2131, introduced in the 94th Congress. Included here as Exhibit II, this bill:

EXHIBIT II

94TH CONGRESS
1ST SESSION

S. 2131

IN THE SENATE OF THE UNITED STATES

JULY 16 (legislative day, JULY 10), 1975

Mr. THURMOND (for himself and Mr. EASTLAND) introduced the following bill;
which was read twice and referred to the Committee on the Judiciary

A BILL

To amend title 18, United States Code, relating to the production of false documents or papers of the United States, and the use of false information in obtaining official documents and papers of the United States, involving an element of identification.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*
3 That chapter 47 of title 18, United States Code, is amended
4 by adding at the end thereof the following new sections:
5 “§ 1028. **Use of false documents or false use of official doc-**
6 **uments to obtain official identification**
7 “ (a) Whoever, for the purpose of obtaining for himself
8 or another any official document or paper of the United

EXHIBIT II (continued)

2

1 States, or any agency or department thereof, involving an
2 element of identification, knowingly uses or supplies false
3 information, false or falsified documentation, or any docu-
4 ment or paper evidencing or purporting to evidence the birth
5 or identity or entry into the United States of any individual
6 other than the individual officially intended to be documented
7 thereby, shall be fined not more than \$, or imprisoned
8 not more than years, or both.

9 “(b) Whoever, for the purpose of obtaining for himself
10 or another any official document or paper of any State
11 (including any political subdivision thereof) or any agency
12 or department thereof, involving an element of identification,
13 knowingly utilizes or causes to be utilized any facility in
14 interstate or foreign commerce, including the mail, to send,
15 transport, transmit, carry, deliver, or otherwise move in
16 interstate or foreign commerce any false information, false or
17 falsified documentation, or any document or paper evidenc-
18 ing or purporting to evidence the birth or identity or entry
19 into the United States of any individual other than the
20 individual officially intended to be documented thereby, shall
21 be fined not more than \$, or imprisoned not more
22 than years, or both.

EXHIBIT II (continued)

3

1 **“§ 1029. Production, sale, or transmission of false docu-**
2 **ments to be used, or sale or transmission of**
3 **official documents used or intended to be used**
4 **falsely, in obtaining official identification.”.**

5 “(a) Whoever, for a monetary or other consideration—
6 “(1) falsely makes, forges, counterfeits, or alters,
7 or makes improper or unauthorized use of, any official
8 document or paper of the United States, or any agency
9 or department thereof, involving an element of identifica-
10 tion;

11 “(2) falsely makes, forges, counterfeits, or alters,
12 or makes improper or unauthorized use of, any official
13 document or paper of any State (including any political
14 subdivision thereof), or any agency or department
15 thereof, involving an element of identification, knowing
16 that such document or paper is being used or is intended
17 for use in obtaining any official document or paper of
18 the United States, or any agency or department thereof,
19 involving an element of identification; or

20 “(3) sells, transfers, or otherwise delivers any such
21 document or paper of the United States or of any State
22 knowing such document or paper to have been so made,

EXHIBIT II (concluded)

4

1 forged, counterfeited, or altered or so used or intended to
2 be used improperly or without authorization—
3 shall be fined not more than \$, or imprisoned not more
4 than years, or both.

5 “(b) Whoever utilizes or causes to be utilized any
6 facility in interstate or foreign commerce, including the mail,
7 to send, transmit, carry, deliver, or otherwise move in inter-
8 state or foreign commerce any document or paper purporting
9 to be an official document or paper of the United States or
10 any State [including any political subdivision thereof], or
11 any agency or department thereof, involving an element of
12 identification knowing that such document or paper has been
13 falsely made, forged, counterfeited, or altered, or is being
14 or is intended to be used improperly or without authoriza-
15 tion, shall be fined not more than \$, or imprisoned
16 not more than years, or both.”.

17 SEC. 2. The analysis of chapter 47 of title 18, United
18 States Code, is amended by adding at the end thereof the
19 following new items:

“1028. Use of false documents or false use of official documents to obtain
official identification.

“1029. Production, sale or transmission of false documents to be used, or
sale or transmission of official documents used or intended to be
used falsely, in obtaining official identification.”.

- Prohibits false applications for Federal documents by prohibiting the knowing use or supplying of false information or falsified documentation when obtaining Federal identification documents.
- Prohibits the knowing use of the mails or other channels of interstate commerce for transporting any false information or documents for the purpose of obtaining state identification documents.
- Prohibits the unauthorized making or altering of any Federal identification document.
- Prohibits the unauthorized making or altering of any state identification document when there is knowledge that such document will be used to obtain any document issued by the United States; and prohibits the sale or delivery of any such state identification document.
- Prohibits using the channels of interstate commerce or the mails to transmit any false Federal or state identification document or one intended to be used improperly.

The Committee recommends that the knowing possession of fraudulent documents of the U.S. or any state with intent to obtain Federal documents also be made a felony; and recommends that the following language be included in S. 2131:

"(c) Whoever, with the intent to defraud, receives, possesses, uses, furnishes, or attempts to receive, possess, use or furnish to another, any false, forged, counterfeited or altered document or paper purporting to be of the United States, or any agency or department thereof, or of any State (or any political subdivision thereof) knowing that such document or paper is being used or is intended for use in obtaining any official document or paper of the United States, or any agency or department thereof, involving an element of identification, shall be fined not more than \$ _____ or imprisoned not more than _____ years, or both."

Sec. 2. The analysis of Chapter 47 of Title 18, United States Code, is amended by adding at the end thereof the following new items:

"1028. Use of false documents or false use of official documents to obtain official identification.

"1029. Production, sale, transmission or possession of false documents to be used, or sale, transmission or possession of official documents used or intended to be used falsely, in obtaining official identification."

The following is the text of S. 2131 put into the new format for the criminal code revision proposed in S. 1, 94th. Congress:

Sec. 1345. Using a False Identity Document

"(a) Offense - A person is guilty of an offense if with intent to deceive or harm a person or government or for monetary or other consideration he:

"(1) traffics in an identity document that is false or relates to another person;

"(2) makes, receives, utters, or possesses a counterfeit, or forged identity document;

"(3) utters, receives or possesses an identity document that is false or relates to the identity of another; or

"(4) makes a material statement that is false to obtain an identity document.

"(b) Definitions - As used in this section the term:

"(1) 'counterfeited identity document' means an identity document that purports to be genuine but is not, because it has been falsely made or manufactured in its entirety;

"(2) 'forged identity document' means an identity document that purports to be genuine but is not, because it: (A) has been falsely altered, completed, signed, or endorsed; (B) contains a false addition thereto or insertion therein; or (C) is a combination of parts of two or more genuine written instruments;

"(3) 'identity document' means a written instrument issued by a federal, state, or local government agency that may be used to establish or assert the identity of a person; an identity document is false if it is used or intended to be used to pertain to a person other than the true subject of the document;

"(4) 'utter' means to issue, authenticate, transfer, publish, sell, deliver, transmit, present, display, use, certify, or otherwise give currency to.

"(c) Grading - An offense described in this section is:

"(1) a Class D felony in the circumstances set forth in subsections (a)(1) or (a)(2);

"(2) a Class E felony in any other case.

"(d) Jurisdiction - There is federal jurisdiction over an offense described in:

"(1) subsection (a)(1) if the identity document is or purports to be issued by a federal government agency, or by any State where the offender knows that the document has been falsely made, forged, counterfeited, or altered or so used or intended to be used improperly or without authorization;

"(2) subsections (a)(2)(3) if the identity document is or purports to be issued by a federal government agency, or by any State (or any political subdivision thereof) where the

offender knows that such document or paper is being used or is intended for use in obtaining any official document or paper of the United States, or any agency or department thereof, involving an element of identification;

"(3) this section if: (A) the United States mail or a facility of interstate commerce is used in the planning, promotion, management, execution, consummation, or concealment of the offense; (B) movement of a person across a State or United States boundary occurs in the planning, promotion, management, execution, consummation, or concealment of the offense."

There may be other loopholes in Federal statutes which should be closed to prevent false identification crimes. For example, under Federal law 18 U.S.C. Ch. 25 (42 U.S.C. 408) it is not illegal to manufacture or possess a counterfeit or altered Social Security card. The Committee recommends that the Department of Justice, the Social Security Administration, and other agencies further study such loopholes in statutes dealing with Federal identification documents and recommend specific legislation to close such loopholes.

ACTION TO COMBAT FRAUD AGAINST GOVERNMENT

(Implements FACFI Proposed Solution Nos. 36, 43)

Welfare Fraud

We believe that the Federal government can take positive action to reduce the incidence of false ID fraud against government by revising its auditing procedures on assistance payments programs and by adopting more stringent guidelines for identification of applicants for government documents and benefits.

Auditing Improvements Needed

In attempting to define the magnitude of false ID fraud against public assistance programs, the FACFI was severely hampered by the vague nature of public audit reports on these programs. Each state that participates in cost-shared assistance programs is required to conduct regular "quality control" audits of the programs. These audits are reviewed by the Federal government, which is also empowered to conduct independent audits of state programs. Reports of these audits are expressed in terms of "error rates," i.e., the fraction of cases sampled in which recipients were found to be ineligible or receiving either overpayments or underpayments. These reports, though compiled at great expense to both state and Federal government, do not provide any indication as to the extent of possible fraud in the programs. The reports lump suspected fraud by recipients or agency personnel together with innocent mistakes, minor irregularities in procedures, and gross negligence into the cryptic categories of "agency error" and "client error."

Federal auditors are supposed to inform the proper state authorities in cases of suspected fraud; however, there appears to be no readily available public record of such reports or an accounting of state responses to them. In the interest of improved public accountability as well as a more accurate determination of the scope of false ID fraud, we recommend that both state and Federal audit reports be required to enumerate referrals to state authorities of suspected agency and client fraud. We have outlined Federal legislation to prohibit the use of false IDs in application for benefits under Federal programs; upon enactment of this legislation, we recommend that audit reports also enumerate referrals to Federal authorities for investigation of suspected false ID fraud.

It appears that no new legislation or changes in Federal regulations are required to implement these improvements in audit reports. The Secretary of Health, Education and Welfare has the authority to determine reporting requirements for benefits programs under his jurisdiction. The Secretary of Agriculture has similar authority with respect to the food stamp program.

Minimum Guidelines For Identification

The FACFI recommends that the Federal government establish more effective guidelines for the identification of applicants for Federal or cost-shared assistance programs. If authority for the establishment of such guidelines is deemed to require legislation, we suggest the following language:

Social Security Act Amendment

- a. The Secretary (of Health, Education and Welfare) shall require as a condition of eligibility under any federally-assisted program administered pursuant to the Social Security Act that each applicant for or recipient of aid shall furnish to the state agency administering such program his Social Security account number (or numbers, if he has more than one such number).*

 - b. Such state agency shall require that each applicant furnish evidence, in addition to a Social Security account number, sufficient to accurately establish his age, citizenship, or alien status, and true identity; and that whenever possible, the
- *[Note, see 42 U.S.C. 405 which requires similar action but has not been adequately enforced by the Secretary]

validity of such evidence shall be established
prior to assistance being granted to any applicant.

Similar language should be added to Title 7, United States Code
to cover the food stamp (coupon) program.

We recommend that the guidelines established under such authority
provide clear guidance for state agency workers to decide whether the
evidence of identity presented is sufficient. An excellent tool
for assisting such decisions is a Decision Logic Table
of the type developed for New York State by Welfare Research, Inc. [61]
A table of this type lists the conditions encountered in making a
decision (in this case, whether the applicant and eligible dependents
are correctly identified) and the actions to be taken for each com-
bination of conditions. We suggest that evidence of identity include:

- A full certified copy of birth certificate issued
by a state or state-controlled office, or
- Verification of birth record by the state registrar, or
- Passport, or
- Alien ID Card (INS Form I-151 or I-186) or Naturaliza-
tion Papers, plus one or more of the following:
- Driver's license,
- State-issued ID card,
- Military ID or discharge papers,

- Credit or charge account cards with signature,
- Verified personal contact.

Direct agency-to-agency verification of the information contained on the birth certificate is listed as an acceptable substitute for a full certified copy of the certificate itself. Because an applicant intent on committing fraud can easily make arrangements with an accomplice to "verify" his identity by telephone, we recommend that personal contacts be accepted only when they also can be verified. A very effective means of verifying such contacts are "criss-cross" directories, which are compiled for almost all areas of the U.S. and are widely used by direct mail advertisers, telephone canvassers and journalists. These directories cross-list individuals by telephone number, street address, and often include occupation as well. They are usually available from the local telephone company or from private publishers at rental fees of \$100 to \$150 per year.

We recommend that a procedure similar to that outlined above also be followed in confirming the identity of adult applicants for new Social Security accounts. H.R. 3737, introduced in the 94th Congress, would require that anti-counterfeit features be employed on all future Social Security cards. The Committee favors such Legislation.

Photo ID Cards For Welfare Recipients

The FACFI also recommends that recipients of public assistance and food stamp benefits be issued photo ID cards by the participating state agencies. These cards should be required in order to cash welfare checks or to purchase food stamps. The cards should incorporate significant safeguards against counterfeit and alteration and should contain, as a minimum, the portrait and signature of the authorized

bearer. The card should contain a number matched to the regularly issued check or Authorization to Purchase (ATP) document. If this number is embossed on the card, it can easily be transferred to the check or ATP document when it is negotiated.*

COOPERATION WITH THE STATES

(Implements FACFI Proposed Solution Nos. 10, 11, and 49)

Several FACFI recommendations call upon the Federal government to encourage the initiatives of individual states in their efforts to combat false ID crime, and also to take an active part in fostering interstate cooperation in this area. Implementation of these recommendations in most cases requires no new legislation or regulation changes, but simply an allocation of internal resources by Federal agencies. In other cases, Federal demonstration grants and matching funds under existing programs can be used to good effect in promoting state efforts in reducing false ID fraud and in improving the reliability of existing state identification documents.

Matching Birth and Death Records

Federal action is necessary to implement this Joint Federal-state proposal. See Section 9 for a discussion of this program.

Improvements To State Driver Licensing Systems

Federal action is necessary to implement this Joint Federal-state proposal. See Section 9 for a discussion of this program.

*Penalties for alteration, forgery or counterfeiting such card should parallel those in the 42 U.S.C. 408 Amendment above.

Improved Exchange of Information

Improved exchange of information between state and Federal government on the abuse of state and local IDs is essential to determine the extent and patterns of such abuse and to encourage corrective measures and prosecution. We have recommended that formal notification of the use of state birth certificates and driver's license as false IDs be given to the appropriate state officials by Federal law enforcement agencies. These reports can originate independently from each agency that discovers an instance of abuse; it is recommended that the Justice Department initiate steps to provide agency procedures for the generation of these reports and supervisory action to insure that these procedures are followed.

Clearinghouse For False ID Information

We believe that more effective detection of patterns and trends may result if such reports were coordinated through an interagency clearinghouse similar to the Fraudulent Document Center currently operated by the Drug Enforcement Agency and the Immigration and Naturalization Service. This Center, formerly located at Yuma, Arizona and now at El Paso, Texas, indexes genuine birth and baptismal certificates known to have been used by illegal aliens to document false claims to U.S. citizenship. The filing of these documents is presently a manual operation. We estimate that a national clearinghouse for false identification documents that records not only abuses of birth certificates but of driver's licenses as well would need to handle approximately 100 times the number of records as the El Paso center, and thus would require automated search and retrieval capabilities. The feasibility, cost, and effectiveness of such a national center should be explored further through a federally-sponsored feasibility study.

Training Programs

We have recommended that Federal agencies which have developed effective techniques for training employees in the detection of false ID fraud share their expertise with other concerned organizations at the Federal and state level. Informal cooperation will probably suffice to implement this kind of information exchange among Federal agencies; however, a more formal channel needs to be opened so that improved training can be given to state and local employees. We recommend that the Department of Health, Education and Welfare institute a series of seminars at regional HEW centers to inform state public assistance administrators and registrars of vital statistics of the problem of false ID use and the techniques used to combat such fraud. A similar service for state motor vehicle administrators should be set up by the Department of Transportation. We strongly encourage the use of demonstration grants for improved state training programs for the detection of false IDs.

Other Programs

The FACFI recognizes and encourages the efforts of Federal agencies to publicize successful innovations by individual states in countering false ID fraud. For example, the Social and Rehabilitation Service, Department of HEW, has periodically issued a series of documents entitled "How They Do It," which illustrate innovative practices in the administration of public assistance. Two such publications have dealt with potential solutions to aspects of false ID fraud. "Bank Distribution Systems for Assistance Payments,"^[62] issued in March 1974, describes projects in New York State and Pennsylvania that had the effect of reducing losses in welfare through theft and forgery; "Photo IDs,"^[63] issued in July 1974, describes the New York State system of

photo identification and its apparent success in reducing losses through check fraud and multiple application for benefits.

Federal Funding

Finally, we recommend that Federal encouragement be given to states which undertake significant efforts to improve the reliability of birth certification and the issuance of driver's licenses and state ID cards. This encouragement can take the form of demonstration grants for innovative projects or Federal loans or other "seed money" for institution of photo licenses, secure birth certificates, and other improvements recommended by the FACFI. We recommend that all interested Federal and state agencies work to establish such programs and provide the necessary funding for them.

SECTION 11

ACTION BY THE PRIVATE SECTOR

Ultimately, it is the private sector -- business and the general public -- that pays the tab for false ID crimes, in direct losses, higher prices, and the burden of wasted tax dollars. Federal and state lawmakers and law enforcement people can and should make life more difficult for the criminal user of false IDs, but only an alert public can put him out of business. In this section, we summarize the means by which all of us can help to prevent false ID crime.

ACTION BY THE BUSINESS COMMUNITY

It is unlikely that use of a highly sophisticated means of false ID fraud will be discovered in the course of a normal business transaction; however, a great deal of loss to business results from very unsophisticated false ID fraud. A business can prevent most of this loss by making use of simple precautions that will not inconvenience either the sales staff or the customer. For example, businesses that accept national credit cards can reduce liability for losses from stolen or altered credit cards by following these simple rules:

- Compare account number on the card with the latest list of stolen, lost, or suspended cards.
- Verify the account status by telephone for all transactions exceeding the card plan's "floor limit."

- Check the signature block on the card for improper background material or a pasted-on layer of material that could indicate alteration.
- Make sure the signatures on the sales draft and the card match.

Businesses that provide check cashing services should consider adopting reasonable rules to reduce potential losses to forgers and counterfeiters. Many businesses limit the amount of any check cashed to a maximum sum or to the amount of purchase, or refuse to accept third-party checks. The American Bankers Association has recommended some general rules^[64] for financial institutions which apply equally to other businesses that negotiate checks:

- Know your endorser. No identification document accepted in lieu of personal knowledge is completely counterfeit-proof.
- Know your caller. Using the telephone directory, check the phone number of anyone provided by the customer as a credit reference.
- Prosecute without compromise. The best way to stop a check thief is to put him out of circulation.

The state driver's license, as the identification document most commonly used in check cashing, deserves special scrutiny. Some minimum steps in validating a license, adapted from a list distributed by Driver's License Guide, Inc., include the following:^[65]

- Check the surface for abrasions, cuts, or changes in density for alterations.
- Compare the license description and signature on the license with the person and the signature on the check.
- Doublecheck laminations. Extra laminations on a license can hide alterations.
- Beware of state IDs that do not carry a state seal or issuing agency identification.
- Be cautious of non-photo licenses.
- When in doubt, ask the individual the birth date, address or Social Security number that appears on the license.

The serial number of any ID accepted should be written on the back of the check to assist in subsequent investigation of a fraudulent item.

Businesses that accept checks for a large portion of their sales should consider installing an automatic check validation system or one of a variety of manual, semi-automatic, or fully automatic identity verification aids that are commercially available. Many of these systems alleviate the need for constant manual scrutiny of identification documents. A number of such systems are described in FACFI staff papers appearing in this report as Appendix C2, "Automated Identification Technology," and Appendix C3, "Some Commercially Available Identification Products."

We would like to emphasize the important role of the business community in the investigation of false ID fraud and in the prosecution of those responsible for it. There is little deterrent value in laws against fraud if the losses from the use of counterfeit and forged checks and stolen credit cards are quietly written off as bad debts by the victim, while the false ID criminal is left undisturbed to strike again. The person engaged in passing phony checks or "working a hot card" is typically operating on a tight schedule; therefore, a prompt report to the police or the credit card association is necessary to prevent a thief's quick getaway. Once the thief is apprehended, further effort on the part of a business will be required for investigating and prosecuting the offender, which may involve expense and even embarrassment to the victim. Such participation in the legal process is, however, the best insurance against future losses.

We have observed that false ID fraud succeeds best with the passive cooperation of the victim: laxity in the examination of credentials, suppression of the losses suffered, and refusal to participate in prosecution of the perpetrator. Conversely, an aroused and alert business community that makes the best use of procedural, technical, and legal defenses against false ID fraud can undoubtedly reduce the profit and the popularity of this type of crime.

ACTION BY THE GENERAL PUBLIC

All of us, as consumers and citizens, have an important role in the coordinated national program recommended by the FACFI to solve the costly problems of false ID fraud. The success of this program is ensured if we each take these steps:

- Patronize the secure business. Businesses that are trying new methods to reduce their losses from false ID fraud deserve our support. If they succeed in reducing such losses, they will be able to pass their savings on to the public in the form of better service and lower prices. Some of the new procedures for cashing checks or completing credit transactions may involve unfamiliar techniques that will require a learning period for both businesses and their customers. This uncomfortable period will transition into a smooth process that should eventually result in quicker and less troublesome authorization of checks and credit. However, if anyone feels the new procedures are an invasion of privacy or involve great inconvenience, those views should be made known to the management. There is enough choice in fraud-resistant identity verification systems that no business is bound to any type that results in the "hassling" of customers.
- Insist that state government protect the integrity of personal identification. You have a right to expect that personal documents issued by the state, such as a birth certificate, driver's license or "state ID" card, will be safeguarded from abuse by counterfeiters, thieves, and imposters. The acceptability of your own documents in another state or in applying for Federal documents and benefits may depend on your state's efforts in adopting proper safeguards. The cost to the state of such safeguards is not prohibitive and can be covered with a nominal increase in licensing or certification fees. In fact,

many improvements could be made with no fee increase at all because present fees more than cover the cost of license and vital registries. The "profit" from these services invariably goes into the state's general fund, which is typically insatiable.

- Support state and national legislation against false identification. The present condition of laws regarding false identification is so confused that it actually constitutes part of the problem. Each separate use of each false document must be proven under a different statute before the user of a false ID can be punished. Because of jurisdictional loopholes, counterfeit versions of state and even U.S. IDs can be, and are, freely offered for sale. The legislation proposed by the FACFI would protect the public against these abuses; however, we believe that a strong showing of public support will be necessary for the rapid passage and vigorous enforcement of these measures.

In the course of our investigations into false ID crimes and in reading the underground literature which advertises false IDs and advocates their use, we have been struck with the open contempt displayed for American society and for the people who work to support it. To the enterprising criminal, a driver's license in a false name is literally a "license to steal" or to commit numerous other crimes. In this report, we have attempted to show how common and expensive this abuse has become, and to outline a coordinated plan to end it. We can limit the abuse of our identification documents without jeopardizing either our liberties or our personal privacy if we discard our present complacency toward this growing national problem and work together towards its solution.

REFERENCES

1. Alvin Toffler, Future Shock (New York: Random House, 1970), pp. 71.
2. The Paper Trip, publisher unknown, undated.
3. Midnight, March 1, 1976, p. 3.
4. David Black, "Shedding Skin," New Times, Oct. 17, 1975, p. 40.
5. See, for example, the Privacy Act of 1974, 5 U.S.C. Sec. 552a.
6. Leonard F. Chapman, Jr., Commissioner, Immigration and Naturalization Service, Address before the New York Chamber of Commerce and Industry, Dec. 5, 1974.
7. U.S. Congress, Senate, Senator Hruska inserting Frances Knight's Remarks on Passport Fraud, 94th Congress, 1st Session, 5 December 1975, Congressional Record 121:179.
8. "Survey of State and Territorial Vital Registration Officials," Report to State and Local Documents Task Force of the FACFI, May 1975.
9. National Highway Traffic Safety Administration, Report to the State and Local Documents Task Force of the FACFI, May 1975.
10. Passport Office, U.S. Dept. of State, Report to the Federal Documents Task Force of the FACFI, May 1975.
11. Visa Office, U.S. Dept. of State, Report to the Federal Documents Task Force of the FACFI, May 1975.
12. Immigration and Naturalization Service, U.S. Dept. of Justice, Report to the Federal Documents Task Force of the FACFI, May 1975.
13. Social Security Administration, U.S. Dept. of Health, Education, and Welfare, Report to the Government Payments Task Force of the FACFI, May 1975.

14. U.S. Dept. of Health, Education and Welfare, Records, Computers, and the Rights of Citizens, DHEW Publication No. (OS) 73-97, July 1973.
15. Testimony of Committee on the Judiciary, House of Representatives, Hearings Before the Subcommittee on Immigration, Citizenship and International Law on H.R. 982 and Related Bills.
16. M. Devi, The Massachusetts Voter Registration Procedure, The MITRE Corporation, Memorandum D81-M-3026, January 14, 1976.
17. Interbank Card Association, Report on Fraudulent Use of Bank Credit Cards, prepared for the Commercial Transactions Task Force of the FACFI, March 1975.
18. Irwin Ross, "The Credit Card's Painful Coming-of-Age," Fortune, Oct. 1971, p. 150.
19. Philadelphia Daily News, January 28, 1976.
20. U.S. Postal Inspection Service, "False Identification Usage in the Cashing of Checks Stolen from the Mails," Report to the Commercial Transactions Task Force of the FACFI, March 1975.
21. Editorial Staff, "How Big is the Bad Check Problem?," Security World, July/August 1974.
22. E. L. Schroeder, Federal Bureau of Investigation, Correspondence to The MITRE Corporation, October 29, 1975.
23. U.S. Customs Service and U.S. Drug Enforcement Administration, Report to the Federal Documents Task Force of the FACFI, May 1975.
24. Committee on the Judiciary, U.S. Senate, Hashish Smuggling and Passport Fraud: 'The Brotherhood of Eternal Love', Document 23-538-0, U.S. Government Printing Office, 1973.
25. Lasko Associates, Inc., quoted in Dept. of Justice press release, December 9, 1975.
26. ICF, Inc., letter to Leonard F. Chapman, Commissioner INS, dated December 4, 1975.
27. U.S. Government Accounting Office, Report on Operations of Immigration and Naturalization Service Chapter 3, (to be released).

28. U.S. Immigration and Naturalization Service; Fraudulent Entrants Study (to be released).
29. "Survey of Police Departments and Sheriff's Offices," Report to Fugitives Task Force of the FACFI, May 1975.
30. Federal Bureau of Investigation, "Case Histories," Report to the Fugitives Task Force of the FACFI, May 1975.
31. Federal Bureau of Investigation, Summary of Statistics for the 1974 Fiscal Year.
32. San Francisco Chronicle, March 21, 1973.
33. Bank Administration Institute, The Impact of Exception Items on the Check Collection System, (Part Ridge, Illinois), 1974.
34. U.S. Dept. of Commerce, Crime in Retailing, 1975.
35. Super Market Institute, "Bad Check Losses: A Report on Current Trends." Special Research Report #5, 1973.
36. U.S. Dept. of Commerce, The Cost of Crimes Against Business, November 1974.
37. American Bankers Association, Report to the Commercial Transactions Task Force of the FACFI, August 1975.
38. "Driver's License Leads False ID," The ABA Bank Insurance and Protection Bulletin, Vol. LXVIII, No. 11, May 1976.
39. Organized Crime - Securities: Thefts & Frauds, Hearings Before the Permanent Subcommittee on Investigation, Committee on Government Operations, U.S. Senate, 93rd Congress, 1st Session, Part 1, Document No. , p. 20.
40. U.S. Marshalls' Service, U.S. Dept. of Justice, Bank Security Survey Report, undated p. 31.
41. Thomas T. Murphy, The Magnitude of Lost and Stolen Securities at N.Y.S.E. Member Firms 1969-1972, The New York Stock Exchange, August 1973, Table 1.
42. "False Identification Problems in the Broker-Dealer Community," Report of the National Association of Securities Dealers Inc. to the FACFI, May 1975.

43. Washington, D.C. Metropolitan Police Department, Report to Commercial Transactions Task Force of the FACFI, August 1975.
44. G. Christian Hill, The Wall Street Journal, March 12, 1976.
45. Congressional Record, September 15, 1975, p. S15926-27.
46. Sunday Denver Post, March 7, 1976, p. 1.
47. Office of New York State Comptroller, Audit Report on Photo I.D. Program, New York City Human Resources Administration, Report No. NYC-22-74, February 15, 1974.
48. N. Ferraro, "Report on Investigation of Welfare Fraud for 1974," Office of AJEENS County, N.Y., 1975.
49. Report of the Federal Grand Jury for the Eastern District of Pennsylvania on Welfare Check Theft and Fraud in Pennsylvania and the Administrative Processing of Pennsylvania Welfare Recipient Complaints of Non-Receipt, undated.
50. U.S. Fact Book, The American Almanac, 95th Edition, Grosset and Dunlap, (New York,) 1975.
51. Office of New York State Comptroller, Audit Report on Fraudulent Duplicate Check Claims, New York City Human Resources Administration, Report No. NYC-50-74, April 1, 1974.
52. "Food Stamp Survey," Government Payments Task Force of the FACFI, July 1975.
53. Statement by Richard A. Feltner, Assistant Secretary of Agriculture, before the Committee on Agriculture and Forestry U.S. Senate, November 19, 1975.
54. Social Security Administration, Bureau of Retirement and Survivors Insurance, Social Security Administration Fraud Deterrence Program, 1970-1973, (to be released).
55. D. Goldenberg, correspondence with J. Purcell, Division of Check Claims, U.S. Treasury Dept., The MITRE Corporation, memorandum D70-M1883, December 17, 1975.
56. Minot v. Curtis, Cumberland, 441, (1811).
57. Memorandum to All City and Town Clerks, et al. from Francis X. Belotti, Attorney General and Paul Guzzi, Secretary of the Commonwealth, December 5, 1975, p. 1.

58. Federal Register, Vol. 41, No. 117, pp. 24431-24437, June 16, 1976.
59. Public Health Service, U.S. Department of HEW, Model State Vital Statistics Act, PHS Publication No. 794, 1960.
60. Public Health Service, U.S. Department of HEW, Model State Vital Statistics Regulations, Document No. 616.6, 8/7/73. Also see Appendix D1.
61. M. F. Micciantuono and J. H. Avis, Decision Logic Table Handbook, Welfare Research, Inc., undated.
62. U.S. Department of HEW, Publication SRS-74-21213.
63. U.S. Department of HEW, Publication SRS-75-21220.
64. American Bankers Association, Identification With and Without Credentials, 1974.
65. "ID Checklist," Driver's License Guide, Inc., 1976.

PART IV

APPENDICES

APPENDIX A

TASK FORCE REPORTS

In order to address the many aspects of the use of false identification and to focus the concerns and expertise of its members, the FACFI divided into these five Task Forces:

- **Task Force I – Government Payments**, which focused on false identification fraud in programs that involve disbursement of monies to individuals by local, state and Federal agencies.
- **Task Force II – Commercial Transactions**, which was concerned with the fraudulent use of personal identification in over-the-counter sales and bank transactions.
- **Task Force III – Fugitives**, which concentrated on the use of false identification by fugitives to avoid detection and arrest or linkage to a previous criminal record, to remain in a covert status, or to aid in the commission of further crimes.
- **Task Force IV – Federal Documents**, which investigated the use of false or fraudulently obtained Federal documents in the conduct of criminal activity.
- **Task Force V – State and Local Documents**, which focused on the use of false or fraudulently obtained state- and community-issued documents in the commission of crimes.

The initial assignment for each Task Force was to determine the nature and scope of the false identification problem in their area. Task Force reports were to include their findings and preliminary suggestions for solutions. To gather the necessary information, each Task Force examined a variety of public reports and agency records, and conducted seventeen mail surveys of national and international scope. The material gathered in this fashion reflects the experience and the records of several hundred responsible individuals in business, law enforcement, and government.

First drafts of the five Task Force reports were issued between May 1975 and September 1975. The FACFI staff used these reports in developing a summary of the national false identification problem and in formulating preliminary proposals for solutions. The reports from Task Forces I through V have since been redrafted to reduce the amount of repetitive material and to obtain a more uniform and readable format. They are included herein as Appendices A1 through A5, respectively.

APPENDIX A1

**REPORT OF THE GOVERNMENT PAYMENTS TASK FORCE
ON THE
SCOPE OF THE FALSE IDENTIFICATION PROBLEM AND
PRELIMINARY RECOMMENDATIONS FOR SOLUTIONS**

Submitted to

**Federal Advisory Committee On False Identification
David J. Muchow, Chairman**

May 1976

TABLE OF CONTENTS

	<u>Page</u>
SECTION I - INTRODUCTION	A- 7
Purpose	A- 7
Scope	A- 7
Data Gathering	A- 7
Evaluation of Data	A- 8
SECTION II - THE FALSE ID PROBLEM	A- 9
General	A- 9
Application Phase	A- 9
Use Phase	A-10
Analysis of Programs	A-10
Aid to Families with Dependent Children	A-11
Medicaid	A-19
Food Stamps	A-20
Social Security Programs	A-26
SECTION III - PRELIMINARY RECOMMENDATIONS	A-31
General	A-31
Recommendations to State Government	A-31
Recommendations to Federal Government	A-33
ATTACHMENT I - COMPOSITION OF THE TASK FORCE	A-34

Report of the Government Payments Task Force
on the
Scope of the False Identification Problem and
Preliminary Recommendations for Solutions

SECTION I

INTRODUCTION

Purpose

The mission of the Task Force is to investigate the national impact of false identification fraud on programs that involve payments by local, state, and federal governments to individuals.

Scope

Four areas, each of which involves programs of national scope, were investigated by the Task Force. These areas included the Aid to Families of Dependent Children (AFDC) and Medicaid programs administered by the Assistance Payments Administration, Department of HEW; the Food Stamp Program of the Department of Agriculture; and four programs administered by the Social Security Administration: Supplemental Security Income (SSI), Health Insurance (HI), Disability Insurance (DI), and Retirement and Survivors Insurance (RSI).

Programs administered by the Veterans Administration and the Department of Housing and Urban Development that involve government payments were not investigated.

Data Gathering

Questionnaires were prepared for each of the four areas investigated. Eighty-six sets of questionnaires covering AFDC, Medicaid and Food Stamps were sent to Directors of Welfare in each state as well as Guam, Puerto Rico and the Virgin Islands; Welfare Quality Control Directors in several states; state and county auditors in several states; and the Inspectors General of New York and Michigan. Twenty sets of questionnaires covering the four Social Security Administration programs were sent to Social Security Headquarters and Regional Offices throughout the country.

Evaluation of Data

Approximately 40% of the questionnaires have been returned. Evident thus far is the apparent lack of information relative to the frequency of false ID fraud and its fiscal implications. This lack of information should not be taken to mean that a problem does not exist. Results of several investigations carried out independently by individual states and localities will be cited that show significant impact from false ID fraud in government payments programs. Several of the returned questionnaires have contained expressions of deep concern about the use of false identification and the hope that something can be done to alleviate the problem. The Office of the Commissioner of Welfare, Department of HEW, has recommended on several occasions to the National Welfare Fraud Association that information on frequency and impact of false ID fraud should be collected by the states and reported to the NEW National Center of Social Statistics in Washington, D.C.

SECTION II

THE FALSE ID PROBLEM

General

False ID fraud in government-assisted welfare and social insurance programs has significant national problem potential because of the ubiquitous nature and staggering dollar volume of such programs. For example, in January 1975, a nationwide average of 11.1 million AFDC recipients were receiving benefits at the rate of \$730 million each month; this represents an annual cost to taxpayers of \$8.8 billion. The federal government issued over 100 million benefit checks in fiscal 1975 under SSI, DI, and RSI programs; these checks represented a total dollar value of over \$13.7 billion. Benefits under the HI program (which includes Medicare) amounted to an additional \$9.2 billion in fiscal 1975.

Government payments programs have generally displayed a steady growth in beneficiaries over recent years; the growth of some programs, such as Food Stamps, has been spectacular. In 1965, recipients of Food Stamp benefits numbered 400,000 and total benefits were \$36 million. As of January 1975, the program had expanded over a hundredfold to encompass 19.1 million recipients and a payment level of \$5.2 billion per year. Programs of this scale present many opportunities for abuse by fraud, whether by false ID or not. Even if only a small percentage of the transactions between government and the beneficiaries of these programs are fraudulent, the total dollar loss to taxpayers in direct payments and costs of fraud detection and prosecution can be very high. Thus, although our surveys have indicated that false ID fraud is generally viewed as only a small part of total program abuse, the Government Payments Task Force has concluded that such fraud constitutes a significant national problem that is deserving of further study.

Government payment programs are subjected to false ID fraud in both "application" and "use" phases of the programs and these are discussed below.

Application Phase

All the programs studied by the Task Force require some sort of application for future benefits. During this "application phase," applicants are asked to identify themselves and any dependents on whose behalf program benefits are sought. The types of identification documents currently required by state agencies

were found to vary widely, ranging from none at all to a self-consistent set of official documents. The most commonly used documents in false ID fraud in this phase appear to be birth and baptismal certificates, state-issued driver's licenses, and Social Security cards.

Fraudulent documents are obtained in a number of ways. Birth certificates are usually genuine documents that have been altered and then photocopied. Baptismal and some birth certificates, on the other hand, can be easily generated by forging data on official appearing blanks bought at stationery stores or through mail order companies. Fraudulently used driver's licenses are obtained through theft and counterfeiting; they can also be obtained by application, using a false birth certificate as a "breeder" document. Although the Social Security card was never intended to be used as an identity document, it is used extensively as such in both legitimate and fraudulent transactions. Until recently, little identification was required to establish a new Social Security account. Thus, it was possible for an individual to establish accounts under several aliases. This has led to the collection of multiple benefits not only from Social Security programs but also from other government payments programs in which the multiple Social Security cards served as "identity documents" at application. Social Security cards have also been obtained by theft or counterfeiting. Unofficial "permanent" Social Security cards made of metal can also be obtained by supplying mail-order firms with an account number that is assumed or fictitious; these unofficial cards are sometimes used successfully for identification.

The period between application for government benefits and the receipt of benefits varies from a few days (or weeks) in the case of emergency relief payments to several months (or years) in the case of certain Social Security programs.

Use Phase

False ID has been employed in the "use" phase when persons fraudulently assume the identity of others to collect their benefits. This use of false ID occurs most commonly in the cashing of stolen government checks or Food Stamps. Apparently, many banks and businesses are willing to cash these instruments without adequate identification of the endorser.

Analysis of Programs

The following sections present analyses by the Task Force of surveys of AFDC, Medicaid, Food Stamp, and Social Security programs.

The analyses describe the range of requirements for recipient identification in application and use phases of the programs, and give available data on the scope of the false identification problem.

Aid to Families with Dependent Children

Sources of Information

Twenty-eight responses to the questionnaires on the use of false identification to obtain Aid to Families with Dependent Children (AFDC) have been received. Respondents represent twenty-five states, one county (Los Angeles), one territory (Guam), and the Commonwealth of Puerto Rico.

The Normal Process

The AFDC process begins when an applicant (generally one adult and one or more children) indicates verbally or in writing that they are in need of public assistance. Initial application may be made by phone, in writing or by personal appearance at a local political subdivision. Eligibility for public assistance under the AFDC program is limited to U.S. citizens and legal aliens permanently residing in the U.S. Eligibility criteria include resource and income limitations, financial need and deprivation. When application is made and the welfare organization is satisfied that the applicant is indeed eligible, instructions are generally forwarded to an office of the state welfare organization from which grants are issued. In some states, grants are prepared centrally within counties, in others by the state welfare office and still others by the state controller or treasurer.

Once AFDC eligibility is established, states are not required to issue an AFDC identification document to recipients. Of the twenty-eight respondents to the questionnaire, 5 issue a photo ID, 2 issue an ID with no photo and 21 issue no ID at all.

The financial assistance provided to AFDC recipients is usually in the form of a semi-monthly check or warrant. Nationwide, as of January 1975, there were an average of 11.1 million AFDC recipients receiving benefits each month.

ID for Benefits

It is evident that a wide variety of documents are acceptable for the initial identification of AFDC applicants. The types of documents accepted and the number of respondents accepting them follow:

1. Birth Certificate.....	22
2. Social Security Card.....	16
3. Drivers License.....	14
4. Welfare ID (if former recipient).....	7
5. Credit Cards.....	6
6. Employer Identification Card.....	10
7. Selective Service Card.....	10
8. Military Identification Card.....	10
9. Military Discharge Papers.....	13
10. Food Stamp ID.....	8
11. Union ID Card.....	8
12. Immigration and Naturalization Documents...	17
13. Baptismal Records.....	5
14. Marriage Certificates.....	4

Of interest is the fact that five states returning questionnaires make no attempt to verify an applicant's identity. Some states only require identification to verify the birth of the children for whom assistance is sought, but none for the adult applicant who will also receive assistance. Most jurisdictions rarely, if ever, check the authenticity of "breeder" identification documents.

The importance of an effective identification program is illustrated by a report¹ of the Office of the New York State Comptroller.

The New York Legislature, according to this report, mandated that the New York City Human Resources Administration issue photo identification cards to all recipients of public assistance in the AFDC program. "The primary purpose of the Photo ID was to (reduce or) prevent the cashing of lost and stolen checks."

¹Audit Report on Photo ID Program, New York City Human Resources Administration, Report No. NYC-22-74, Feb. 15, 1974.

This report found that "as of May, 1973, about 3,000 cases were closed as a result of the Photo ID program. This represented a savings of about \$7.2 million a year in payments to ineligible recipients."¹ This reduction in caseload apparently came about either as the result of fictitious cases being closed or an "unwillingness" to be photographed on the part of some recipients.

ID for Check Cashing

The types of documents accepted as a means of identifying recipients when benefits are obtained (e.g., when AFDC checks are cashed), depends on the criteria established by the banks and merchants who cash the checks. Unfortunately, a significant number of banks and merchants require little if any identification when cashing government checks.² Checks are cashed under the false assumption that government issued checks are automatically "good." Evidence of this can be seen in Figure 1, a chart prepared by the Department of the Treasury, Fiscal Service, Operations Planning and Research Staff in a study entitled "Report on Forged Treasury Checks."

The basis of the Treasury report was a review of all forged checks for which a formal affidavit of forgery was filed with the Treasurer of the United States during the month of August, 1972. A total of 3,978 forged instruments were reviewed. The chart, comparing the types of identification used with the establishments accepting them, reveals that 81.3% or 3,236 forged checks did not contain written evidence on the check that an ID was used at the time of cashing. The study found that "the rate of acceptance of drivers' licenses and Social Security cards as a means of identification is particularly high in department stores and other establishments whereas these identification forms (except for one instance) are unacceptable to check-cashing firms. Also, use of the Regiscope³ as a means of identification is relatively low in commercial banks (4.6%) and department stores (4.1%), relatively high in grocery (24.4%) and liquor (25%) stores, and extremely high in check-cashing firms (66.6%)."

¹Emphasis added.

²See Appendix A, Part 2, Report of the Task Force on Commercial Transactions.

³A device that photographs both the check and the individual cashing the check.

ENDORSEMENTS IDENTIFICATION

Financial/ Commercial Establishment Where Cashed	Driver's License		Social Security		Regiscope Picture		Employment I.D.		Check Cashing Card		All Other Forms ^{1/}		Total I.D. Forms ^{2/}		Items Showing I.D.		Items Not Showing I.D.		Total Items	
	No.	% of Col. 7	No.	% of Col. 7	No.	% of Col. 7	No.	% of Col. 7	No.	% of Col. 7	No.	% of Col. 7	No.	% of Total in this Col.	No.	% of Col. 10	No.	% of Col. 10	No.	% of Total
Commercial Bank	49	18.6	31	11.7	12	4.6	22	8.3	24	9.1	126	47.7	284	30.8	231	19.1	979	80.9	1210	30.4
Grocery Store	17	14.3	17	14.3	29	24.4	3	2.5	10	8.4	43	36.1	119	13.9	99	15.9	522	84.1	621	15.6
Liquor Store	5	20.8	3	12.5	6	25.0	1	4.2	-	-	9	37.5	24	2.8	22	13.5	141	86.5	163	4.1
Check-Cashing Firm	1	5.6	-	-	12	66.6	-	-	1	5.6	4	22.2	18	2.1	18	16.5	91	83.5	109	2.8
Department Store	14	28.6	8	16.3	2	4.1	6	12.2	2	4.1	17	34.7	49	5.7	38	32.8	78	67.2	116	2.9
Other Estbm. ^{3/}	6	33.3	4	22.2	2	11.1	-	-	-	-	6	33.3	18	2.1	18	8.6	192	91.4	210	5.3
All Others	17	16.3	14	13.5	14	13.5	8	7.7	2	1.9	49	47.1	104	12.2	92	13.6	585	86.4	677	17.0
Total Legible Items	109	18.2	77	12.9	77	12.9	40	6.7	39	6.6	254	42.6	596	69.6	518	16.7	2588	83.3	3106	78.1
Items Not Legible	44	16.9	20	7.7	10	3.8	13	5.0	1	.4	172	66.2	260	30.4	224	25.7	648	74.3	872	21.9
Total Items	153	17.9	97	11.4	87	10.2	53	6.2	40	4.7	426	49.8	856	100.0	742	18.7	3236	81.3	3978	100.0%

^{1/} Covers all other forms of I.D. presented, including principally military I.D. (32), Credit Cards (17), Fingerprints (7), voter card I.D. (7).

^{2/} The total number of I.D. forms presented is greater than the number of items bearing I.D. information because in 114 cases two forms of I.D. were shown on one item.

^{3/} Covers six other types of establishments, each cashing more than ten checks, as follows: Gasoline Stations (55), Drug Stores (54), Bar (44), Savings & Loan Associations (36), Realty Firm/Housing Authority (11), and Nursing Home (10).

Figure 1 — Establishment Where Checks Cashed Relative to Identification Shown

AFDC Fraud

The survey requested specific information on the extent and impact of AFDC identification-related fraud. Data requested included the number of fraud cases investigated in which false ID was used, the fiscal impact of the fraud, estimates of the percentage of total AFDC frauds that involve false ID, administrative costs of prosecuting false ID, and types and use of false ID encountered.

Twenty-three of twenty-eight responses to all these queries left the questions blank or stated that the information was either not available or unknown. The states supplying some of the requested information estimated that less than 2% of AFDC fraud cases involved the use of false identification. However, one state readily admitted that because fraud reports do not generally specify the nature of the fraud, true percentages are likely to be much higher. As a result, the Task Force has concluded that the frequency of the use of false identification remains undetermined because of the lack of adequate information at all levels of government and the private sector.

Because of the dearth of information, it is necessary to turn to specific welfare fraud reports in order to demonstrate the seriousness of the false identification problem. It should be pointed out that the available reports are not limited to obvious problems of false identification, but include numerous other fraudulent practices such as forgery, which is a false ID crime, the check itself being the false ID. It is abundantly clear that if proper identification is required at the time a public assistance check is cashed, millions of dollars can be saved annually.

The Mail Theft Issue

One of the most serious problems encountered by jurisdictions that mail checks to welfare recipients is mail theft. A Pennsylvania study¹ has found that "Pennsylvania welfare checks are stolen with much greater frequency" than any other checks sent by mail. A prime reason for this is due to the length of time it takes Pennsylvania to complete an investigation on reports of lost or stolen checks. In September and October, 1974, it was found that investigations of

¹Report of the Federal Grand Jury for the Eastern District of Pennsylvania on Welfare Check Theft and Fraud in Pennsylvania and the Administrative Processing of Pennsylvania Welfare Recipient Complaints on Non-Receipt.

non-receipt complaints currently in progress in the Philadelphia area were for "checks issued in July of 1971." It should be noted that similar delays are common in many of the larger metropolitan areas throughout the country.

Most states, including Pennsylvania, upon receiving a report of a lost or stolen check, have the recipient complete an affidavit and issue a replacement check within twenty-four or forty-eight hours. These affidavits are used as the basis for collecting information to be used in any subsequent investigation. The Pennsylvania Grand Jury found that the majority of non-receipt claims cannot be resolved after a search of the files of the State Treasury Department. Statistics indicate that "approximately 41% of the cases are determined to involve checks that have been stolen or forged." Another 20% of the cases are determined to constitute fraud, that is, a check was received and cashed by the welfare recipient but subsequently reported as lost or stolen, in order to obtain a double payment. A study by the New York State Comptroller¹ found that over thirty percent of the checks for which replacements have been issued are subsequently determined to have been fraudulently cashed.

These percentages are shocking when one considers the number of replacement checks issued. The Pennsylvania Federal Grand Jury found the following:

"For the month of January, 1971, the incredible total of over twenty-six thousand replacement checks was issued in Philadelphia alone. Since the average welfare check amounts to approximately one hundred and eight dollars, the value of these replacement checks was more than two million six hundred thousand dollars. In 1972 and early 1973, ten thousand replacement checks, totalling over one million dollars, were being issued each month in Philadelphia alone. That figure is currently reduced to four or five thousand replacement checks per month, with an approximate value of one-half million dollars. This reduction, however, should not lull us into believing that there has been a proportionately great reduction in the rate of theft of welfare checks. The continued and diversified enforcement efforts of the

¹Audit Report on Fraudulent Duplicate Check Claims, New York City Human Resources Administration, NYC-50-74.

Postal Inspectors and some improvements in the processing of these checks have reduced the theft rate. However, most of the reduction of monthly replacement checks from twenty-six thousand to five thousand is the result of a substantial reduction in the number of checks being delivered by the mails."

The Fraudulent Duplicate Check Claims audit in New York City revealed that in fiscal year 1974, the City's public assistance payments were approximately \$1.2 billion. The audit found that "during the year ended October, 1973, HRA (Human Resources Administration of New York City) replaced 310,000 checks worth \$28 million which had been reported lost or stolen." They also found that "as of November, 1973, there was a backlog of 110,000 fraudulently cashed checks worth \$9.7 million on which no recoupment action had been taken."

These figures are substantiated by the Report on Investigation of Welfare Fraud by Office of the Queens District Attorney for the Year 1974. This report states that "the most serious problem faced in the administration of Public Assistance and one for which there are no adequate present safeguards is the multiple collection of welfare payments by people using several aliases." The report further states that "it appears that the only way to eliminate this type of welfare cheating is to require a form of identification which is absolutely unique to each individual and which is not capable of fraudulent duplication."

A recent article in the Washington Post on check thieves and their victims, with emphasis on federally issued checks, indicates that upwards of \$15,000,000 are lost due to forgery. The article stated:

"The check thieves steal about \$50,000 a day by forging government checks. Most of those direct losses are carried by the banks and businesses that cash the forged checks. The indirect costs borne by various government departments that investigate and replace the stolen checks runs into the millions each year."

A recent review conducted by the New York State Office of Audit and Quality Control showed that welfare checks issued by the State of New York alone account for \$12,000,000 in fraudulently cashed checks each year. It is likely that if similar studies were made of fraudulently cashed government checks issued in other major metropolitan areas across the county, these figures

would double or triple. It is unlikely that the New York and Philadelphia metropolitan areas are the only ones experiencing these problems.

False ID Suspect Profile

The most common characteristics of individuals who have come under investigation for using fraudulent identification in order to obtain AFDC benefits are as follows:

1. 20-30 years of age;
2. Female;
3. Unemployed;
4. Has completed 12 years of education;
5. Resides in a metropolitan area;
6. The fraud occurred in a metropolitan area;
7. Had no prior criminal record; and
8. Has resided in present residence six months.

Apparent thus far is the fact that the amount of detectable fraud is commensurate with the effort made to detect it. As an example, of 343 cases sent to the prosecutor by the Special Investigative Section of the Department of Social and Health Services in the State of Washington, 338 or 98.5% resulted in guilty verdicts. This occurred in the first year of their operation beginning August, 1973. The annual report of the Special Investigation Unit for Suffolk County, New York, stated that "as a result of activities by the Special Investigation Unit in the year 1974, over one million dollars in fraud was uncovered, and resulted in an additional savings to the County of \$900,000 in Public Assistance cases being closed."

The Treasury Department¹ expresses the frustration of those in government concerned with the fraudulent cashing of checks and the question of proper identification. They state:

"It is apparent that check-cashing establishments, and particularly banks, do not take proper precautions. They are accepting checks (in some cases for large dollar amounts) with questionable endorsements and

¹"Report on Forged Treasury Checks," Department of the Treasury, Fiscal Service Operations Planning and Research Staff.

forms of identification which are not, obviously, reliable. It is entirely conceivable that strict observance of the simple maxim 'Know your endorser - require identification' would reduce substantially the incidence of encashment of stolen and forged Treasury checks."

Medicaid

Sources of Information

Twenty-six responses to the questionnaires on the use of false identification to obtain Medicaid benefits have been received by respondents representing twenty-four states, one county (Los Angeles) and one territory (Guam).

Analysis of Data Received

While all states issue some form of Medicaid identification card and/or Medicaid labels, the conclusion that must be drawn from the responses received is that states have little, if any, knowledge concerning the use of false identification in the Medicaid program. A common response is that states are "not required" to keep Medicaid fraud statistics and, therefore, do not.

The states that did provide some information indicate that the problem appears to be more in the nature of provider fraud rather than recipient fraud. One state that found some recipients using Medicaid cards belonging to other persons discovered that in most instances the imposters were themselves eligible for Medicaid or other medical assistance but had lost or mislaid their own Medicaid ID.

The Task Force is, therefore, unable to provide any meaningful data relative to the use of false identification in obtaining Medicaid benefits.

The Task Force believes that states should be required to maintain uniform and detailed statistics on Medicaid fraud. In addition to providing meaningful national data, such statistics would serve as administrative tools for corrective action at all government levels.

Food Stamps

Sources of Information

The Food Stamp questionnaire was mailed to Welfare Departments of all U.S. states and territories. Twenty-four responses have been received; respondents represent twenty-two states, one county (Los Angeles), and one territory (Guam). Maryland's response consisted of twelve separate questionnaires filled out by officials of as many counties.

The Normal Process

The Food Stamp application process begins when an individual or family applies for benefits at a local or state welfare office (in many urban areas, community service organizations serve under contract to the state as registration offices). Eligibility for Food Stamp benefits is limited to U.S. citizens and legal aliens in permanent residence and is based on income level, number of dependents, and certain other eligibility requirements. Recipients of federally-supported state assistance programs such as Aid to Families with Dependent Children (AFDC) are automatically eligible for Food Stamp benefits. If the local registration office is satisfied that the applicant meets eligibility criteria, the application is forwarded to an office of the state welfare department for a final determination. Upon a favorable determination, the applicant is provided with a Food Stamp ID card and (in most states) his first Authorization to Purchase (ATP) card. The Food Stamp ID is usually not a photo ID card; in Massachusetts, for example, it is a machine-readable card containing the applicant's name, Social Security Number, and signature. The name and signature of an authorized proxy may also appear on the card. The ATP document is also a machine-readable card containing the authorized face value of food coupons to be purchased and the purchase price. The purchase price is determined by the need of the applicant and ranges from zero to slightly less than the face value of the coupons. Food Stamps may be purchased at state-authorized outlets, which are usually banks but may be retail stores or community service agencies. The "stamps" (more properly coupons) are issued by the federal government. ATP are presently issued monthly; revalidation, which entails redetermination of eligibility and issuance of a new Food Stamp ID, is required every three months.

ID at Registration

It is apparent that there is no nationally-accepted standard for identification of Food Stamp applicants upon registration.

Eight states require no identity documents at this point. Fourteen of the twenty-six respondents accept a Social Security card as identification at registration; nine accept a driver's license, and eleven accept immigration and naturalization documents. Several respondents noted "if applicable" on immigration documents, implying that selection was exercised in demanding proof of citizenship. One respondent (a Southwestern state) indicated that ID was required "only if citizenship is questioned." All the documents suggested as choices¹ are accepted by at least three of the respondents. Other documents not listed but accepted by one or more respondents include library cards, income documents, bills, and "personal papers." Some of the respondents indicated that the responsibility of the state agencies is to determine the eligibility and need level of the applicant, not his true identity.

ID for Claiming Stamps

The standards for identification of recipients picking up Food Stamps in person are apparently tighter and more uniform than those applying at registration. Twenty-three of the twenty-six respondents accept a current Food Stamp ID at this point; several respondents accept only this document for Food Stamp pickup. Ten respondents would accept the Food Stamp ID of a former recipient, six a driver's license, and five a current welfare ID. Only one² respondent indicated that most of the documents listed as choices² are accepted; none indicated that no ID is required for Food Stamp pickup.

ID for Food Purchase

The Food Stamp ID was also most frequently mentioned (nineteen responses) as the usual document required when Food Stamps are used to purchase food. Nine respondents indicated that an old Food Stamp ID would be accepted. Four respondents stated that the required ID would depend on the "sales outlet" at which the stamps were used, while two believed that no ID is usually required by food stores.

Food Stamp Fraud

Specific information was requested to the extent and impact of Food Stamp Fraud. The number of fraud cases investigated in which

¹The list of suggested documents appears in the description of AFDC programs in this report; current and expired Food Stamp ID's were added to this list.

²Same as suggested for Food Stamp application.

false ID was used, the fiscal impact of the fraud, estimates of the fraction of total Food Stamp frauds that involve false ID, administrative costs of prosecuting false ID, and types and use of false ID encountered. Unfortunately, the most common response (ten of twenty-six) to all these queries was "Information Not Available." One respondent's comment summarized the apparent attitude of many state welfare departments: "No record kept (of this type of information) since there is no requirement to do so." Almost as common (nine responses) was the comment that false ID fraud is nonexistent in the respondent's jurisdiction¹. This was not only the response of such sparsely populated rural states as Oklahoma, North Dakota, and Montana, but also of urban states such as Connecticut and Delaware.

Completely in contrast to these responses was the report submitted by the State of Arkansas. This report covered only Non-Public Assistance Food Stamp recipients in North Pulaski County, which includes only 2.5% of statewide Food Stamp recipients. Nevertheless, in FY 73-74, this county (which includes part of Little Rock, Ark.) recorded 57 cases of false ID fraud carrying a loss to the Federal government of \$18,740. All cited cases involved false ID at the time of application; seven cases also included the use of false ID at the time of food purchase. In 31 cases, imposter identification was used; counterfeit identification was used in 24 cases; and altered identification in 2 cases. The state estimated its administrative cost in prosecuting these cases to be \$3500.

The Arkansas data are extremely significant, considering the relatively small sample of Food Stamp recipients that yielded all these cases. Two possible explanations of the data are suggested: either Little Rock, Ark. is a hotbed of false ID fraud, or the problem is being overlooked (and therefore declared nonexistent) in most of the nation. Some additional information, quoted from the Arkansas response, suggests that the latter explanation is more nearly correct:

"Since April 1974, the prosecuting attorney in Pulaski County has been extremely concerned with all aspects of recipient abuse of the Food Stamp Program and has been very active in the prosecution of food stamp fraud cases. To date, three hundred and ten (310) felony charges of false pretense have been filed against one hundred and

¹If no records are maintained, it is questionable as to whether such a statement can be given much credence.

twenty-seven (127) persons in Pulaski County. Thus far eleven (11) persons have been found guilty with sentencing ranging from five (5) years in the State Penitentiary to one (1) year suspended."

Substantive data on false ID fraud was also received from Los Angeles County, California. However, no special breakout for Food Stamp fraud could be provided: the figures given refer to welfare fraud of all types. False ID fraud cases investigated increased from 24 in FY 70-71 to 103 in FY 73-74. Estimated welfare and Food Stamp payments to recipients as a result of this fraud totalled \$24,170 in FY 70-71 and \$85,148 in FY 73-74.

Common ID Fraud Documents

The documents most frequently used in false ID fraud in Arkansas are Social Security Cards and Food Stamp ID documents. Social Security Cards are obtained by application under one or more false names; unofficial "permanent" Social Security cards made of aluminum are obtained by mail order and sometimes used as ID documents. The most frequent abuse of the non-photographic Food Stamp ID is the "loan" of it to unauthorized parties who then use it in purchasing Food Stamps. Apparently, the intermediate ATP document is not used in Arkansas.

California listed baptismal and birth certificates and driver's licenses as the most frequently abused ID documents. Birth certificates are commonly used to support the existence and ages of claimed dependent children; blank baptismal certificates are available in stationery stores, while birth certificates are most frequently genuine documents that are altered and then photocopied. Most of the driver's licenses used in false ID fraud in California were counterfeit documents.

False ID Suspect Profile

Arkansas and California showed good agreement in their profile of the typical suspect in false ID investigation; both identified a young (18-30) unemployed woman resident in a metropolitan area. California described the typical suspect as not having a prior criminal record, while Arkansas could not supply data on prior criminal records. Both states cited metropolitan areas as the most common locales for ID fraud.

Extent of the Problem

None of the twenty-six respondents to the Food Stamp survey indicated a belief that false ID fraud represents a majority of total Food Stamp fraud cases. However, the Arkansas response, which contained the most detailed data on false ID fraud, estimated the proportion of false ID cases as 10% of the total fraud cases. Much more common methods of fraud include falsification of income, medical expenses, or number of dependents. In Los Angeles County, the percentage of welfare fraud cases investigated that involved false ID was less than 1% for all years reported (FY 70-74 inclusive). Estimates of false ID fraud as percentages of total Food Stamp fraud supplied by other respondents ranged from below 1% to 5%; no basis for these estimates was given.

Analysis of ID Fraud Data

These estimates establish clearly that the use of false ID is perceived as a minor problem with respect to overall abuse of the Food Stamp program. Three comments, however, appear to be in order. They are: (1) Based on the wide variance of the Arkansas response from the national sample, false ID fraud is probably much more widespread and considerably more frequent than most state welfare departments realize; (2) All of the methods of false ID use that were detected are very primitive. This includes the unauthorized use of Food Stamp ID, phony or duplicate Social Security Cards, and counterfeit driver's licenses; and (3) More sophisticated methods of false ID (such as Infant Death Identity)¹ could be in widespread use but not currently detected.

Disposition of Cases

Cases of Food Stamp fraud, when discovered, are referred to the local prosecutor's office (usually county-level) for disposition. The cost-sharing provisions of the Food Stamp program do not provide a strong incentive for state and local prosecution of Food Stamp fraud; in fact, they provide the states with a strong disincentive. The states pay a portion of the administrative costs of the program, including costs for the apprehension and

¹See Part I, Section 3 of the FACFI Final Report.

prosecution of offenders. The entire cost of the coupons fraudulently obtained, on the other hand, is borne by the Federal government. Therefore, added emphasis on fraud results in added costs to the state, yet all funds recovered must be returned to the Federal government. Stolen or forged Food Stamp ID and ATP cards can be used at banks and retail stores to obtain and "spend" coupons where no effort is made to confirm the identity of the bearer. The Food Stamp ID used in most states is not a photo ID and can, in certain cases, be used by a proxy to purchase coupons for a designated recipient. These characteristics make it relatively easy to counterfeit or to use if stolen. Federal guidelines for state action (FNS [FS] Instruction 736-1) make it extremely unlikely that states will elect to prosecute any but the most flagrant abusers of the Food Stamp program. Finally, several respondents to the Food Stamp survey indicated that communication is poor between state and local welfare officials regarding abuses of the Food Stamp program.

Suggestions for Solutions

Several suggestions were made by survey respondents to consider the problem of false ID fraud. Establishment of a photo ID system was the most common suggestion. One respondent, however, in making this suggestion noted that this "would be one more harassment to Food Stamp Program participants." One state suggested that others follow its practice of mailing Food Stamp ID and ATP documents in separate envelopes; this makes it more difficult for a thief to obtain both documents. One respondent preferred the (apparently older) FS-4 form to the ATP card "since the former permits close control over currency of ID." The Arkansas respondent suggested requiring more than one form of ID at intake to the program. Finally, one respondent appealed to the Federal government to "simplify program specification to free workers to perform other tasks, such as checking ID!"

An overall view of the responses suggests the need for some uniform type of identification requirement to be used at application. Application frauds using counterfeit or imposter identities appear to be the most common types of known ID fraud. The Social Security card was mentioned most frequently as a document used in false ID fraud; until recently it has been very easy to obtain Social Security cards under assumed identities. It remains to be seen whether new regulations by the Social Security Administration will have a long-range effect on the false ID problem. For the present, acceptance of the Social Security card

alone as an ID for the Food Stamp program should certainly be discouraged. More fundamentally, there is a need to restructure the balance of state and Federal responsibilities in the Food Stamp program to improve the efficiency of its administration and to discourage abuses of the program.

Social Security Programs

Sources of Information

The Social Security questionnaire was sent to appropriate Social Security Administration bureaus, including those responsible for Supplemental Security Income (SSI), Health Insurance (HI), Disability Insurance (DI), and Retirement and Survivors Insurance (RSI). In addition, copies were sent to the Division of International Operations (RSI) and the Documents Analysis Laboratory in the Office of Administration, a rich source of information. It was the opinion of the Laboratory Chief that "false identification" is a very small part of the false documentation problem at the Social Security Administration.

The Normal Process

Social Security programs are unique among those considered by the Government Payments Task Force in that a large majority of the working population of the U.S. is registered for benefits under these programs. Registration or opening of a Social Security Account typically takes place upon an individual's first application for salary or wage paying work. Prior to 1974, little or no documentary evidence of identity was required to register for Social Security benefits. There is some evidence of multiple registrations under a variety of aliases, a procedure which can enable the collection of multiple benefits. The Social Security Administration instituted procedures in 1974 calling for presentation of documentary evidence of identity upon registration.

Once registered, an individual in covered employment is subject to withholding of Social Security contributions; similar contributions are required of employers. Federal law requires that any change affecting contributions to the program, such as marriage and acquisition or loss of dependents, be reported promptly to the Social Security Administration.

Application for benefits, as distinct from registration, normally occurs when an individual enters a status eligible for benefits. Eligible circumstances include retirement after age 62,

permanent disability, blindness, and for survivors, the death of a covered wage earner. Documentary evidence of eligibility must be presented with the application for benefits. However, no investigation of the claim is usually made unless there is some reason for suspicion. Referrals of possible fraud in Social Security cases generally originate from voluntary informants.

ID Required

Only the birth certificate and Social Security card were listed by all components as being accepted for initial determination for eligibility. The Supplemental Security Income Program appears to accept more types of documents initially than any other bureau of the Social Security Administration.

The types of documents shown as an acceptable means of identifying recipients when benefits are obtained, either when checks are cashed or services received, are varied. All four bureaus indicated that documents such as driver licenses, marriage certificates, credit cards, etc., are used. In fact, only two types of identification mentioned on the questionnaire that were not used by any bureau were the Welfare ID and the Food Stamp ID. From these statistics, it appears that the most common document used for identification purposes is the driver's license which is easily obtained, altered, and forged. Another in common use is the Social Security card which was never intended to be used for identification purposes.

Social Security Program Fraud

The most common response to fraud impact question was "information not available." The survey yielded a total of only 56 cases investigated for fraud in the four fiscal years 1970-1974 that involved the use of false identity. Of these, 17 cases were classified as altered ID, 5 as counterfeits, and 21 as imposter cases; classification was not made for the other 8 cases. No records of fraud based on false identity have been kept by the Disability Insurance Bureau.

In response to Question F, number of cases in which applicants for benefits were refused benefits because they could or would not provide identification, the Bureau of Health Insurance stated that in their program, services could conceivably be performed in emergency situations even if an individual did not have his health insurance identification card. They pointed out, though, that the physician or provider may not be able to collect from

Medicare if it develops that the patient was not entitled to the services performed. All other respondents indicated that they were not aware of any cases.

It was generally agreed among the respondents that it cannot be assumed that if identification is required, fraud has not taken place. In most cases, if a person decides to file a false application he would also have obtained false identification. In addition, it is not always possible to detect the fraudulent act unless a complete and extensive investigation is initiated when the claim is filed. In many cases, the fraudulent act is detected by reports from informers or through development of the initial claim, a subsequent claim, or a post adjudicative discrepancy.

Relative to administrative costs and manpower resources for fraud investigation involving false identification, it appears that only a very small percentage of time is spent on the problem of false identification. In fact, 5 percent or less of all cases examined for possible fraud by the Document Analysis Laboratory at the Social Security Administration involve false identification. These cases usually do not involve attempts at false identity. Rather, the individual has attempted to change certain facts about himself for personal benefit. For example, he may attempt to show that he is older than he actually is in order to qualify for retirement benefits.

False ID Techniques

The most common techniques for obtaining fraudulent identification as reported were:

1. File several Forms SS-5 (Application for a Social Security Account Number) using completely different identifying information on each application (i.e., different name, parent's names, place of birth, birth date). When application is made on the various account numbers, a false birth certificate or affidavit supposedly signed by the parent is used;
2. Find or steal another person's Social Security card;
3. Applicant, who may be receiving wife's or widow's benefits, can file for retirement insurance using maiden name and falsely state that she had not previously filed for benefits;

4. An applicant can obtain the birth certificate of a person who died at an early age and then proceed to use that individual's identity to build up another wage record and subsequently file under the new account number;
5. An applicant can assume the identity of a wage earner's legal wife, with the wage earner's knowledge, using the marriage record pertaining to the legal wife as proof of age on the basis of her allegation that this was the only proof of age available;
6. Contact a church and obtain a baptismal certificate of an individual who is not the requester of said certificate;
7. Obtain fraudulent documents from outside the United States from both civil and religious sources, such as local civil registries and church records. It is sometimes possible to bribe the civil or church official to issue fraudulent documents.

False ID Suspect Profile

There was general agreement among all respondents as to the profile of the typical suspect in false ID investigation: most are at least 65, can be either male or female, many are unemployed, with little known regarding their educational backgrounds. There are more cases of attempted use of false identification in metropolitan areas than rural or suburban areas, possibly because little or no identification is required in less populated areas since people tend to know each other better.

Control of Abuse

It is a Federal offense subject to criminal penalties for an individual to furnish false information to the Social Security Administration in connection with the establishment and maintenance of Social Security earnings records, to use a Social Security number (SSN) with false information, to use a counterfeit SSN, or to use someone else's SSN.

There are definite procedures to follow when a beneficiary fails to receive a check. Briefly, a beneficiary reports the non-receipt to the SSA district office which in turn will forward the

nonreceipt allegation to the Treasury Disbursing Center which has responsibility for issuing the payment. At this point, a request is made to place a stop payment in the Treasury system against the original check. If the original check is later presented for payment, the Treasury will make the determination as to the proper method of recovery. When a nonreceipt claim is received and the original check is paid by the Treasury and the check is found to bear an unauthorized endorsement, the Department of the Treasury will request directly the refund of these payments.

Suggestions for Solutions

Several suggestions were made to counter the problem of false ID fraud. The use of the Social Security numbers as a universal identifier was the most common suggestion. However, this has already been considered in terms of the danger of invasion of privacy, the cost to the Federal Government, the time required to institute the system and the effectiveness of such a system for alleviating the problem. The use of the number for such a system seems unlikely at this time. Other respondents suggested that more specific care should be taken in identifying the claimant. They further suggested that all documentary proofs should be examined carefully. If any document appears altered or not authentic, a Document Specialist should be requested to verify the document. When fraud is suspected, development of the fraud aspects should be started quickly. Another suggestion was the universal use of one or more corroborating documents, rather than the use of only one. Along these lines, an applicant for a Social Security number must show convincing evidence of identity. Preferably, the evidence will show his age or date of birth, his address, and his signature, and be at least several months old. Still another common suggestion was that all individuals applying for Social Security numbers could be fingerprinted when applying for benefits in order to establish their identity. This too would probably be unfeasible and not readily accepted by the public.

SECTION III

PRELIMINARY RECOMMENDATIONS

General

The Government Payments Task Force presents in this section a list of preliminary recommendations to reduce the incidence of false ID fraud in the programs studied. These recommendations were developed from survey responses, by individual Task Force members after a review of survey findings, and by other individuals with whom Task Force members had contact. It should be emphasized that these recommendations represent individual viewpoints and do not necessarily reflect the opinions of all Task Force members. The recommendations have also not yet been screened, compared, and examined with respect to such criteria as cost effectiveness, practicality, and likelihood of public acceptance. Since detailed management of cost-shared welfare programs, including AFDC, Medicaid, and Food Stamps, is relegated to individual states, while Social Security is a strictly Federal program, recommendations have been divided into those that apply to state and Federal governments.

Recommendations to State Government

1. Provide a tamper-proof identification card which may be used for all assistance programs in the state, (i.e., AFDC, Food Stamps, SSI, HI, DI, and RSI). It is suggested that this ID card, as a minimum, contain the following information:
 - a. Name and address of recipient (embossed);
 - b. Social Security Number of recipient (embossed);
 - c. Case or other state number (embossed);

Note: This number should correspond with a case number and/or Social Security Number included on the assistance check, Food Stamps, etc.
 - d. Color photograph of recipient large enough to cover at least one-half of one side of the card;
 - e. Signature of the recipient;

- f. Name and telephone number of the office issuing the card;
 - g. The right and left thumb print of the recipient;
 - h. Issuance and expiration date of the card;
 - i. Any other data necessary to satisfy requirements of the program for which the card is issued; and
 - j. A postage free return mailing statement and a warning, in bold type, of the consequences of misuse of the card. The card should conform to standard credit card size so that it can be used in credit card embossing machines.
2. Consider requiring merchants and others who cash public assistance checks to impress the embossed information from the ID card onto the check prior to cashing (i.e., similar to the use of credit cards);
 3. Consider sending or transmitting electronically public assistance checks to conveniently located banks where recipients would be required to personally claim and sign for their benefits. This would make it practically impossible for a recipient to obtain a replacement check by falsely claiming that he did not receive the original. This would also substantially reduce the problem of assistance checks being stolen from the mails. This procedure would probably be more practical in metropolitan areas, which the Task Force surveys have shown to be high-risk areas for false ID welfare fraud;
 4. Recipients should be required to report stolen welfare checks directly to the local police and to sign an affidavit under penalty of perjury before being issued a replacement check;
 5. Identification should be required (ID card as described above) for cashing Food Stamps; merchants should not be paid for fraudulently used Food Stamps;
 6. Penalties for knowingly accepting fraudulently cashed Food Stamps should be made severe;

7. Uniform standards for identification of recipients and claimed dependents at intake should be adopted by all states;
8. The security of "breeder" documents such as birth certificates and driver's licenses should be upgraded so as to resist alteration, counterfeiting, and use by imposters. Steps such as mandatory matching of birth and death certificates and carefully controlled issuance should be immediately implemented.

Recommendations to the Federal Government

1. The Federal government should develop comprehensive standards for recipient identification for cost-shared assistance programs, and provide financial assistance to the states in implementing these standards;
2. The Food Stamp Program should be restructured by legislation requiring state sharing of stamp cost and providing more Federal Assistance in costs of prosecuting Food Stamp fraud. These measures would provide the states with incentives for improved control of this program;
3. Food Stamps should be redesigned to resist use of stolen coupons. One means of doing this would be to provide two signature blocks for recipients. One block would be signed upon the receipt of the stamps and the other at the time of use (i.e., similar to the use of Traveler's Checks);
4. Positive identification of recipients should be required prior to approval of applications for Social Security benefits.

ATTACHMENT I

COMPOSITION OF THE TASK FORCE

The members of the Governments Payments Task Force and their professional affiliations are as follows:

Carl B. Williams, Chairman	Deputy U.S. Commissioner of Welfare, U.S. Department of Health, Education and Welfare
Laurence J. Love, Cochairman	Attorney, Office of the Secretary, U.S. Department of Health, Education and Welfare
George Berlinger	Port Authority of N.Y. and N.J.
Richard DeMeo	Social Security Administration
Peter Kimball	American Bank Note Company
Paul Lamberth	U.S. Department of Agriculture
Robert Magee	U.S. Department of Agriculture
Theo Manos	Polaroid Corporation
Leon Walters	Social Security Administration
<u>Staff Assistant</u>	
Thomas Kabaservice	The MITRE Corporation

APPENDIX A2

**REPORT OF THE COMMERCIAL TRANSACTIONS TASK FORCE
ON THE
SCOPE OF THE FALSE IDENTIFICATION PROBLEM AND
PRELIMINARY RECOMMENDATIONS FOR SOLUTIONS**

Submitted to

**Federal Advisory Committee On False Identification
David J. Muchow, Chairman**

May 1976



TABLE OF CONTENTS

	<u>Page</u>
SECTION I - INTRODUCTION	A-39
Purpose	A-39
Scope	A-39
Data Gathering	A-39
Evaluation of Data	A-41
SECTION II - THE FALSE ID PROBLEM	A-43
General	A-43
Losses Sustained	A-43
Type of False ID Used	A-44
Types of Fraud	A-45
Encashment of Checks Stolen From the Mails	A-46
Social Obligations - Impact on False ID Fraud	A-48
False ID Involvement	A-50
Bank Card Fraud	A-50
National Association of Securities Dealers Survey	A-53
National District Attorneys Association Survey	A-54
Recommendations	A-55
SECTION III - PRELIMINARY RECOMMENDATIONS	A-57
General	A-57
Recommendations From Business and Banking Representatives	A-57
Technical Devices	A-58
Employee Training	A-59
Credit and Bank Card Measures	A-60
The Dilemma	A-61
Current Countermeasures	A-62
For the Future	A-63
Recommendations From Law Enforcement Representatives	A-65
REFERENCES	A-69
ATTACHMENT I - COMPOSITION OF THE TASK FORCE	A-71
ATTACHMENT II - SUMMARY OF MATERIAL IN TASK FORCE FILES	A-73

Report Of The Commercial Transactions Task Force

On The

Scope Of The False Identification Problem And

Preliminary Recommendations For Solutions

SECTION I

INTRODUCTION

Purpose

The Commercial Transactions Task Force of the Federal Advisory Committee on False Identification has identified its central concern as the fraudulent use of personal identification in its primary form: over-the-counter sales and bank transactions.

Scope

In order to structure the investigation in a useful and practical way, a model for a commercial transaction has been selected. It is a one-time, face-to-face encounter between a businessman or banker and an individual who wishes to procure goods and/or services using credit or a check, and who remains at the point of sale for only a few minutes. It is recognized that securities and other brokerage transactions generally do not fit into this model because of extensive federal and self-regulatory requirements governing the opening and maintenance of customers' accounts including the strictly applied "know your customer" and suitability rules. Security transactions are not therefore usually executed as a result of a "one time, face to face encounter. However, the model is intended to represent the vast bulk of commercial transactions: those in retail establishments and bank offices. The Task Force has, accordingly focused on the following commercial instruments: checks including Traveler's Checks, Bank Cards, and Securities.

Data Gathering

The main sources of information and statistical summaries used in this report were the business and trade organizations and agencies of government and the law enforcement community most closely concerned with frauds which include false ID. Not the least of the resource available to the Task Force was the personal experience and expertise of the members themselves and that of their associated organizations.

Specific sources of information are noted below.

Reports on the scope of the false identity problem were submitted from the following organizations:

American Express
National Association of Securities Dealers, Inc.
Interbank Card Association
Metropolitan Police Department
U.S. Postal Inspection Service
American Bankers Association
National District Attorneys Association

The following organizations conducted formal surveys:

American Bankers Association
National Association of Securities Dealers, Inc.
American Express
National District Attorneys Association

The following have conducted analyses and/or contributed a sampling of records available to them:

Interbank Card Association
Metropolitan Police Department
U.S. Postal Inspection Service

Summaries of the above surveys and analyses are attached to this report. Reference is also made to the following periodicals for a substantial concurrence with the surveys and analyses:

Protection Management & Crime Prevention

Richard B. Cole
(W. H. Anderson, Co.)

White Collar Crime

Chamber of Commerce of the United States

The National Notary, January/February, 1975

(Commercial)

The Cost of Crimes Against Business

U.S. Department of Commerce

Identification With & Without Credentials

American Bankers Association

Evaluation of Data

The fact that the Task Force is composed of representatives of both law enforcement and business communities led to some disparities in the perception of the false identification problem and in the types of solutions seen as appropriate to the problem. The difference in viewpoint between law enforcement and business interests has been expressed as follows by Task Force Co-Chairman Nathaniel Kossack:

"In short, the commercial sector is sensitive to the nth degree to cost effectiveness of remedies, which does not permit them to go beyond the recognition of the ratio of losses to the total amount of business. Remedies suggested by business include operational corrections only and do not include referrals to law enforcement which are made routinely. The law enforcement sector has placed the crime of false identification and the crimes using false identification on a low level of priority and have downgraded the traditionally poor "white collar" crime record system to an even lower status. For example, 'paper hanging' is the popular term for check passing and law enforcement tries to avoid the enveloping morass of its volume. Lastly there is an instinctive mutual mistrust between law enforcement and business built up by reason of the conditions of the problem. Commerce complains that law enforcement won't 'protect' them in these cases which can potentially flood the prosecutor's office. Law enforcement does not trust the standards of care (or lack of care) used by commerce and terms the neglect scornfully as 'cost of doing business.' All in all the condition creates a very unsatisfactory record by another artificiality--the anonymous 'third party' victim. That is, the banks do not consider check forgery an important source of loss. The merchant minimizes the loss because he is insured or takes a tax deduction. Like matter, the loss does not disappear; it is merely transferred down the line."

The difficulty of obtaining complete statistical information was also stressed by co-chairman Hollis Bowers in submitting a report to the Task Force on behalf of the business and banking community prepared by himself and Edward Smith, Assistant Director, Communications Group, American Bankers Association:

"There are as many different statistics on fraudulent commercial transactions involving the use of false identification as there are sources of statistics. Generally speaking, there is a paucity of empirical information as experience following creation of this Task Force has shown that more often than not a commercial enterprise will show losses based on the instruments presented, e.g., checks, without recording the forms of identification used to establish lawful possession of the check instruments. It is believed, however, that the figures cited in this report best represent the presently known situation. In absolute dollar figures the losses due to fraud are tremendous; when averaged out against astronomical bona fide transactions, they seem less imposing. No matter how they may be regarded, the facts and figures reported herein confirm that the commission of the crime using false identification poses a problem for America's bankers and executive, and judicial branches of local, federal and state governments as best they can within the constraints of social, cultural, and business life in the United States. The recommendations in this report are framed within the real-world limitations of business and banking, and are believed to represent the best possible solutions to the problems of false identification and crime in commercial and banking transactions, given today's business and banking environment."

The description of the false identification problem was constructed from information supplied by members of both business and law enforcement communities. However, the difference in viewpoints is recognized by the presentation in Section III of this report of different sets of preliminary recommendations by the two communities.

SECTION II

THE FALSE ID PROBLEM

General

Commercial transactions take place in a wide variety of locations, ranging from securities houses and stock exchanges to retail and service establishments to the offices of financial institutions. No matter where commercial transaction takes place, however, if the transaction is fraudulent, false identification may be used to add plausibility to an individual's claims and thus to make the transaction possible.

Losses Sustained

Losses resulting from such fraudulent transactions are normally borne by the individual or business that first accepts an invalid instrument, be it a forged check, a check written on insufficient funds or a stolen, altered or counterfeited credit card or security certificate. Thus, the brunt of these losses is suffered by businesses rather than by banks; while a bank may ultimately identify a check as having been forged or a credit card as having been stolen, the loss in the transaction is more often that of the business. Only when a bank is the first acceptor of a fraudulent or invalid check or credit card does the bank itself suffer financial loss.

In dollar terms, this distinction is most apparent. Extrapolating from the results of a 1972 survey, the American Bankers Association (ABA) estimates that in 1974 bank losses due to forgeries totaled approximately \$50 million. If that figure is divided by the number of bank offices in the nation (more than 40,000), forgery losses came to only \$1,250 per banking office for the year. Significantly, a study of bank operating losses by the Audit Commission of the Bank Administration Institute set 1973 check losses at \$45,447,000. Even if these figures were doubled the average per banking office would be quite low. Actual losses certainly vary from bank to bank, depending upon such things as a bank's size, the variety of its services, the quality of its employee training programs, the uniformity of its policy enforcement, the number of transactions in which it is involved, etc. It should be noted also that the number of forgeries reported each year is growing, and to these should be added a broad assortment of other fraudulent "paper" transaction schemes.

In a recent ABA study, stolen and forged checks accounted for the largest proportion--32.4%--of the check fraud schemes. Other

check fraud schemes in the order of their occurrence were: counterfeit checks, 23.8%; stolen blank checks, 16.4%; starter checks, 12.5%; split deposit, 9.4%; and others, 5.5%. Retail businessmen estimate bad-check and credit card losses have been approximately \$4 billion annually; however, the basis for this figure is not known. Based on 1967 census of business, the U.S. Chamber of Commerce estimates that there are more than 1.6 million business establishments in America. . Thus, average annual business loss per establishment are approximately \$2,500. Again, individual businesses' losses vary from operation to operation, just as is the case with banks.

Type of False ID Used

In a recent ABA study, the Insurance and Protection Division investigated the fraudulent check schemes reported in state bankers association warning bulletins in 1974. One part of the study dealt with the frequency of various types of false identification. The type of false identification used most often--in 86.35% of the cases--was impersonation. It was not possible to establish subdivisions of impersonations because of the lack of detail in the reports. This lack was attributed to 2 factors. First, 72.6% of the check fraud checks involved counterfeit checks, stolen blank checks, or stolen and forged checks. In these cases, a form of identification is seldom requested by the bank teller because the check passer persuade the tellers that he is the lawful owner of the check. Second, banks and merchants seldom document the form of ID used when they cash checks for strangers. If there is some doubt about the ownership of a check, the bank or merchant refuses to cash it there are few if any records of the type of ID in aborted cases.

Other types of false ID, in order of frequency, were: driver's licenses, 8.2%; ID cards and other personal identification, both 2.7%; and social security number, 0.05%.

What forms of personal identification are used in these fraudulent transactions? A driver's license and perhaps a "merchant's" or "major" credit card are frequently all that is requested by a merchant. All too often these forms of personal identification prove to be insufficient to protect the merchant. In other transactions, however, many different forms of false identification may be used, depending often on the relative sophistication of the swindlers and their intended victims.

It should be pointed out that many merchants and service operators face a "point of diminishing returns" in establishing the identity of customers presenting checks or credit cards. Obviously, the merchant who refuses to accept either checks or credit cards is automatically

alienating a significant portion of the buying public. In the same way, excessive caution or a suspicious attitude in verifying a customer's identity can cause offense and the loss of business. Thus, it can be argued that many merchants accept certain risks and losses due to crimes involving false identification as part of the cost of doing business.

In bank transactions, required signature (or other) verification from the bank's own records for an "on us" check, plus personal recognition of the customer, as well as additional methods of verifying identity (such as photo ID, thumbprint, computer check on funds in the account, etc.) help to discourage passers of forged checks, insufficient funds checks (NSF), or split-deposit swindlers. All of these measures contribute to the positive control of banks' losses as result of crimes involving the use of false identification.

Types of Fraud

Check Fraud

Bank Instruments

Americans are now writing more than 25 billion checks a year,³ and the total is expected to exceed 40 billion a year by 1980, in spite of the predicted rapid growth of electronic funds transfer systems (EFTS).⁴

A 1974 Bank Administration Institute (BAI) study entitled "The Impact of Exception Items on the Check Collection System" also helps to add perspective to the scope of the problem of check fraud and related use of false identification.⁵ Of the 25 billion checks written in 1973, the study states,

"return items accounted for approximately two-thirds of one percent of all checks processed--one return for every 150 items processed by each bank ... And of those return items only 12 percent were identified as missends, forgeries, and unlocated accounts..."

The Federal Reserve System, which clears 85 per cent of all checks written in the U.S. on American banks, indicates that approximately 100 million out of 1973's 25 billion checks (1 of every 250) were returned for one reason or another. Of that 100 million, only 25 million finally did not clear--and not all of those were the result of fraud or crimes involving false identification, since customer or bank inadvertence causes some bad checks.

The growth in volume of check-writing in the U.S., as well as the nation's population growth, also helps to put incidence of fraud into perspective.

A 1970 study by Arthur D. Little, Inc., for the American Bankers Association points out that,

"since checks are a form of payment for goods and services and are issued against demand deposit accounts, it is reasonable to assume that the volume of checks is related to the level of production of goods and services and to the number of people and organizations holding checking accounts. Employment, income, and various measures of economic flow will also have an influence, given any stable pattern of payment habits."⁶

The report shows that by 1968 the number of checking accounts was growing at an annual rate of 4.1 per cent, while the nation's adult population was growing at a rate of only 1.3 per cent. In 1968 also the average number of debits to demand deposit or checking accounts was growing at an annual rate of 12.6 per cent.⁷ Thus, with both the number and use of checking accounts growing at a rapid rate, a certain increase in the absolute number of check frauds, including those involving the use of false identification, can be expected.

Encashment of Checks Stolen From the Mails

The Inspection Service of the U.S. Postal Service reports that "false identification use for the cashing of checks stolen from the mails ... most critically affects postal crimes. However, false identification is used in many other postal offenses including, but not limited to, mail fraud schemes such as check kiting operations, credit card frauds and the renting of post office boxes for unlawful purposes."⁸

The U.S. Postal Service figures reported below were gathered in a 20-city sampling carried out by 29 inspectors in 20 major U.S. cities during January and February of 1975. These figures are the result of investigations of checks stolen from the mails; the 20 cities covered were New York, Newark, Boston, El Paso, Seattle, Los Angeles, San Francisco, Buffalo (New York), Philadelphia, Washington (D.C.), Atlanta, Birmingham, New Orleans, Dallas, Chicago, Cleveland, Detroit, Minneapolis, Kansas City (Missouri) and Louisville.

Says the Postal Service Report:

"During Fiscal Year 1974, 140,864 checks with a total face value of \$22,331,451 were reported to this Service as stolen from the mails and subsequently cashed. During the two-month (Jan.-Feb. 1975) sampling period, 22,552 checks with a total face value of \$4,150,655 were reported as stolen. The sampling covered 5,949 checks."

Information developed from the sampling disclosed that false identification was known to have been used in the cashing of 1,466 of the 5,979 checks. In all probability, false identification was used in cashing many of the other checks but no information was developed to confirm this. Nothing was written on the checks to indicate that any identification was required and the persons accepting the checks were unable to remember what identification, if any, was required. The face value of the checks which were cashed with false identification totaled \$315,122,07.⁹ (Emphasis added)

In these crimes the three most-frequently used forms of false identification were, in order of use, a commercial photo identification card (496 times), a welfare identification (267 times) and a state driver's license (147 times).¹⁰ Several methods of obtaining false ID were used. False pretense was listed as having been the method used to obtain false identification in the case of commercial photo identification, while stolen welfare ID's accounted for 238 of the 267 incidents reported involving that ID. Further, 101 of 147 of the fraudulently used driver's licenses were stolen.

To take one example of crimes involving checks stolen from the mail--and almost certainly also involving the use of false identification--the Feb. 7 1975, issue of THE AMERICAN BANKER reported that the City of Philadelphia, Pa. alone 10,000 replacement welfare checks with a face value of \$1 million were issued monthly in 1972 and 1973. (A grand jury report stated much of the fraud was committed by recipients who falsely claimed not to have received their checks and eventually cashed both the original and replacement checks, though certainly a large proportion of the losses, perhaps as much as half, were caused by outright thefts from the mail.) These reports suggest massive, continuing fraud conducted with false credentials.

These losses were cut by half--or \$500,000 per month-- by the simple expedient of requiring all but bedridden or crippled welfare recipients to pick up their checks at their neighborhood bank branches, rather than mailing the checks to the recipients. Nevertheless, welfare check losses of a half million dollars per month in just one major city should constitute an absolutely unacceptable situation.

These figures illustrate the need for constant review of all check encashment operations to design changes which will reduce losses as new needs arise. Such a review should encompass alternatives to "welfare checks" such as direct deposits to welfare recipients' accounts. An explanation of this alternative is contained in Direct Deposit of Federal Recurring Payments, Department of The Treasury, Operations Planning and Research Staff.

Social Obligations - Impact on False ID Fraud

Many banks feel a social obligation to cash checks for certain non-depositors, and this obligation comes to the fore with such financial instruments as welfare and social security checks, as well as salary checks of local, state and federal government employees in the banks' communities. Criteria for proper personal identification in such cases will necessarily vary from community to community, but often an in-state driver's license or employee identification card will be accepted as proof of identification in such cases. In such cases, the bank recognizes that it is running a substantial risk of loss, but feels that it has little real choice in the matter.

Instructions from the U.S. Treasury govern the identity which can be accepted from persons presenting U.S. Savings Bonds to a bank for payment. Among other things, the Treasury requires full notation of the forms of personal identification presented to and accepted by the bank, including such items as military service serial number, date and place of issue and service branch. In the case of drivers' licenses, notation should be made as to what state issued the license what the license number is, and when it was issued.¹⁴ The Treasury Department requires that these measures be taken for it to guarantee payment to banks.

The American Express Company surveyed 6,175 Travelers Cheques regarding identification used with the encashment of the cheques. There were 153 or 2.48% of these that showed some form of identification other than the comparison signature on the check itself. Significantly, over 50% of the identification used were "Driver's Licenses" (see Table I below).

In commentary provided, American Express stated that false identification is not a real problem in the encashment of their travelers cheques. Moreover, the acceptance procedures requires in connection with the encashment of travelers cheques merely require the acceptor to witness the countersignature, of the travelers cheque, and compare the countersignature with the original signature. If the signatures are comparable, American Express agrees to honor that travelers cheque.

TABLE I
 SURVEY OF IDENTIFICATIONS USED IN CASHING TRAVELERS
 CHEQUES AMERICAN EXPRESS COMPANY

Type - I.D. Used	No. of Items	% No. of Times I.D. Used
Dirver's License	77	50.3
Credit Card	20	13.0
Passport	8	5.2
Vehicle Registration	4	2.6
Social Security	7	4.5
Armed Services		
Coast Guard		
Company Employee I.D.	1	.6
Government I.D.		
Courtesy Card		
Student I.D.		
Bank Book		
Union Book	2	1.3
Unemployment Book		
License (other than Driver's)		
*Other	34	22.2
TOTAL	153	99.7

*Miscellaneous information on back of T/C's, addresses, phone numbers, and other information of which identity of documents presented could not be determined.

If the acceptor is suspicious of the countersignature, American Express recommends that the acceptor have the person again endorse the travelers cheque on the reverse side and again compare signatures. It is not a requirement that an individual produce any type of identification upon the presentation of a travelers cheque.

American Express has stated that merchants, for their own protection, will require an individual to produce some identification at the time of presentation of a travelers cheque, but it is not an American Express procedure. The false identification problem, in connection with the presentation of different types of identification, usually relates to a counterfeit travelers cheque. Over the years, American Express has had a number of individuals who attempted to counterfeit cheques and has noted that on this type of encashment there is more false identification used than in other types of encashment.

False ID Involvement

As noted, the true extent of false ID use in the accomplishment of check fraud schemes of all descriptions must be conjectural for lack of extensive hard data. A notion of the role played by false ID in check fraud activities can be obtained, however, by examination of the data presented in Table II, Check Forgery, Fraud and Embezzlement Data, compiled by the Check Section, Metropolitan Police Department, Washington, D.C. Of note in Table II is the high incidence of detected false ID use in Forgery and Fraud schemes.

Table III from the same source illustrates the type of false ID commonly used, in rank order, and the customary means of acquisition of the false documents.

Bank Card Fraud

The bank card segment of the banking industry continues to grow rapidly although less than in previous years. Growth in retail volume was 26.5 percent in 1974, for example, as compared to 34.6 percent in 1973. In dollar figures, National BankAmericard Inc. and Interbank Card Association (BankAmericard and Master Charge, respectively) report that the 1974 gross volume of billings was \$17.6 billion.¹¹ At the end of 1974, 12,899 banks and 2,182,993 merchant outlets were participating in bank card plans. The average sale was \$23.91, and cash advances in 1974 totalled \$518 million.

It should be recognized that credit card or bank card fraud is a "second-order crime,"¹² one made possible by an earlier crime; for example, theft of or tampering with a valid card, or counterfeiting of a card. A 1974 study of The MITRE Corporation, "Security

TABLE II

CHECK FORGERY, FRAUD AND EMBEZZLEMENT DATA

I. FORGERY	
A. Number of complaints.	711
B. Amount of loss.	\$202,109
C. Number of complaints cleared.	406
D. Number of arrests	391
E. Number of complaints where stolen or false identification used.	90%
II. FRAUD (False Pretense - bad checks - confidence schemes)	
A. Number of complaints.	876
B. Amount of loss.	\$333,772
C. Number of complaints cleared.	499
D. Number of arrests.	285
E. Number of complaints where stolen or false identification used.	50%
III. EMBEZZLEMENT	
A. Number of complaints.	143
B. Amount of loss.	\$393,763
C. Number of complaints cleared.	89
D. Number of complaints where stolen or false identification used.	15%
E. Number of arrests	81

TABLE III

ID USED TO CASH NEGOTIABLE INSTRUMENTS

<u>TYPES OF IDENTIFICATION</u>	<u>HOW OBTAINED</u>
A. Drivers permits	Stolen, counterfeit, false names
B. Credit cards	Stolen, false applications
C. Social Security cards	False names, stolen, counterfeit
D. Government ID cards issued to employees	Stolen, counterfeit
E. Private Business ID cards issued to employees	Stolen, counterfeit, false names
F. Commercial ID cards	Issued by commercial photo companies in any name, no proof of true ID needed.
G. Check cashing courtesy cards	Stolen, false names
H. Bank ID cards	Stolen, false names
I. Selective Service cards	Stolen, counterfeit
J. Governmental Services ID cards issued to recipients	Stolen, counterfeit, false names
K. Passports	Stolen, counterfeit, false names

Aspects of Bank Card Systems," identified three categories of bank card fraud, which may also be considered as fairly representing all credit card fraud: misuse of a valid lost or stolen card; use of a counterfeit card; and application for a card by a person with criminal intent.

A typical profile of criminal misuse of credit cards is described by The MITRE Corporation as follows:

"First the cards must be obtained by the criminal, then they can be used to commit fraud. These two crimes can be considered independent events. First a pick-pocket, burglar or thief steals the bank card. (The criminal may not necessarily be concentrating on cards, but if they are available they will generally be stolen.) The criminal will in turn attempt to sell the stolen cards to criminals who specialize in bank card fraud. Since stolen cards must be used quickly, a small number of criminals can display a voracious appetite for cards: three to ten cards a week, 150 to 500 cards a year. Moreover, not all of the stolen cards will be used fraudulently; the conditions under which the card was stolen or offered might turn off the criminal buyer."¹³

The statistics gathered by The MITRE Corporation reveal, however, that following a massive wave of bank card fraud in the late 1960's when these credit instruments were introduced, criminal misuse of bank cards has receded since 1970. Total number of bank card fraud cases reported by nine banks in various areas of the nation annually dropped from 5,472 in 1970 to 5,331 in 1974. The real decline, however, is apparent in the drop of the average dollar figure involved in these losses: from \$255.64 in 1970 to \$164.18 in 1973.

National Association of Securities Dealers Survey

The report submitted by the National Association of Securities Dealers, Inc. (NASD), the self-regulatory agency for the over-the-counter securities market, was based on a survey conducted of its over 3,000 member firms. These members, who are also registered as brokers and dealers with the Securities and Exchange Commission, account for approximately 80 percent of the nation's brokers who transact securities business interstate on registered national securities exchanges and in the over-the-counter market. The NASD received 2,734 replies which represents an unusually high response rate of about 90 percent.

In constructing its model for commercial transactions, the Commercial Transactions Task Force determined that securities generally

do not fit into the definition because extensive federal and self-regulatory rules, designed to prevent the execution of transactions by way of false representation, result in few executions of securities transactions in a "one time, face to face encounter" between a customer and a broker-dealer. (See Section IIA, Definition of the Problem.) The Association recognizes that such situations could occur, however, where a firm was not entirely mindful of its responsibilities under the rules or was careless in the implementation thereof. The study was therefore conducted to determine the extent of the problem. It revealed that during the period 1972-1974 a total of only 18 of the 2,734 responding firms experienced losses as a result of false identification. These firms reported 44 cases in which false identification was cited as the underlying cause of losses. The dollar value of losses reported for these 44 cases totals \$563,412.

On the basis of this evidence, the NASD concluded that false identification in the securities industry is only a nominal problem. According to the NASD's report, this low incidence rate of false identification problems is a direct result of the many rules governing the opening and maintenance of customers accounts including the strictly applied "know your customer" and comprehensive suitability rules prescribed and enforced by the various self-regulatory agencies.

The NASD noted, however, that lost and stolen securities, as distinguished from losses resulting from false identification, continue to be a major problem confronting the broker-dealer community and, as such, current efforts in this area must be strengthened and new programs developed. Efforts are underway in this area but such is not the subject of inquiry by this Task Force.

National District Attorneys Association Survey

A national survey of local prosecuting attorneys disclosed that local prosecutors do not have the record facility and capacity to capture false identification data or trend. This points up the fact that adequate records of false identification offenses are no more complete at local levels than at Federal levels.

The prosecutor, in the main, is unmindful and therefore unaware of the false identification problems except in the isolated criminal prosecution. He knows that there is a "flood" of bad check and illicit credit card cases "out there" but his priorities keep him far away. He looks to his police departments for his record information. When he sees the false identification problem, it is mainly in connection with stolen or counterfeited documents and involves credit cards, social security cards, driver's licenses, uniforms and badges, draft cards, police identification cards, passports and visas, alien identification cards, motor vehicle registrations, check books,

government or payroll checks, and company identification cards. These are used by individuals (1) to misrepresent their identity; (2) in conjunction with corroborating false documents; (3) after being altered to correspond with the holder's appearance to assume a new identity either real or imagined and in the commission of a forgery.

It is interesting to note MITRE's* analysis of the use to which false documents are put as derived from NDAA's survey. The fugitive problem alone can develop meaningful statistics. MITRE draws some conclusions from the survey which must be guarded ones in view of the limited responses to the survey as a source for false ID conclusions.

"...the number of incidents of the use of false identification per year equals approximately 1% of the population.

"...reported impact of false identification incidents when averaged by dollar value per incident would appear to be about \$400 per incident. Based on these figures, the cost of false identification incidents (known to prosecutors) annually to the USA would approach \$90,000,000. The most significant item of analysis is that only 20% of the prosecutors reported maintained any records under their own cognizance.

Recommendations

- a. Require more substantial identification.
- b. Educate clerical help in the methods used by holders of false identification.
- c. A better system of identification, e.g., social security card to include a color photograph and fingerprint of the holder.
- d. Tighter controls over the issuance of governmentally authenticated documents. (i.e., birth certificate, driver's license, social security cards)

It is obvious the prosecutor sees the problem as one involving theft and counterfeiting and the use of the false identification to commit a serious offense. Unfortunately in the latter, his case records do not disclose those incidents involving false ID as an instrument of prosecutable crime. The average prosecutor views the multi

*An informal paper presented to the Task Force.

standards and loose approach of merchants to ID issues with some scorn, and will not give a high priority to these cases even when the proof is more than marginal. The prosecutor often tends to view the false ID problem primarily as an operational one better suited for industry and commerce control. To that end he prosecutes a minimum of such cases presented. He views the law as adequate.

SECTION III
PRELIMINARY RECOMMENDATIONS

General

The preliminary recommendations of the Commercial Transactions Task Force are presented in two separate sections, reflecting the differences in viewpoint between the representatives of the commercial and the law enforcement communities. The two disparate viewpoints are considered generally complementary and the recommendations of these two groups are not, in general, mutually exclusive although the operational premises do differ greatly.

The first section, representing the ideas of banking and business members, emphasizes the precautions against false ID fraud that are practical at the present time, without recourse to additional technology or legislation. The second section, developed from the suggestions of District Attorneys and other law enforcement personnel, stresses improvements in technology and customer education.

Section III also includes a brief discussion of Automated Personal Identification, a developing field of technology by which individuals may be identified by comparing values of measured personnel characteristics against values of other characteristics previously stored in a computer data base. This type of identity verification requires no identification documents.

Recommendations from Business and Banking Representatives

General

Many swindlers operate almost completely without credentials of any sort, depending instead on their persuasive abilities, their power to "con" their intended victims. They may, for example, try to confuse or embarrass a bank teller or retail sales clerk with a series of special requests -- changing and re-changing money, loud claims to be bona fide depositors, split deposits (which should in themselves be a warning signal), etc. -- and hope that in the resulting confusion, the teller or sales person will fail to follow procedures for establishing identity and validating credentials in order to cash a check or accept a credit card. Thorough employee training and well-conceived management policies are probably the best preventive measures against such swindles, and such training programs should include strict adherence to the bank's or business's identi-

fication policies and procedures and support by management when employees adhere to the prescribed procedures.

Identification With and Without Credentials, a publication of the American Bankers Association, notes that "no bank has a legal obligation to cash a check drawn on another bank. Although every bank is required to pay on demand a bona fide check drawn on itself, every bank is also permitted to delay cashing any check for any of at least five reasons."¹⁵ These reasons also constitute an excellent checklist for verifying a presenter's identity and his right to cash the check he presents. Acceptors should verify that:

- "1. the signature is genuine;
2. the maker has sufficient funds on deposit to cover the check (in the case of an 'on us' check);
3. payment has not been stopped;
4. the presenter is adequately identified; and,
5. the bearer of the check has title to the instrument."¹⁶

Technical Devices

Many highly sophisticated technical devices now exist which can aid in the later identification of persons who have fraudulently presented a check or credit card to a banker or merchant. These include fingerprint identification devices and photo records of the presenter and of the instrument. While these devices may help to identify and track down criminals, they do not necessarily deter actual fraud.

The possibilities for machine control of credit card fraud are almost endless - and, in some cases, very expensive. They range from laser analysis of materials embedded in the card to machine-reading of metallic wafers sandwiched inside the card to optical scanning. The central concerns are to prevent tampering with a card's magnetic strip, which is the crucial operative portion of a card, and to ensure that only the lawful owner of such a card can use it. It appears that developing technology will be able to meet the challenges posed by the criminal world. A full exposition of recent developments in this area is included in Security Aspects of Bank Card System, a study by The MITRE Corporation for the American Bankers Association.²¹

Employee Training

The old dictum, "know your customers", still serves as the best preventive to crimes committed with false identification.

Many common sense procedures that do not require special equipment also are available to merchants and bankers. White Collar Crime, published by the Chamber of Commerce of the United States, stresses this point.

Acceptors of credit cards -- especially their money-handlers, such as cashiers -- can play a particularly critical role in preventing credit card fraud and in enhancing an establishment's reputation for being 'no pushover': Check the dates on the card indicating when it becomes valid and when it expires. Refer to issuer's card cancellation bulletin. Note if the card appears altered or defaced. Compare the signature on the card with that on the sales slip. Call the issuer's special authorization number if any of the danger signals...(such as multiple purchases on the same day, split purchase to keep under authorization limit, etc.) arouse suspicions...Keep card imprinters and blank charge slips under tight control. Drop floor limits, in retail operations, to zero in selected departments occasionally. Keep cashier areas well-lighted to discourage unauthorized transactions and to reduce errors. Select as a cashier someone who has basic intelligence and who has been well trained. Do not allow waiters to imprint charge slips. Investigate customer allegations of mishandled credit card transactions.¹⁷

Employees' lack of familiarity with basic identification documents such as drivers' licenses can make the use of false identification easy for criminals. Employees may even not know how to read codes on a driver's license or what to look for to verify the authenticity of a document presented to them. White Collar Crime recommends the following steps to limit check fraud losses:

Safeguard blank checks and check-writing equipment. Require identification before cashing checks. Do not accept the following for identification purposes -- Social Security cards, business cards, club cards, letters. Become familiar with the driver's license issued by your state and neighboring states (one source for this information is Drivers License Guide, published annually by Drivers License Guide Co., 1492 Oddstad Drive, Redwood City, Calif. 94063). Certain built-in features -- such as year of birth as part of the license number -- may help you identify counterfeits presented for identification.

Compare not only the person's signature but also his appearance with what is indicated by his identification document. Do not accept an updated or postdated check, nor one that is dated more than 20 days previously. Require personal checks to be made out for the exact amount of the purchase...Witness endorsements. If the check is already endorsed, have it re-endorsed...Do not cash checks written in pencil.¹⁸

Other steps listed in White Collar Crime are designed to prevent fraud committed with an individual or merchant's own checks. "Inspect the middle and back sections of check books, especially after a theft has been committed on the premises...Safeguard bank statements and cancelled checks. They reveal your bank balance, signature, and check design...Do not prepare checks with typewriters utilizing 'lift off' ink."¹⁹

Credit and Bank Card Measures

Security measures instituted by the issuers of credit cards and bank cards have contributed substantially to the reduction of losses due to frauds involving their cards. While some of these measures depend on the intelligent cooperation of merchants and their sales staff, others operate strictly internally, for example, through computer-monitoring to detect card usage that varies from certain norms.

White Collar Crime outlines some of these measures:

Shortly after cards are mailed, a follow-up inquiry is sent to determine if the card arrived. This simple procedure has cut fraud losses substantially, thanks to the timely information it elicits. To reduce even further the possibilities of theft from the mail, some issuers use registered mail when cards are sent to 'high risk' Zip code zones.

Various security features are built into cards on a periodic basis as an anticounterfeiting measure.

Computers of many card issuers can alert officials if a cardholder's spending departs from his traditional pattern; if so, the cardholder may receive a phone call from the issuer and be asked to confirm if his card is still in his possession.

Depending on an acceptor's fraud-loss record, he may be required to seek authorization -- via phone -- from the issuer before honoring a user's card in transactions above a prescribed amount. Computers of some issuers are able

to relate the fraud-loss experience of an establishment to that of others in the same area. Where losses seem out of line, investigators may be sent to the scene. Card cancellation bulletins, which contain the numbers of stolen or lost cards, are sent to acceptors periodically and rewards are given to those who pick up unexpired cards listed in these bulletins. Experimentation is now under way with regard to computer-linked terminals that employ scanners to validate cards at the point of sale.²⁰

In addition, credit card issuers now scrutinize applications for their cards very closely, and investigations may take as long as six to eight weeks. Such careful and thorough investigations help to avoid the issuance of cards to persons who may have falsely identified themselves and have made their application with criminal intent.

The Dilemma

Clearly, there is almost no limit to the amount of identity verification that can be carried out in commercial transactions. In general, the rules outlined above work equally well for merchants and bankers. Certainly, some identity documents simply should not be accepted; among these are commercial personal photo identification cards, library cards, blood donor cards, and Social Security cards. Tellers and sales persons should be familiar with the documents that they do accept so that a customer's identity can be properly established. On the other hand, the more restrictive a merchant's check-cashing or card-accepting policy, the more limited his field of customers becomes. Likewise, the more time-consuming it becomes to cash a check in a bank or to open a checking account, the less happy a banker's customers are. The dilemma is the same for bankers and businessmen. If you make your operation totally fraud-proof -- and it probably can be done -- you run the distinct risk of making it customer-proof, too.

This fact helps to explain why it is easy to open a checking account today. In general, no more than a Social Security number is required; lacking that, a student ID or other such card will be accepted. The bank customer supplies two specimens of his signature, and the account is opened. Why is it so easy? Simply because a bank wants to provide a broad spectrum of customer services, and it is through a checking account that an individual receives his first introduction to full banking services. The same factor affects merchants, who must do business to stay in business. Each operator must balance for himself the relative risk and profit potential in each decision on accepting a check or credit card. Refusing to accept checks, credit cards or certain personal identification documents may cut a merchant off from a certain portion of

his market; on the other hand, the wholesale, indiscriminate acceptance of checks, credit cards and personal ID's very likely will expose a merchant to considerable losses.

In the same way that merchants are reluctant to risk offending a legitimate customer, bankers are reluctant to make it more difficult to open checking accounts. The provision of bank services -- personal, installment and business loans, trust services, bank cards, etc. -- constitutes an important source of bank revenues. In addition, the funds available to banks from customers' deposits in checking accounts have become very important for loan purposes. Finally, it should be pointed out that the overwhelming majority of bank transactions are legitimate; this has been true historically and continues to be true.

Current Countermeasures

Recognizing the dangers of fraud inherent in the free operation of checking accounts, some banks have taken steps to control these possibilities. For example, most banks mail printed checks to their customers, rather than handing them over on the spot, since this helps to verify the customer's address. Many banks have eliminated courtesy checks. Banks also may require a telephone number and verify the customer's residence by a phone call. Some banks have eliminated counter checks, and the Federal Reserve System no longer handles counter checks through its clearing houses. The intent of these steps is to minimize the possibilities of check fraud, as well as to achieve standardization for processing purposes.

While banks' losses due to check and credit card fraud continue to diminish each year, even as the nation's annual volume of checks doubles each decade, it must be recognized that merchants' losses have in some cases reached intolerable levels. However, when the preventive steps outlined in earlier sections of this report are followed carefully and conscientiously, they can significantly reduce merchants' losses from check and credit card frauds.

Of all the methods currently available to protect the security of "cash machines" now in use by some banks, the "Personal Identification Number" seems to be the most effective. This is a number known only to the customer and the computer. When the customer inserts his magnetic card into the cash machine, he must punch out his Personal Identification Number in order to verify his identity before any transactions can take place. When electronic funds transfer systems (EFTS) achieve wider acceptance, it is possible that the use of a Personal Identification Number at point-of-sale, on-line computer terminals could effect the same goal of ensuring security of

the system. The use of the Personal Identification Number is by far the cheapest and most effective system now available, The MTRE Corporation concluded.¹²

(More information on EFTS is available in A Digest of Electronic Funds Transfer Systems Thinking Today, a publication of the American Bankers Association.)

For the Future

It is concluded that procedures currently known and available, if consistently used by merchants and bankers, could significantly and satisfactorily reduce losses due to crimes involving false identification. These procedures, which involve authentication of identification documents at the time of the commercial or banking transaction, have been outlined above. As previously noted, banks which have followed such procedures have successfully minimized losses due to fraud.

The eventual implementation of electronic funds transfer systems will also help to reduce such crimes. When, for example, the funds involved in a supermarket transaction can be instantly debited to the customer's account and credited to the merchant's account (at the same moment that the computer codes verify the customer's identity), the problems of bad checks and customer inadvertence, as well as many of the problems of forgery, will be virtually eliminated. These new systems, however, will require their own elaborate safeguards; such protective devices and procedures are now under development and hold great promise of success.

In addition, direct deposits through electronic funds transfer systems are helping to diminish the possibilities for fraud, since if a check is not physically existent it cannot be stolen and cashed fraudulently. For example, the Treasury Department is currently experimenting with direct deposits to Social Security recipients in certain Southeastern states; it is hoped that such direct deposits of recurring government payments will eventually be established nationwide. Again, direct electronic payments through privately-operated automated clearing houses are eliminating check fraud and achieving significant economies in processing of payments. Minimization of losses remains a major goal of these innovations, and as each new electronic funds transfer system enters use, steps are taken to avoid computer crime as well.

Many banks now exercise tight control over information and materials likely to make check and credit fraud possible, within

their commitment to provide full customer service. This control includes refusing to cash checks for non-depositors and refusing split deposits unless approved by management personnel. It is felt that, on the whole, retail merchants have also moved in recent years to curtail losses caused by crimes involving false identification.

Clearly, it would be desirable for all banks and retail establishments to keep detailed records of documents accepted for purposes of authenticating an individual's identification. This procedure can be useful in locating persons who presented invalid instruments. The usefulness of this procedure depends, however, on the ability of sales persons and tellers to correctly evaluate identity documents presented to them and to make thorough notations regarding those documents. A business or bank which suffers chronic major losses due to fraud perpetrated with false identification could well consider tightening policies and upgrading employee training in the evaluation of identification documents, as well as noting the identification presented.

Legislative Solutions

Given both bankers' and merchants' need to maintain the free flow of business activity, it is felt that restrictive legislation which might adversely affect the present freedom of business activity is not needed. Bankers and merchants through establishment of firm policies and procedures can minimize their losses due to fraudulent transactions. On the other hand, any legislation which could speed the apprehension, prosecution and punishment of criminals using false identification would be welcome. Certain recent legislation, notably PL 93-495, which was signed into law in October of 1974, moved in that direction. That law doubles the maximum sentence for credit card crime from 5 to 10 years and lowers the threshold at which federal prosecution may be triggered, as well as expanding the list of federal credit card crimes.

Agency and Institutional Process

It is felt that thought should be given to the question of who issues and guarantees the validity of personal identification documents. For example, as noted by other Task Forces of this Committee, what steps are taken to verify the identity of an applicant for a driver's license or for a duplicate license? Again, crosschecks of birth and death certificates are desperately needed, since it is apparent at present that would-be criminals can use states' and localities' laxity in this area to establish convincing false credentials with relative impunity. How difficult is it to forge or misuse these documents? Experience leads to the conclusion: "not hard enough."

Active Prosecution

How often is anyone prosecuted for counterfeiting or fraudulently possessing Federal, state or local identification documents? Too often the illegality of these acts is forgotten, and prosecution takes place solely on the basis of some other crime committed by the individual.

Institutional Policy and Intelligence Activities

Constant review by banks and retail establishments of their check cashing and credit card accepting policies remains a must, since the ingenuity of criminal elements never flags. Monitoring of criminal trends by banks and businesses must be carried out constantly so that commercial practices regarding financial instruments can be adjusted to meet the ever-new challenges of the criminal world. However, as noted above, most of these actions are best carried out by individual banks and businesses, taking into account local needs, business potential and risk exposure.

Recommendations from Law Enforcement Representatives

General

In their attempts to combat crime based on false identity, police and prosecutors are often frustrated by insufficient resources and conflicting priorities, compounded by the feeling that the problem is aggravated by the "loose" practices of their banking and commercial constituents. From the surveys of District Attorneys and the statistics of the Washington, D.C. police, the following conclusions may be drawn:

1. The most prevalent methods of obtaining false identification appear to be theft and counterfeiting.
2. The losses to the individual businesses and enterprises are "small" in comparison to the total industry business but awesome when grouped together as a national figure. Also important are the "losses" not calculable in monetary terms, such as those resulting from the ability of dangerous criminals to operate unmolested thanks to false identification documents.
3. The cost effectiveness argument is the swindler's best friend.
4. Law Enforcement has no clear picture of the problem and will not until its record keeping capacity is improved.

The recommendations which appear to gain the most support are:

1. Improving the integrity of the most frequently used documents -- birth certificate, driver's license.
2. Instituting a national identification document as proposed by the Passport Office.
3. Developing standards to be used by check cashers, sellers, etc. The sanctions can be in the collectability of insurance and, in the less frequent situation, the declination of prosecution. This recommendation depends on:
 - (a) The improvement of selected identification documents.
 - (b) The willingness of industry and commerce to adopt the standards even though the "cost effectiveness" presents some problems. (No one expects industry to lose money, but a large initial investment followed by success can turn the cost "effectiveness" argument around.
4. Developing an educational program that can reach in simple understandable terms the clerk, the cashier, the merchant in their crowded life. The other side of the coin is an educational program to induce the honest citizen to use only selected types of identification. This will help militate against the argument that strict standards chase the customers away.
5. Developing of a uniform record-keeping system for law enforcement to use to measure the scope of the problem and suggest changes in priorities in the implementations of existing laws by law enforcement.

Automated Personal Identification

Automated Personal Identification,²² a study by the Stanford Research Institute's Long Range Planning Service, provides some possible long-range solutions to the problem of false I.D. This document has a message even for the non-skilled. It makes a strong case for fully automated devices for identification (as distinguished

from manual) verification of credit by clerks resorting to an I.D. document or to an electronic computer terminal. In the fully automated system one or more personal characteristics (e.g., fingerprint, weight, voice, memory) will be used as identification. The study contains a recognition of all the psychological constraints. It is even contemplated that a "no card" automated system could be devised where a person to be identified would supply a name or identification number and access is made to a personal data record in the central file.

REFERENCES

1. Federal Register, Vol. 39, No. 205, October 22, 1974, pp. 37515-37516.
2. Roy Jacobus, official statement to Task Force on Commercial Transactions.
3. Robert H. Long, Charles R. McClung and Walter W. Stafeil, The Impact of Exception Items on the Check Collection System (Park Ridge, Ill., 1974), a report by the Bank Administration Institute, p.3.
4. Major events in evolution of EFTS are occurring with rising frequency, report in Banking, a journal of the American Bankers Association (May 1975).
5. Same as footnote 3, pp. 3-6.
6. Arthur D. Little, Inc., The Outlook for the Nation's Check Payments System, 1970-80, a report to the American Bankers Association, (Boston, Mass., 1970), p. 114.
7. Ibid., p. 115.
8. William J. Cotter, chief inspector, U.S. Postal Service (letter to Hollis W. Bowers of American Bankers Association, 1975.
9. "False Identification Usage in the Cashing of Checks Stolen from the Mails", a report by the U.S. Postal service (Washington, D.C., 1975), March 1975, pp. 1-2.
10. Ibid., p.2.
11. ABA Bank Card Letter, a newsletter of the American Bankers Association (Washington, D.C., 1975), April 1975.
12. M. Ferdman, D. W. Lambert and D. W. Snow, Security Aspects of Bank Card Systems, a report to the American Bankers Association by The MITRE Corporation, (Bedford, Mass., Dec., 1974), I. p. 15 (study to be released).
13. Ibid., p. 15.
14. Protective Bulletin (Washington, D.C., 1950), American Bankers Association, Sept. 1950.

15. Identification With and Without Credentials, a publication of the American Bankers Association (Washington, D.C. (1974), p. 7.
16. Ibid., p. 7.
17. White Collar Crime, a publication of the Chamber of Commerce of the United States (Washington, D.C. 1974), pp. 75-76.
18. Ibid., p. 77.
19. Ibid., p. 77.
20. Ibid., p. 76.
21. M. Ferdman, D. W. Lambert and D. W. Snow, Security Aspects of Bank Card Systems, a report to the American Bankers Association by The MITRE Corporation, (Bedford, Mass., Dec., 1974), I, p. 15 (study to be released).
22. Raphael, David E. and Young, James R., Automated Personal Identification, Stanford Research Institute, Report No. 539, Dec. 1974.

ATTACHMENT I

COMPOSITION OF THE TASK FORCE

The Commercial Transactions Task Force is composed of representatives of police agencies, prosecutors' offices, the banking and securities industries, credit card associations, and the U.S. Department of Justice. Specifically, the organizations and representatives which originally comprised the Task Force are as follows:

- HOLLIS BOWERS (Co-Chairman), Director, Insurance and Protection Division, American Bankers Association, 1120 Connecticut Avenue, N.W., Washington, D.C. 20036, (202) 467-4046.
- NATHANIEL E. KOSSACK (Co-Chairman), Principal Consultant, National District Attorneys Association, Economic Crime Project, 1900 L Street, N.W., #601, Washington, D.C. 20036, (202) 872-9507.
- ROBERT BRECHEISEN, District Sales Manager, Polaroid Corporation, 3720 Browns Mill Road, Atlanta, Ga 20315, (404) 762-1711.
- PAUL B. CHAPMAN, National Security Manager, Sears, Roebuck & Company, Department 731 B.S.C. #42-27, Sears Tower, Chicago, Il 60684, (312) 875-8431.
- DONALD FOSTER, Counsel, National District Attorneys Association, Economic Crime Project, 1900 L Street, N.W., #601, Washington, D.C. 20036, (202) 872-9507.
- JAMES C. KINGSBURY, Trade Specialist, Bureau of Domestic Commerce, U.S. Department of Commerce, Washington, D.C. 20230, (202) 967-3818.
- THOMAS F. KIRK, Area Manager, Intelligence Division, Internal Revenue Service, IRS Building, Room 7239, 1111 Constitution Avenue, N.W., Washington, D.C. 20224, (202) 964-6113.
- THOMAS KNIGHTEN, General Credit Manager, Giant Food, Inc., P. O. Box 1804, Washington, D.C. 20013, (301) 341-4143.
- MICHAEL R. KOBLENZ, Trial Attorney, U.S. Department of Justice Securities Unit, Federal Triangle Building, Room 508, 315 Ninth Street, N.W., Washington, D.C. 20530, (202) 739-2723.

LEONARD KOLODNY, Manager, Retail Bureau, Metropolitan Board of Trade, 1129 20th Street, N. W., Washington, D.C. 20036, (202) 659-6400.

LT. KENNETH V. MORELAND, Criminal Investigation Division, Metropolitan Police Department, 300 Indiana Avenue, N.W., Room 4071, Washington, D.C. 20001, (202) 626-2211.

DAVID P. PARINA, Assistant Director, Department of Regulatory Police and Procedures, National Association of Securities Dealers, Inc., 1735 K Street, N. W., Washington, D.C. 20006, (202) 833-7247.

ALLEN O. PEFFER, Postal Inspector, Projects Coordinator, External Crimes Branch, U.S. Postal Service, Inspection Service, L'Enfant Plaza, Washington, D.C. 20260, (202) 245-5464.

ANDREW F. PHELAN, Vice President, Corporate Security Inspector's Office, American Express Company, 67 Broad Street, New York, N.Y. 10004, (212) 797-5080.

FRED RAYNE, Director, Burns International Investigation Bureau, 1681 John F. Kennedy Causeway, Miami, Florida 33141, (305) 965-6753.

ROBERT J. SCULLY, Assistant Vice President, Interbank Card Association, 110 East 59th Street, New York, N.Y. 10022, (212) 486-1100.

DAVID SPEARS, Representative, Polaroid Corporation, Industrial Division, Cambridge, Mass 01020, (703) 524-2806.

STEPHEN M. WEGLIAN, Trial Attorney, Securities Unit, General Crimes Section, Criminal Division, U.S. Department of Justice, Washington, D.C. 20530, (202) 739-2670.

FRANK J. WILSON, Senior Vice President, Regulatory Policy and General Counsel, The National Association of Securities Dealers, Inc., 1735 K Street, N.W., Washington, D.C.

Staff Associate, ROBERT J. ELLIS, The MITRE Corporation.

ATTACHMENT II

SUMMARY OF MATERIAL IN TASK FORCE FILES

1. Statement of Mr. Roy Jacobus, The MITRE Corporation to The Task Force, 11 March 1975.

This statement defines and bounds the "commercial transaction" of interest to The Task Force, structures the types of transaction, the negotiable instrument and the common ID required. Some common types of fraud are described with the fraud detection issues related to them. Suggestions for correction of specific statistical data are also given.

2. Survey conducted by the U.S. Postal Inspection Service, January and February, 1975.

This survey tabulates the results of a false ID sampling study involving 20 major cities to determine the scope of the problem relative to postal crimes - mainly the cashing of checks stolen from the mails. Other false ID related postal offenses such as check writing operations, credit card frauds and the renting of P.O. Boxes for unlawful purposes.

The statistical presentation includes the value of checks lost, false ID use in cashing of stolen checks (25%), frequency of use data for types of false ID, and racial, sex, age, employment, etc. profiles of individuals using false ID to cash stolen checks.

3. Survey Conducted by American Express Company, May 7, 1975.

This survey shows the ID used to cash traveler's checks together with the frequency of use. The survey results imply that for TC's, false ID does not represent a serious problem in general. The use of false ID is asserted to associated mainly with the use of counterfeit TC's.

4. Survey of the Metropolitan Police Department, Washington, D.C., 1974.

Data are presented on false ID use for the crimes, forgery, fraud, and embezzlement. Further data are supplied relating false ID type with the classic means for acquiring.

5. Report of Interbank Card Association, March 5, 1975.

This report summarizes the data obtained from The Association's ongoing fraud reporting process. It describes the false ID problem relative to bank cards, presents information on typical application for and use of cards, the ID requested for each phase and estimate, the use of false ID in these transactions. Further, a "profile of false ID users" is put forth along with countermeasures, information and suggestions for solutions.

6. Report of the National Association of Securities Dealers, (NASD), Inc., False Identification Problems in the Broker - Dealer Community, May 9, 1975.

This document reports the results of a survey of the Association's membership and solicited comments from various industry and trade associations. It gives the background of the organization, verbal comments on the survey and preliminary recommendations.

7. Survey of the National District Attorney's Association - National Survey on False Identification, January.

The National Survey examines the nature of the false ID problem and related issues, presents an ordering of common false ID, document type, and the methods and devices used to acquire them. Included are comments on the scope of the problem, typical offender profiles, victims and preliminary recommendations for solution.

APPENDIX A3

**REPORT OF THE FUGITIVES TASK FORCE
ON THE
SCOPE OF THE FALSE IDENTIFICATION PROBLEM AND
PRELIMINARY RECOMMENDATIONS FOR SOLUTIONS**

Submitted to

**Federal Advisory Committee On False Identification
David J. Muchow, Chairman**

May 1976

TABLE OF CONTENTS

	<u>Page</u>
SECTION I - INTRODUCTION	A-79
Purpose	A-79
Scope	A-79
Data Sources	A-81
SECTION II - THE FUGITIVE FALSE ID PROBLEM	A-83
Classes of Fugitives	A-83
The Militant Terrorist/Revolutionary	A-83
The Juvenile	A-83
The Traditional Criminal	A-84
Types of False ID	A-84
SECTION III - FUGITIVE CRIMES	A-87
General	A-87
Fraudulent Check Passing	A-87
Passport Frauds	A-88
Social Security Account Card Frauds	A-88
Narcotics Trafficking	A-89
Illegal Aliens	A-89
Insurance Frauds	A-90
Credit Card Schemes	A-91
Traveler's Check Schemes	A-91
Automobile Theft Rings	A-93
Bank Fraud and Embezzlement	A-94
Internal Security	A-96
SECTION IV - PRELIMINARY RECOMMENDATIONS	A-99
ATTACHMENT I - COMPOSITION OF THE FUGITIVES TASK FORCE	A-101
ATTACHMENT II - MATERIAL IN TASK FORCE FILES	A-102
ATTACHMENT III - INTERPOL RESPONSE	A-103

Report of the Fugitives Task Force
on the
Scope of the False Identification Problem
Recommendations for Solutions

SECTION I

INTRODUCTION

Purpose

The task of the Fugitives Task Force was to examine the ways in which and the extent to which false identification is used to impede the apprehension of fugitives in our society.

Scope

In examining the nature of fugitives, it is necessary to examine and categorize the crimes or potential crimes which have engendered the assumption of fugitive status. It is axiomatic that maintenance of a fugitive status is much aided by a false identity and that continued criminal activity while in this state may -- most often does -- require a series of false IDs. Otherwise, the original false ID becomes as harmful to the fugitive as a true ID would be.

It is assumed that the fugitive state begins at the planning stages of a crime. When the intent assumes reality, acquisition of a false ID with which to commit the crime impedes correct and early assignment of responsibility for the crime, and aids the criminal in maintaining a fugitive status.

Accordingly, the use of false identification by fugitives to avoid detection and arrest or linkage to a previous criminal record, to remain in a covert status, or to aid in the commitment of further crimes, were the areas of primary concern to the Task Force.

The extent of this issue is vividly set forth in a statement by the Montgomery County Sheriff's Department of Dayton, Ohio. It states:

"There is not a standard from which you can draw specific types, as criminals' use of false ID has become commonplace among persons engaged in all walks of illegal activity. A common belief that alias names are restricted to forgery types of crime is a gross misconception. The growing and thriving business in underworld sale of false identification and related items has become so standard that not only does the common thief have ready access to any type of false ID he wishes, but also he finds the going street price within the easy reach of his budget. As a result, it is possible for anyone to assume an identity other than his own and to provide upon demand almost any type of identification to substantiate it.

"All areas of criminal activity, including persons perpetrating forgeries of checks and credit cards, persons who know they are wanted for criminal violations, persons who are engaged in organized criminal activities, arrested persons, traffic violators, and even high school students who want to change their ages for beverage purchases, are known to purchase and use ID of this type.

"For practical purposes, it is safe to assume that any and all documents that can be used for the identification of a true name can and are being used to provide false identification. State operators' permits, credit cards, social security cards, employment cards and badges, draft cards, hospitalization cards, fraternity and special club cards are among the most common; however, it is not unusual to find stolen or counterfeit birth certificates, baptismal records or passports in the possession of known criminals. We have encountered multiple pieces of ID, all in the same alias name, in the possession of suspected persons, and in several cases, multiple ID in different names thus allowing the person to assume a variety of identities.

"The Montgomery County Jail has an average of eight to ten persons booked into the jail each month under alias names. These figures are based on known statistics."

Data Sources

The methods utilized to gather information included surveys of selected sheriff's offices, metropolitan police departments, Interpol¹, and the Federal Bureau of Investigation. Sources of other information included the Administration of the Internal Security Act of the Committee of the Judiciary, United States Senate, and the 1973 and 1974 FBI Annual Reports.

Quantitative data on the number of incidents of each type of use of false identification by fugitives were not obtained, since this type of information is rarely recorded or assembled for easy retrieval. Fugitives guilty of major crimes are seldom additionally charged with fraudulent use of false identification, since this is usually only a misdemeanor. In other cases, prosecution for fraudulent use of false identification is not often undertaken, since the fugitive is not a criminal (e.g., minor runaway, illegal alien).

¹See Attachments II and III.

SECTION II

THE FUGITIVE FALSE ID PROBLEM

Classes of Fugitives

Three classes of fugitives are usually associated with the use of false identification. These are:

1. The militant terrorist or revolutionary;
2. The juvenile; and
3. The traditional criminal.

They are discussed below.

The Militant Terrorist/Revolutionary

The militant terrorist or revolutionary has espoused a cause varying from racial protest to overthrow of the government through armed force. Protest actions eventually take the form of criminal activity requiring the militant to "go underground." After going "underground", the militant assumes a false identity to avoid detection and arrest and to remain in a covert status. The false identity is supported by false documents sufficient to create the illusion of authenticity. Activities are continued under the assumed identity until arrest or until the false identity becomes linked to the true identity, whereupon another false identity is assumed. If arrested, the militant may utilize the false identity documents to avoid being connected to previously committed illegal acts.

The Juvenile

The juvenile assumes false identity for a number of reasons. These range from the borrowing of a friend's driver's license to purchase alcoholic beverages or to gain access to a restricted movie, to the acquisition of a means by which to escape from an unhappy home or institutional environment. Juvenile fugitives impose an expense upon society through the additional burden their escapes place upon police and juvenile authorities. However, this type of fugitive is considered outside the scope of the Task Force's deliberations. Unfortunately, a juvenile fugitive seeking to establish a permanent false identity may become involved in narcotics or vice through association with those who possess the capability

to provide false identity documents. Such involvement would bring the juvenile fugitive back under the Task Force's consideration as a criminal.

The Traditional Criminal

The third class of fugitive is the criminal who engages in crime for personal gain. Included in this class are: bad check passers, fraudulent users of credit cards, robbers, rapists, shake-down artists, confidence men, drug traffickers, embezzlers, murderers, illegal aliens, etc. Some of the activities of these criminals and their use of false ID is discussed in great detail in the reports of the Commercial Transactions Task Force (Appendix A2) and the Government Payments Task Force (Appendix A1). Accordingly, only a brief description is given here.

Criminals may assume a false identity before or after the commission of a crime, usually dependent upon the nature of the criminal activity. Some criminal activities are independent of identity (e.g., murder, burglary, theft); some depend upon a known identity, usually factual (e.g., embezzlement); and some are dependent upon assumed identity (e.g., forgery, fraudulent use of credit cards, passport violations, illegal entry into the country). Criminals may carry false identification to avoid being linked to previous criminal activities. Escapees from penal institutions almost always assume a false identity. A growing area of concern is the use of false police identification by criminals to gain access to premises for the purpose of committing crimes such as robbery and rape or to shake down pimps, prostitutes, addicts or homosexuals.

In New York City, false impersonation of police officers is a growing phenomenon. During 1974, incidents involving police impersonators increased by 88 percent. Arrests for this crime increased from 215 in 1973 to 265 in 1974, an increase of 23 percent.

Types of False ID

Types of false identification utilized by all three classes of fugitives are similar. These include: birth certificates, driver's licenses, Social Security cards, Selective Service cards, and credit cards. It is important to recognize that the first four of these are used purely for identification by the fugitive

and are documents which are issued by government entities¹. Birth certificates and driver's licenses are state and local documents; Social Security and Selective Service cards are federal documents.

Other documents which have been used in the establishment of false identity are: marriage licenses, school records, voter's registration cards, medical assistance records, and military identity cards. Since all of these are also documents which are issued by governmental entities, the problem is addressable by government itself.

¹See Appendix A4, Report of the Federal Documents Task Force; and Appendix A5, Report of the State and Local Documents Task Force.

SECTION III
FUGITIVE CRIMES

General

There are a number of crime types which are commonly used to maintain a fugitive or which are the reason for fugitive status in the first place. Some of these crimes are explored in greater detail by the FACFI Task Forces on Commercial Transactions, or Government Payments (Appendixes A2 and A1, respectively). They are discussed in the context of this report because many are repeating crimes which become a source of livelihood to the criminal and are, in fact, necessary to maintain a fugitive status; if forced to work in the ordinary way, many fugitives would have difficulty avoiding detection and arrest. Accordingly, a circular pattern develops in which a crime is committed, sometimes with the aid of false ID, causing the individual to become a fugitive for which continued use of false IDs and accomplishment of false ID related crime is essential.

It is worthwhile, therefore, to consider the nature of crimes in which false ID has some effect. The most prominent types are discussed in the following subsections.

Fraudulent Check Passing

The passing of fraudulent checks has long been an investigative nemesis of all areas of law enforcement. Checks have without question become one of the most important transactional instruments in the world today. A recent publication issued by the Public Information Department, Federal Reserve Bank of New York, reported: "We use checks to pay \$9.00 out of every \$10.00 we spend. Today, there are about 91 million checking accounts in the United States."

The best estimates of check losses through false ID (forgery and counterfeiting) which FACFI has been able to obtain place annual losses at over \$1 billion per year. These estimates have been derived from a Bank Administration Institute study¹ and the results of a special study² on check fraud. Further details on check fraud are contained in Section 4 of the FACFI Final Report.

¹Bank Administration Institute, The Impact of Exception Items on the Check Collection System (Park Ridge, Illinois), 1974.

²Editorial Staff, "How Big is the Bad Check Problem?" Security World, July/August 1974.

Passport Frauds

Recent congressional testimony¹ asserts:

"There is no mystery as to why persons engaged in criminal activities desire U.S. passports and will go to any lengths to obtain them. In most cases, these individuals are already known in their true identities by law enforcement agencies, and some of them are being sought as criminals by law enforcement agencies. To continue their illegal activities, they need new identities."

Also:

"In the fiscal year 1973, we discovered 449 domestic frauds... in addition to the frauds perpetrated by drug traffickers and illegal aliens; we also have frauds perpetrated by militant groups, confidence men, and fugitives."

The example, as set forth above, is one of many which would be cited by this Task Force relative to fugitives' use of fraudulent passports as part of false identification documentation.

Social Security Account Card Frauds

Social Security Account Cards issued today carry the following notation: "For Social Security and Tax Purposes - Not for Identification." Numerous Social Security Account Cards are, however, being obtained daily by fugitives as part of their false identification documentation. Fugitives recently arrested by the FBI and other law enforcement agencies have frequently been in possession of these cards. Investigations have revealed the criminal element utilizes

¹Partial testimony of Mr. William E. Duggan, Chief Legal Division, Passport Office, Department of State, before the Senate Subcommittee to Investigate the Administration of the Internal Security Act and other internal security laws of the Committee on the Judiciary, October 3, 1973.

the Social Security Account Card as an integral part of false identification documentation and in many of the instances such cards were secured in the names of deceased infants.

Narcotics Trafficking

Investigations conducted by all of law enforcement undeniably reveal the narcotics trafficker and false identification are nearly inseparable. Narcotics trafficking is certainly big business. To confirm this, the following statistics covering hashish seizures are set forth.

During the aforementioned hearings¹ conducted by the Senate Subcommittee of the Committee on the Judiciary, Mr. John R. Bartels, Jr., then Acting Administrator, Drug Enforcement Agency (DEA), testified that in 1968, 534 pounds of hashish were seized and in 1972, 30,094 pounds.

During these hearings, Mr. Bartels also testified, relative to a case involving the Brotherhood of Eternal Love (BEL), a drug trafficking organization that,

"Their mode of operation placed heavy reliance on the use of false passports; and with their financial resources and false documents, they achieved complete international mobility. During the period of their successes, we have estimated on the basis of hard intelligence that approximately 24 tons of hashish was smuggled into this country."

Illegal Aliens

Investigations conducted by the Immigration and Naturalization Service (INS) reveal there is an ever-rising trend of immigration frauds. This trend is well-illustrated by the following INS statistics:

"For the Fiscal Year 1965, 5,233 fraud investigations were completed, and for the Fiscal Year ending June 30, 1974, there were 16,676 Service investigations of indicated immigration frauds."

¹Ibid.

INS has also recently reported:

"During the intervening years of rising immigration fraud activity, fraudulent schemes have been encountered incident to nearly every method and category of entry into the United States and have extended to the misrepresentation, altering, and counterfeiting of the majority of entry and status documents issued to aliens seeking entry and/or residence in this country. The arrangers and vendors of such schemes and related documentation normally work independently or in small groups, both in the United States and abroad. Behind these frontmen, however, there is frequently an organized group of document counterfeiters, alterers, and thieves who specialize in stealing valid documents for alteration and copying. It is these groups who keep the vendors supplied with their merchandise."

To further show the magnitude of this problem the following information was set forth in the November 16, 1974 issue of the "Washington-Star News":

"In the 12-month period that ended June 30, the Immigration and Naturalization Service caught 788,185 illegal aliens. Eighty-eight percent, or 693,084 of them, crossed the border without papers. They were 'wetbacks,' although the term is a misnomer because most simply walked across and never came near the Rio Grande."

The remaining 12 percent - 95,061 people - were tourists or students who overstayed their visas and just tried to blend into the community.

Insurance Frauds

The criminal element, utilizing false identification, has also found this area of endeavor quite lucrative. Investigations have revealed that individuals obtain automobile insurance under a number of false identities with several insurance companies. Once the necessary insurance is obtained, these individuals then falsely claim loss due to thefts of clothing, cameras, jewelry, and other expensive merchandise.

As an example, evidence of criminals' involvement in insurance fraud and the use of false ID, the following case is cited.

During the summer of 1974, information was received that an unknown individual in California had requested and obtained the birth certificate of a deceased infant. Subsequent investigation developed that the unknown subject had (1) subsequently secured a United States passport under this deceased infant identity; (2) had a paramour who had also adopted the identity of a deceased infant, and (3) had secured a fraudulent passport using this false identity.

Extensive investigation ultimately identified both individuals, who were subsequently arrested on charges of obtaining fraudulent passports. Once the male subject was identified, it was determined he, under his true name, was in the process of suing an insurance company for over \$5,000,000.00 for an alleged injury; the subject settled for \$75,000.00.

Credit Card Schemes

Credit cards present a fertile field in which the criminal subject, utilizing false identification, can operate. Of the high volume of arrests being made throughout the United States each day, in many instances the arrested subject has in his possession a copy of "The Paper Trip"¹, a well-publicized underground "How to do it" book.

"Paper Trip" explains in detail how to secure and utilize false identification. On page 21, the following is set forth under the caption "Credit Cards":

"Professional ID inevitably includes the full range of commercial cards -- both paper and plastic. Although a few companies are beginning to use customers' photos on the card, as a class they generally have no personal ID information whatever. Your name, signature, account number, and dates between which the card is valid are about as far as they go in providing individual data. The rest is stored in their computer file, based on your original credit application.

"In today's increasingly cashless society, credit cards are becoming the controllable link between people, income, and property. They are immediately accepted for a multitude of specific financial jobs, and in most transactions

¹The Paper Trip, anonymous author, undated.

they are the only ID required. THE PAPER TRIP considers them ID and thus includes here its own ideas on how to obtain them. What you do with them is of course your own business.

"The first rule, unquestionably, is DON'T USE SOMEBODY ELSE'S CARD!! Much too dangerous and criminal. Infinitely better is to get the credit card companies themselves to send you their cards, but under any name you choose. The credit companies and banks who issue these cards are very anxious for your trade, and double anxious to issue the real card to all those who qualify. So the secret is, OBTAIN YOUR OWN CARDS, LEGITIMATELY!!! You do this by studying their brochures and applications to determine more or less what they expect. Even though your new name will have no existing record, a \$400.00 minimum deposit at a large bank will put you on the road to a geometrically expanding credit rating."

Traveler's Check Schemes

Traveler's checks offer the criminally inclined excellent opportunities to finance their criminal activities, as well as afford them financial resources while in a fugitive status.

As evidence of the above, the following example is cited to show the criminal's use of this type of scheme.

During the latter part of 1971, an individual was arrested by a local law enforcement agency on the West Coast for perpetrating a larcenous traveler's check refund operation. At the time of his arrest, the subject furnished a name which was believed to be fictitious. Subsequent investigation revealed the arrested subject had assumed the identity of a living individual, who was not in any way involved in any criminal activities.

For an approximately three-month period, the arrested subject refused to furnish his true identity. He subsequently agreed to cooperate with police authorities and at that time furnished his true identity.

The arrested subject, when interviewed in detail, confessed his extensive involvement, during 1970-1971, in a fraudulent traveler's check scheme in which he used a number of false identities, some fictitious and some of deceased individuals. The subject advised that during the year he used eighty to one hundred different false identities. He added that during his most prolific

activity, he used approximately thirty different identities in almost daily refund frauds. From the monies obtained, the subject was able to finance his criminal status with considerable ease.

Automobile Theft Rings

Investigations have revealed that automobile thefts are constantly being perpetrated by criminals operating under the protection of false identification. The following is a case in point.

During the early part of 1974, an individual was arrested on the West Coast on a charge of obtaining a fraudulent passport. Investigation revealed this individual had assumed the identity of a deceased infant and had completely documented this identity, which included the securing of a fraudulent passport. Following the arrest of this individual, further investigation revealed he had apparently been directly involved, since 1968, in a car theft ring involving expensive automobiles. There is every indication that as many as 55 to 60 vehicles, valued from \$15,000.00 to \$20,000.00 each, were involved in this operation.

The FBI reports¹ relative to interstate automobile theft rings:

"Interstate automobile theft rings operated by skilled professionals continued to receive a large measure of FBI attention under the Interstate Transportation of Stolen Motor Vehicle (ITSMV) Statute in Fiscal 1973.

"A multimillion-dollar auto theft ring investigation was successfully concluded on May 25, 1973, when a Federal Jury in Bowling Green, Kentucky - after hearing testimony for eight weeks from 982 witnesses - returned guilty verdicts on 19 persons on the charge of conspiring to violate ITSMV Statute. Two other subjects previously had entered guilty pleas.

"The trial culminated more than two years of investigative work by the FBI in cooperation with state and local law enforcement agencies.

¹1973 Uniform Crime Reports.

"During Fiscal 1973, FBI investigations of ITSMV violations resulted in 2,017 convictions. Sentences imposed amounted to 3,934 years' imprisonment, 2,093 years in probationary sentences, and 716 years in suspended sentences. Fines totaling \$95,900 were assessed. Some 1,154 ITSMV fugitives were located."

Bank Fraud and Embezzlement

Criminal fugitives have not neglected this area of endeavor in their criminal activities. Each day, investigations show that individuals are traveling from state to state establishing bank accounts under assumed identities. Once such accounts are opened, they use such accounts to support a variety of criminal endeavors, such as check "kiting," split deposit fraud, and loan frauds.

The 1973 FBI Uniform Crime Reports included the following information relative to this matter:

Some 1,064 convictions resulted from FBI investigations as amounts of money involved in bank frauds and embezzlements continued to increase.

These FBI investigations¹ vary from inquiries into mysterious disappearances of nominal amounts of money to complaints involving defalcations of major sums.

During the past decade, the number of convictions in these cases has almost doubled - 577 in Fiscal 1963, as compared to 1,064 in Fiscal 1973. The amounts of shortages have increased yearly, from \$14.1 million in 1963 to \$135.6 million in Fiscal 1973. The number of cases reported also has climbed over the decade -- from 2,469 to 6,787.

White collar crimes -- offenses committed by persons in a responsible position in government and private enterprise -- increased dramatically during the past fiscal year.

In a report to the Commercial Transactions Task Force, the Washington, D.C. Police Force assert that about 15 percent of the embezzlement cases which come to their attention² involve the use of false ID. It can be reasonably inferred, therefore, that the use of false ID is a nontrivial component of this crime.

¹It should be noted that a majority of fraud and embezzlement cases are not subject to FBI investigation.

²Appendix A2. Table II.

There is increasing evidence of a new form of false ID bank and business embezzlement found involving computer controlled accounting of credit transactions. In this context, a computer expert and bank executive¹ recently stated:

"The base form of an asset is no longer necessarily a 40 ounce gold bar; now assets are simply magnetic wiggles on a link."

The fraudulent use of computer keys, codes, passwords and the like, and abuse of computer files, data, and operating systems is a false ID crime and one with enormous loss potential.² Further, these frauds and embezzlements are difficult to either detect and counter or protect against, and there is some evidence³ that victimized institutions are often reluctant to bring charges against their own employees for fear of losing public confidence.

There is also evidence that this method of fraud is either growing rapidly or being detected with greater frequency, and that criminal organizations are becoming involved as well as technically clever and innovative individuals.⁴

In summary, we repeat the conclusion of a recent newspaper article⁵:

"The potential rewards and the seeming ease of escaping any heavy punishment have made credit fraud an enormous secret industry."

¹Richard Mills, Vice President, First National City Bank, "Waiting for the Great Computer Rip-Off," Fortune, July 1974.

²Op. cit., Fortune, July 1974.

³Ibid, one reported case involved a loss of \$5 million. A cited 1971 study found that twelve cases of computerized bank embezzlement averaged \$1.09 million apiece - about ten times the average embezzlement loss.

⁴Ibid.

⁵"New Credit Risks: Loan Swindle, Subverting Data Banks Spread," The Wall Street Journal, April 18, 1976.

Internal Security

Investigations clearly reveal the use of false identification plays a prominent role in internal security areas. This is evident in information set forth in the 1973 FBI Annual Report, under the subcaption "Weatherman," which reads, in part, as follows:

"Weatherman began in 1969 as a faction of the militant Students for a Democratic Society (SDS). Thereafter, Weatherman quickly evolved into a separate Marxist group which is dedicated to the violent overthrow of the government. In early 1970, Weatherman members abandoned their offices and residences and entered underground status. They did so to better pursue armed struggle against the Government.

"Since entering underground status, Weatherman has used sophisticated techniques of false identities and clandestine communications.

"During a speech made on November 11, 1974, when making reference to Weatherman, FBI Director Clarence M. Kelley commented, 'Since early 1970, the Weather People have been underground. By underground, we mean their adherents live under aliases, using false identification papers and fabricated life histories.'"

With every passing day, investigations vividly reveal criminals are entering fugitive status on an ever-rising basis. This aspect is certainly borne out by the following data as reported in the 1974 FBI Annual Report:

"An all-time high of 37,891 FBI fugitives were located during Fiscal 1974. Those apprehended included bank robbers, kidnapers and deserters, as well as felons, wanted by local authorities. Some 3,478 were sought at the specific request of state and local authorities for violations of the Fugitive Felon Act.

FBI Director Kelley states:¹

"To the law-abiding citizen, the specter of expanding lawlessness cannot help but provoke anguish - and for good reason. It is his tax dollars that have financed the war on crime, and it is his safety, possessions, and community that are mainly threatened by lawlessness...

¹"Law Enforcement Bulletin," Vol. 43, No. 11, November 1974.

"To combat crime effectively requires at the outset a realistic examination. One reality of crime is that repeat offenders are at the core of the problem. Studies of criminal histories reveal convincing evidence that as much as two-thirds of all offenses are committed by recidivists -- persons who have been arrested for and convicted of crimes previously."

SECTION IV

PRELIMINARY RECOMMENDATIONS

Since most of the type of documents used in the establishment of false identifications are issued by governmental agencies, the following steps could contribute to a solution of this problem:

1. Applicants for any of the type of identification documents listed above should be required to provide adequate proof of identity prior to receiving the requested documents;
2. More rigid safeguards should be imposed upon the storage of blank forms so they might be less prone to theft;
3. The quality of identification documents could be improved so that falsification through alteration or counterfeiting would be more difficult. This could be accomplished through the incorporation of a photograph, a fingerprint, and a coded number which could incorporate identity features of the issuee;
4. The public could be better educated in methods for verifying the identity of the identification holder and the reasons why they should be concerned about this problem;
5. Procedures for checking criminal identity upon apprehension could be improved so that the true identity of the suspect could be ascertained prior to the release from custody;
6. Stiffer laws could be passed with regard to users of false identity. Such laws could include:
 - a. Removal of applicability of the statute of limitations when the use of false identification is involved in a crime;
 - b. Refusal of probationary sentences to users of false identification in the commission of a crime;

- c. Stiffer sentencing of users of false identification; and
7. Laws could be passed which would impose severe penalties upon anyone who is convicted of manufacturing, selling, distributing, or passing false identification documents.

ATTACHMENT I

COMPOSITION OF THE FUGITIVES TASK FORCE

The following members comprise the Task Force.

Chairman

Mr. Emil L. Schroeder	Federal Bureau of Investigation Room 4427, J. Edgar Hoover Bldg. Washington, D.C. 20535 (202) 324-4587
-----------------------	---

Members

Mr. Thompson Crockett	International Assn. of Chiefs of Police
Mr. Elmer C. Cone	American Bank Note Company
Mr. William B. Wharton	Passport Office, Department of State
Mr. Albert H. Solomon, Jr.	Committee on Judiciary, U.S. House of Representatives
Mr. Truman H. L. Walrod	National Sheriff's Association
Lt. Glenn W. Ramey	Metropolitan Police Dept., Washington, D.C.
Mr. Louis B. Sims	Interpol

ATTACHMENT II

MATERIAL IN TASK FORCE FILES

EXCERPTS FROM RESPONSES OF SHERIFF'S DEPARTMENTS AND MUNICIPAL
POLICE DEPARTMENTS

Summary

An evaluation of the responses to survey letters sent by the Task Force on Fugitives to a number of sheriffs and metropolitan police departments located throughout the United States unmistakably confirms the fact that these police organizations are being confronted with the criminal's ever-increasing use of false identification. It is further evident that these law enforcement agencies are experiencing considerable investigative difficulties as a direct result of the criminal's adoption of the false identity technique.

Law enforcement agencies, when responding to surveys requested by this Task Force, specifically pointed out that they are greatly concerned over this problem and that solutions to it must be sought.

Responses were received from:

1. The City of New York Police Department;
2. City of Chicago - Department of Police;
3. Los Angeles Police Department;
4. Las Vegas Metropolitan Police Department;
5. Montgomery County Sheriff's Department, Dayton, Ohio;
6. Denver Police Department;
7. Baltimore Police Department;
8. Boston Police Department;
9. San Jose (California) Police Department;
10. San Diego Police Department; and
11. New Orleans Department of Police.

ATTACHMENT III

INTERPOL RESPONSE

International

The General Secretariat, International Criminal Police Organization - Interpol, through the United States National Central Bureau - Interpol, furnished information concerning the problem of false identification on an international basis, which includes counterfeiting and/or altering of passports, drivers' licenses, and other identification cards and the methods which appear to provide a maximum degree of protection against counterfeiting and/or altering of these documents.

For the alterations, a legitimately issued document is obtained from the rightful owner by theft or other means, or a legitimate document is obtained from the issuing agency by fraudulent means, usually followed by alteration of the text and signature of authentic passports or other forms of identification, such as drivers' licenses, identity documents, letters of credit, and so forth. The forgers principally use three methods: scraping, erasing and washing, or by the addition or substitution of lines, letters, photographs or entire pages.

For the counterfeits or complete production of a false document, the counterfeiters use basically the same methods/procedures as currency counterfeiters, such as acquisition of a genuine document followed by obtaining plates or type molds by photograph or moldings, manufacture of stereotype plates by engraving or printing, using typographic or planographic methods.

Methods which are considered to provide a maximum degree of protection against counterfeiting or altering documents are as follows.

1. At the Manufacturing Stage

An identification document should be printed on special paper, "protected," made of pure pieces and producing no fluorescence under ultraviolet light. This paper should be of strictly maintained thickness and quality and should have well-patterned watermarks.

Security indications, such as fluorescent "planes," can be incorporated into the paper during its manufacture.

The printing should be carefully done, preferably using typographic methods. A security background, printed with thin or reactive ink, in the form of cartridges, in the areas to be filled out by identification data or signatures, will greatly complicate modifications through washing and scraping.

The numbering should be typographically done with a numerator with specially engraved characters, having original designs that are easily recognizable; for numbering purposes, the use of fluorescent ink will permit rapid verifications, using very simple materials.

The cover should be strong, semi-rigid and, if possible, include a seal in relief.

The cover and pages should be bound in such a way that it is difficult to remove or add pages (the use of special rivets seems advisable).

2. At the Stage of Issuing the Document

The use of indelible ink of a special sort is desirable, but in practice difficulties might be encountered.

The lines containing the identification data should be completed by conventional signs, so as to avoid the addition of letters.

The use of a dry stamp is indispensable, but it should have subtlety (fine and closely drawn lines along the border, for example) which makes it difficult to pick up the print of the dry stamp.

The photograph should be attached with glue that is insensitive to heat, water, and most solvents; synthetic polymerized glues seem to provide the most guarantees.

Finally, a process which seems likely to prevent the substitution of photographs consists in placing the print of one of the holder's fingers partly on the passport and partly on a border of the photograph.

A review of the problem of false identification on an international basis since 1947 reveals that it has been a continuing problem.

At an Interpol Symposium held in December 1974, the problem of false drivers' licenses was considered. The delegation from Spain reported that through international cooperation they had recently detected a large number of counterfeit drivers' licenses of Portugal, France, Germany, Morocco, Venezuela, and Argentina. The ensuing discussion revealed that of some 20 countries represented, almost every country has a large number of false drivers' licenses in existence. They ranged from complete counterfeits to genuine licenses altered and genuine licenses obtained through the use of false identity documents. The use of these false driver's licenses, frequently accompanied by the use of fraudulent passport, provided the basis necessary in security frauds, leasing of vehicles and subsequently stealing same, and all other types of criminal activity.

APPENDIX A4

**REPORT OF THE FEDERAL IDENTIFICATION DOCUMENTS TASK FORCE
ON THE
SCOPE OF THE FALSE IDENTIFICATION PROBLEM AND
PRELIMINARY RECOMMENDATIONS FOR SOLUTIONS**

Submitted to

**Federal Advisory Committee On False Identification
David J. Muchow, Chairman**

May 1976

TABLE OF CONTENTS

	<u>Page</u>
SECTION I - INTRODUCTION	A-113
Purpose	A-113
Scope	A-113
Data Gathering	A-114
Evaluation of Data	A-115
SECTION II - THE FALSE ID PROBLEM	A-117
Application Phase	A-117
Eligibility and Enablements	A-117
Visa	A-117
Immigrant Visa	A-117
Non-Immigrant Visa	A-118
Alien Registration Receipt Card (Form I-151)	A-118
Nonresident Alien Mexican Border Crossing	A-118
Passport	A-119
Application Fraud Estimates	A-119
Analysis of Detected Application Fraud Data	A-121
ID Documentation and Verification	A-122
Visas	A-122
INS Documents	A-123
U.S. Passport	A-124
Customs Verification of Entry Documents	A-124
"Use" Phase	A-125
Fraudulent or Incorrect Usage	A-125
Visas	A-125
Entry Without Visas	A-127
Passport Frauds	A-128
Summary	A-128
INS Documents	A-129
False ID "User" Profiles	A-137

TABLE OF CONTENTS
(Continued)

	<u>Page</u>
SECTION III - SOCIETAL IMPACT AND COSTS	A-139
General	A-139
Welfare Costs	A-139
Health Service Costs	A-140
Income Tax Losses	A-140
Balance of Payment Losses	A-140
Illegal Alien Jobs	A-140
Criminal Activity	A-141
Smuggling	A-141
Fugitives	A-143
False ID Investigations and Prosecutions	A-144
SECTION IV - COUNTERMEASURES TO CRIMINAL USE OF FALSE ID	A-147
General	A-147
Detection of User Fraud	A-148
False Alien Documentation	A-148
False Entry Without a U.S. Passport	A-149
Application Phase	A-150
Visa Office	A-150
INS	A-151
Passport Office	A-152
Use Phase	A-152
Visa Office	A-152
INS	A-153
Customs Service	A-154

TABLE OF CONTENTS
(Concluded)

	<u>Page</u>
SECTION V - RECOMMENDATIONS FOR AMELIORATION OF THE FALSE ID PROBLEM	A-155
General	A-155
International Agreements	A-155
Domestic Practices	A-155
Prosecution of Cases	A-155
Inter-Agency Cooperation	A-156
Inter-State Activities	A-156
Training and Education	A-157
Legislation	A-157
ATTACHMENT I - ORGANIZATIONAL COMPOSITION OF TASK FORCE	A-158
ATTACHMENT II - SENATE BILL NO. 391 - COMMITTEE ON JUDICIARY, STATE OF NEVADA	A-159

LIST OF TABLES

TABLE NUMBER		<u>Page</u>
I	VISAS	A-120
II	INS DOCUMENTS	A-120
III	U.S. PASSPORT	A-121
IV	FALSE ID USE BY ALIENS IN VISA FRAUD	A-127
V	USER FRAUD	A-128
VI	FALSE ID USER PROFILES	A-138
VII	USE OF FALSE ID - NARCOTIC SMUGGLING	A-142

Report of the Federal Identification Documents Task Force

on the

Scope of the False Identification Problem &

Recommendations for Solutions

SECTION I

INTRODUCTION

Purpose

The Federal Documents Task Force was formed to examine the use of personal documents issued by the Federal government in false identification assisted crimes. Both an identification of the scope, crime patterns and societal cost of the problem and suggested solutions are main elements of the work of this group.

Scope

There are many documents of interest to the Task Force. These include particularly The Passport, the Alien Registration Receipt Card¹, the Nonresident Alien Mexican Border Crossing Card², and the Immigrant and non-immigrant Visas affixed to passport documents. For purposes of this study, the visa is considered a document.

The principal Federal organizations associated with either the original issuance of these documents or their subsequent evaluation are: The U.S. Passport Office (PPO), the Immigration and Naturalization Office (INS), the Customs Bureau and the Department of State.

¹Immigration and Naturalization Service (INS) Form I-151.

²INS Form I-186.

Other Federal agencies, bureaus and offices concerned with the false ID problem in one fashion or another include the Department of Transportation, the U.S. Coast Guard, the Selective Service System, the Drug Enforcement Agency (DEA) and the Federal Aviation Administration, all of which are represented on the Task Force.

Data Gathering

Data acquisition was mainly by structured survey. Useful additional information of direct importance to the work of the Task Force was extracted by some organizations (notably the Visa Office and the INS) from extant reports and statistical summaries.

In general, the fraud problem has been divided into three components as follows:

1. Application Frauds, dealing with various misrepresentations in acquisition of documents in the ordinary way;
2. Document Frauds, having to do with alteration or counterfeiting of the documents themselves; and
3. User Frauds, concerning impersonation and imposture in the conduct of transactions involving the use of IDs.

There were several primary sources of data. These included:

1. In-house studies made by the INS;
2. Surveys and extant data by the Visa Office;
3. Case sampling by the DEA; and
4. Case studies by the Customs Service.

The Visa Office contacted all visa issuing posts and solicited the views of Foreign Service and Consular Officers associated with the visa issuing process. Based upon this information, maximum and minimum projections were made bounding the visa fraud problem.

The INS followed the same pattern but provided, rather than a range, firm estimates of the extent of the problem based on data collected by the service.

The report from the DEA was based on a random sampling of 589 cases from which 17 were identified as involving false ID.

Data supplied by the Customs Service is based entirely on specific cases; all involved alien traffickers.

Passport Office data was similarly compiled from specific cases.

Evaluation of Data

Hard data on the false ID issue is not often readily at hand. All contributing sources note the difficulty of retrieving false ID data with precision and surety. In many cases, recourse was made to informed opinion of officials long associated with the problem.

Proper interpretation of hard data which does exist is further hampered by problems of detection. The Passport Office, for example, has data on detected passport frauds; the extent of successful frauds can be only guessed at.

Estimation of societal cost, either directly accruing from false ID crimes or indirectly in benefits, services, the value of activities of alternate to false ID investigation and the like, are as spotty as the false ID estimates themselves. The Visa Office reports:

"...there is great need for statistical data on the scope and dollar impact of the fraudulent identity problem in general. The small fraud unit operating within the Visa Office has not at this stage had the opportunity or the manpower to collect statistics on the problem from a wide range of sources. The officer issuing visas overseas is often overworked and has neither time nor resources to undertake the kinds of investigations and surveys which would produce the needed information. VO is in the process of seeking additional data concerning fraud from the INS and has requested additional manpower in the area of fraud."

In many cases, the ID fraud is not reported as having been considered "peripheral" to the major crime committed. The Customs Office reports:

"The exact data on the incidence of use of false identification is not obtainable because our statistical procedures do not provide for its retrieval. False identification is

the modus operandi used by the perpetrator to commit the Customs violation, i.e., smuggling narcotics, etc. Customs violations are carried in over thirty investigative case categories and reported under same."

Further, there are anomalies in the data reported and the estimates arrived at by expert opinion. For example, the DEA sample, admittedly limited, suggested a figure of about 3% as representing the degree of false ID association with the international cocaine trafficking cases studied. The expert opinion of a DEA official, on the other hand, was that 80-85% of all drug trafficking cases were attended by false ID use. Customs data suggest 79%. All respondents agree that false ID does represent a problem and that the documents their organizations issue, certify, inspect, or otherwise administer are subject to this abuse. Further, there are strong indications in the data that do exist, that false ID abuse of the studied documents is increasing year by year, a phenomena more fully explored in subsequent parts of this report. The societal effect in either dollars or any other measure is less documented and documentable since many of the effects are secondary or tertiary.

There is general agreement among the expressed suggestions for solution to or amelioration of the problem, however, despite different organizational viewpoints and perceptions of the problem. These matters are also discussed in subsequent sections of this report.

The false ID problem is intimately associated with criminal activity on both the purely domestic and international spheres. Some portion of the costs of these illicit activities must be accordingly attached to false ID, which is without any serious question, an enabling influence of substantial aid to the conduct of this activity.

SECTION II
THE FALSE ID PROBLEM

The documents of concern to this Task Force fall generally into two classes: those which enable international movement by individuals either into the U.S. or out of it across international boundaries; or those which entitle individuals to certain social benefits. In the former class are the U.S. Passport, various visas, alien registration documents and the like. In the latter category is the Social Security Registration Card.

There are other Federal documents, U.S. military ID for example, which may be subject to occasional false ID abuse but the preponderance of evidence suggests that most of the false ID problem is associated with the passport, alien documents, and the Social Security card. In order to adequately set forth the false ID problem relative to the documents of interest, it is necessary to expand on a number of issues relating to their proper and improper acquisition and use. Accordingly, the following material addresses these issues. Included are: descriptions of the ordinary document application process including the ID documentation required by the issuing agency or office; the nature and extent of the verification process employed; the degree of fraud detected; and the intended use of the documents. Also included are discussions of document abuse, including particularly the criminal activities in which these documents play a role.

Application Phase

The following material is presented document by document.

Eligibility and Enablements

Visa

Immigrant Visa - The immigrant visa permits the recipient to settle in the U.S. as a permanent resident, to engage in gainful employment as and where he chooses, and eventually to become an American citizen. In general, the immigrant visa applicant must establish that he is entitled to an immigrant visa either as the close relative of an American citizen or permanent resident alien; or that he is a worker or professional whose skills are in demand in the U.S. as certified by the Department of Labor; or that he falls into one or another category that would entitle him to an immigrant visa (i.e., longstanding U.S. government employee, refugee).

Non-immigrant Visa - The non-immigrant visa permits an alien to apply for entry into the U.S. for a temporary stay for a particular purpose: tourism, business, study, transit, international organization employment, crewmember, for example. The vast majority of holders of these visas are not permitted to work and are required to have a residence in a country outside the U.S. which they have no intention of abandoning. The application requirements for most kinds of non-immigrant visas include an application form, a photograph, a valid passport, and proof of entitlement to the non-immigrant status for which application is made.

Alien Registration Receipt Card (Form I-151)

While INS issues many different documents, this discussion will be limited to Form I-151, Alien Registration Receipt Card, and Form I-186, Nonresident Alien Mexican Border Crossing Card.

The Form I-151 is a part of the Immigrant Visa and eligibility therefore is determined by the American consular officer abroad. The entry data is added to the form at the time of the alien's entry to the United States. This card is evidence of the alien's registration and admission as a lawful permanent resident. Aliens having such cards are entitled to take employment in the United States.

Nonresident Alien Mexican Border Crossing Card (Form I-186)

A Form I-186 may be issued to any eligible citizen of Mexico for entry to the United States as a temporary visitor for periods not to exceed 72 hours and is limited to travel within 25 miles from the Mexican border. Holders of this card are not entitled to take employment in the United States. The citizen of Mexico must apply in person for such card to an Immigration Officer at a border port or to an American Consular Officer in the interior of Mexico. He is interrogated as to his eligibility for such card and must support his application with evidence of Mexican citizenship and residence. As a minimum, he must present a regular Mexican passport, a provisional passport issued by the governor of a state in Mexico or a Mexican Form 13, a document issued by the Mexican Immigration Service.

Other ID evidence considered would be previously issued INS documents, birth and baptismal certificates.

Passport

A person who desires to obtain a U.S. passport must apply for it using a stipulated form which must be executed before a person authorized by the Secretary of State to accept passport applications in the U.S. or abroad. Under certain stipulated conditions, a person who has been issued a U.S. Passport within 8 years may complete an application and send it to the Passport Office by mail. The conditions of such "mail-in" applications are strict -- to prevent possible fraud. At the present time such mail-in applications do not present a fraud problem and constitute about 12% of the total volume.

Since U.S. passports may be issued only to nationals of the U.S., applicants must prove by documentary evidence that they are nationals. Also they are specifically required to establish their identity. The nationality requirements are statutory (22 USC 212).

The identity requirement is specifically mentioned in the Regulations (22 CFR 51.28).

The application and evidence are adjudicated by experienced Passport Examiners. If nationality and identity are satisfactorily established, a passport is issued. If not, the applicant is required to submit additional evidence or an investigation is undertaken.

Application Fraud Estimates

Estimates of the scope of the fraudulent application problem are given in Tables, I, II, and III below for visas, INS documents and U.S. Passports, respectively. For visas and INS documents, the degree of the fraud problem is estimated as a fraction of the total number of applications processed. For Passport another figure is given: Applications per detected fraud.

TABLE I

Visas

<u>Document Type</u>	<u>Applications Per Year</u>	<u>Rejected¹ Applications</u>	<u>False² Applications (est.)</u>
Immigrant Visa	325,000	20,000	6%
Nonimmigrant Visa	3,000,000	220,000	7%

TABLE II

INS Documents

<u>Document</u>	<u>Applications Per Year</u>	<u>Counterfeits Detected</u>	<u>Altered Cards Detected</u>	<u>Imposter Use of Unaltered Cards Detected</u>	<u>Percentage of False Application</u>
Alien Registra- tion Receipt Card (Form I-151)	364,000	4,074	1,361	2,086	2%
Nonresident Alien Border Crossing Card (Form I-186)	170,331	585	1,623	6,160	5%

¹In most cases, although outright fraud may not have been attempted, the applicant has sought to deceive the consular official in some way.

²Estimated at 5-10% of the rejected applications. The larger figure is used in Table I.

TABLE III

U.S. Passport

<u>Year</u>	<u>Applications</u>	<u>Applications from High Fraud Potential Groups¹</u>	<u>Detected Application Fraud</u>	<u>Applications Per Detected Fraud</u>
FY71	2,311,789	462,356	288	1605
72	2,605,321	521,064	300	1736
73	2,769,549	553,903	499	1233
74	2,471,461	494,292	553	893

Analysis of Detected Application Fraud Data

Since application fraud is only a part of the false ID problem and the data given are based on detection of fraud at application, the true figures are probably higher than those shown. For entry visas and the two most important INS documents, these figures range from 2% to over 7% of total applications.

Passport application fraud has, over the period cited, increased 92% while the number of total applications increased by only 6.9%. The Passport Office, however, notes that a fraud detection training program was begun in the spring of 1972 and has resulted in the increased detections in FY's 73 and 74.

It is not possible to assess with surety either the extent of application fraud for the subject documents or the time trend from the data presented here. It should be noted, however, that the numbers are not small and the estimates conservative.

¹It was determined that a high fraud potential group can be defined consisting of first time, native-born applicants between age 18 and age 40. There is no known fraud in official government travel applicants and none of any magnitude in family group applications. Combining all these factors, the high fraud potential group is estimated at 20% of total applicants.

The degree of concern which should be attached to these figures must rest with a linking of fraudulent immigration, entry into the U.S. or passport acquisition with specific criminal activities and their societal impact. This issue is treated in subsequent sections of this report.

ID Documentation & Verification

There are a number of documents which may be used to establish ID and status for purposes of acquiring visas, INS documents and passports. In the case of U.S. entry documents which may originate from virtually any area of the world and be processed by consular officials remote from the U.S., document verification may be especially difficult because of the sheer variety of document types encountered. The following discussions set forth these issues in some detail.

Visas

The fact that the whole process of application for a visa and verification of identity factors occurs outside the U.S. presents special problems. In many cultures of an individual name itself is a source of difficulty: surnames may be unknown, or rarely used; a person may be given only one name if he comes from a relatively undeveloped area; there may be comparatively few names in use, so that duplication of name is common; names may be changed for luck, religious reasons, whim, marriage, when honors are granted or trials successfully undergone; names written in scripts other than the Roman may be Romanized in different ways at different times, and so on. Conditions and cultures in many countries make reliable documents hard to obtain or difficult to verify or assess: foreign officials who issue documents may be bribed or persuaded to issue false documents; private persons (relatives, employers) may have no interest other than that of the requester in mind and may issue a false letter or document attesting to an ability, an employment record, a financial condition, a relationship, that may have no bearing on reality. Many life events in non-western societies occur without benefit of civil documentation; in other societies the requirement of documentation is honored largely in the breach. Language is often a problem in that translations of documents are time-consuming; in addition, letters or certificates in English may have been signed by honest officials or private individuals who were deceived by the applicant and had no real idea what the document contained; data keeping on the part of foreign national and local governments may refuse to assist the consular officer in attempting to verify government documents; applicants may be unable or unwilling to return to their native country to obtain documents for fear of

persecution, and the issuing authority may have no interest in providing documents to such persons.

Examination of the alien identity and status documentation always or frequently required to obtain either the Immigrant or the Non-Immigrant Visa reveals:

1. The variety is enormous ranging from birth certificates, passports and national identity documents to property deeds, bank books, divorce and marriage certificates and vehicle registrations. There are nineteen types noted by the Visa Office.
2. Of the nineteen ID document types always or sometimes requested, thirteen are reported to be subject to frequent fraudulent use, five sometimes and only one (the Selective Service Card) with no fraudulent use reported.

Pressures of workload and shortages of investigative personnel at many posts often preclude verification of the authenticity of documents except in cases where there are clear indications of fraud. Routine verifications are generally not possible, though random checks of apparently authentic documentation are sometimes carried out. However, in high fraud areas, some routine verifications of documents are made and investigations launched when indicated.

INS Documents

Identity evidence is required prior to the issuance of any of the INS documents. It consists of previously issued INS documents; immigrant and non-immigrant visas; official foreign documents including birth certificates, police records, military records, marriage licenses; divorce decrees; death certificates; fingerprint checks; affidavits; depositions; and identifying witnesses in some cases.

Authentication of documents is dependent on the specific type of document presented with an application. INS personnel are trained and experienced in questioning and interrogation techniques. This method of examination is generally sufficient to establish the validity of a document and legitimacy of the bearer. Additional authentication measures, including a field investigation, are taken if reasonable doubt exists after questioning an individual.

U.S. Passport

The United States passport is, by definition, a document of identity and nationality. Consequently, a person applying for such document must establish, by documentary evidence, these two factors. Identity is normally established by a reliable document issued by a governmental agency which contains a photograph or physical description and signature. U.S. citizenship is established generally by the submission of a certified copy of a birth certificate showing birth in the United States. The applicant must fill in a passport application.

The evidence of identity and birth is examined by the passport agent accepting the passport application along with the information furnished in the passport application. If the passport agent is satisfied with his short interview of the applicant and his examination of the documentation of identity and citizenship, no verification procedure is undertaken. If, however, the passport agent notices what are called "symptoms of fraud," verification procedures will take place. This verification will depend upon the questionable factors which the agent notices. The verification procedures can be in the nature of telephone or written communication throughout the United States to the source of the documents submitted. It could also include the same type of communication to verify addresses or references given in the application.

In some cases, the verification is undertaken by the investigatory agency for the Passport Office.

Customs Verification of Entry Documents

The Customs examination is the last step encountered by the arriving passenger before entry is made into the United States, whether he is a citizen or an alien. A U.S. citizen is processed by the Passport Office and furnished a passport for travel abroad. An alien is processed abroad by the State Department for issuance of a non-immigrant visa to enter the U.S., and his foreign passport is examined by Immigration at the time of entry. Therefore, the Customs Service does not question the validity of a Declaration as identification, unless a Customs violation is detected, (i.e., narcotic smuggling). Passports are the document most frequently involved in the use of false identification.

"Use" Phase

General. Both non-immigrant and immigrant visas are used to apply for entry into the U.S. They are presented at ports of entry to inspection of the INS. The Alien Registration and Mexican Border Crossing documents are used to effect entry into the U.S. or to remain here and take employment.

A U.S. Passport is used to enter and/or depart the U.S. (8 USC 1185) or primarily for use in traveling or residing abroad. The Supreme Court has stated that the U.S. Passport is a political document which, in effect, identifies the bearer as a national of the United States and requests foreign governments to give to the bearer all lawful aid and protection. In cases of civil strife abroad, the U.S. Passport can be the difference between life and death. It is also the document in which foreign governments place their visas showing that the bearer is entitled to enter such foreign country.

Aside from its official use as described above, it has common usage as identity evidence in commercial transactions in the U.S. and abroad.

Fraudulent or Incorrect Usage

Visas

Both kinds of visas have one primary purpose and use: to permit the bearer to apply to enter the United States. Immigrant visas and a few categories of non-immigrant visas permit the bearer to be gainfully employed in the U.S. But some persons who enter the U.S. on visas which do not permit them to work nonetheless seek and often find employment. If an alien is discovered working illegally, the penalties levied on him and on his employer are not severe, and the chances that he will be detected are small. These aliens who seek and find unauthorized employment take jobs that American citizens and those legally authorized to accept employment could fill. In addition, many illegal aliens pay no taxes on their illegal earnings and consume substantial welfare benefits. The societal impact of illegal immigration is discussed in Section III of this report.

It is difficult to attach a precise figure to the visa aspects of the illegal alien problem. Not all illegal aliens presently in the United States entered on visas; in fact, if INS apprehension statistics are representative of the illegal alien population as a whole, probably no more than 10-15% of the illegals presently in the U.S. had any contact whatsoever with the visa issuance process.

In addition, not all aliens who become illegals intended to violate their status when they applied for visas and their applications had no fraudulent aspects. Not all applicants who did intend to violate status had to resort to identity fraud to do so.

1. Counterfeit non-immigrant visas - A survey of reported counterfeit visas for the period March 1970 through August 1972 revealed 287 confirmed cases. It is generally assumed that where there is one counterfeit, there is more than one, and that for every counterfeit detected, others escape detection. The estimated number of counterfeits for the countries and time involved in the survey (estimates made by the posts involved in the reported cases) range from 1,800 to 7,000. If it is assumed, based on this survey, that the average number of attempts (some successful) to use counterfeit visas ranges from 90-350 per month, the average is 1,080 to 4,200 per year.
2. Refusals - At least 250,000 visa applicants are finally refused visas each year. It is conservatively estimated that 5-10% of these refusals involve some element of identity fraud¹. This adds 12,500 to 25,000 to the total.

Table IV, below, gives the Visa Office's estimated breakdown of the false identification problem:

¹Some visa-issuing posts put this figure at 50% or higher.

TABLE IV

False ID Use by Aliens in Visa Fraud

	<u>Annual False ID Use by Aliens</u>	
	<u>Low Estimate</u>	<u>High Estimate</u>
1. Counterfeit visas	1,080	4,200
2. Aliens Apprehended	4,000	4,000
3. Aliens not Apprehended	8,000	20,000
4. Changes of Status	2,250	2,250
5. Refusals	12,500	25,000
6. Aliens Excluded	<u>26,500</u>	<u>26,000</u>
Total	54,330	81,950

The scope of the false identification problem as it pertains to visas is thus 50,000 to 80,000 instances per year of the use of false identification. The former figure is a conservative estimate and the latter a moderate estimate of the scope of the problem.

Entry Without Visas

It has been estimated that there are from four to twelve million illegal aliens currently in the United States. Six to eight million is now the official INS estimate. Although the preponderance of these aliens are believed to have effected illegal intry between the ports of entry along the Mexican border, many have effected their entry into the United States with false identification. A larger number have utilized false documenta-tion to avoid detection while in the United States. The presence of this volume of illegal aliens in the United States impacts heavily on the INS, Department of State and many other Federal, state, county and city agencies.

Passport Frauds

False identification in passport frauds may be divided into two areas of concern: the United States passport and the foreign passport. Either type of passport is readily accepted on an international basis as the travel document for a person's identity and nationality. However, the fraudulent U.S. passport user is primarily implicated with false identification obtained from within the U.S., whereas the fraudulent foreign passport user is primarily implicated with false identification obtained from without the United States.

It is assumed that each United States passport issued is used many times in traveling from country to country as well as entering and departing the U.S. This obviously amounts to many million uses since there are over 10 million valid U.S. passports outstanding.

Summary

A feeling for the distribution of ID fraud by document type and by type of fraud (Alteration, Counterfeit, or Imposter) is given in Table V below. In Table V, the entries are in percent of detected frauds committed. It should be noted that the distribution of fraud shown in Table V most probably reflects the ease with which these frauds can be committed. If, for example, the INS documents were to be made harder to counterfeit, the 29% of presently detected counterfeits might be expected to drop with a corresponding rise in the other categories. Again, it should be emphasized that the data of Table V imply little of the true distribution of frauds since undetected frauds are not included.

TABLE V

User Fraud

	<u>U.S. Passport</u>	<u>NIV</u>	<u>NIV Supporting Documents</u>	<u>IV Supporting Documents</u>	<u>INS Documents</u>
Altered	5%	30%	30%	30%	19%
Counterfeit	0%	20%	60%*	50%*	29%
Imposter	95%	50%	10%	20%	52%

(NIV = non-immigrant visa, IV = immigrant visa)

*Includes genuine documents issued by corrupt officials to persons not entitled to them.

INS Documents¹

Increased investigative activity by INS and liaison with Mexican officials have resulted in the identification throughout Mexico of many well-organized groups engaged in both counterfeiting and altering these Service forms. Criminal prosecution in that country had been sought, however, the 8th Circuit Court in Tlaxcala, Mexico, found that the falsification of United States immigration documents is not a prosecutable offense in that country. Two well-known document falsifiers who had been arrested in the Juarez, Mexico area were released upon that decision. The tribunal ruled that since the issuance of such documents was not authorized by any Mexican authority, there is no Mexican criminal offense for falsification of such documents. One case came about as a result of information furnished to Mexican authorities by a Service investigator. The Baja California Judicial Police arrested three persons at Mexicali and Estacion Delta, Baja, California, Mexico and recovered falsification equipment and a large quantity of blank Forms I-151. It was learned that the more than 200 blank forms recovered were sold to the leader of the group in Guadalajara by two men who were believed to have been arrested and their counterfeiting equipment confiscated in Guadalajara several months earlier.

Also, an intensive investigation by INS and close liaison with Mexican Government officials resulted in the apprehension in Mexico City of the principal counterfeiter of one of the most wide-spread fraudulent document rings ever detected in Mexico. His headquarters was in Guadalajara where approximately 200 counterfeit Forms I-151 were found in the hands of vendors. Also seized were a small printing press and engraved plates for printing the Forms I-151, selective service cards and an Idaho State Seal, as well as numerous rubber stamps. The counterfeiter had previously been arrested in the United States in 1963 for counterfeiting Forms I-151 and at that time approximately 500 blank counterfeit documents were recovered. He then received a five-year sentence for the 1963 arrest and when last arrested stated that he had spent his entire time in prison perfecting his counterfeiting art.

Among the items seized was a list of the counterfeiter's vendors. There were nine in the State of Jalisco, seven in Guanajuato, three in Michoacan, two in Nuevo Leon and one each in the States of

¹All of the following data was taken from INS Intelligence Reports for FY 1973 and 1974.

Guerrero, Sinaloa, Sonora and Baja, California, as well as four in Mexico City. There were also twelve vendors listed in the United States: eight in California, and four in Illinois.

The use of altered Forms I-186 by individual imposters and by smugglers to facilitate border crossing by their customers continued to be a popular means of obtaining entry into the United States. Ample supplies of valid Forms I-186 are in the hands of alterers and vendors, who find a ready market for their wares among the thousands of interior Mexicans seeking entry into the United States. As in the case of altered Forms I-151, the workmanship of I-186 alterations has greatly improved over the past few years.

The steady increase over the past few years, except 1974, in the use of unaltered Forms I-151 is, in large part, due to an obvious large supply of forms obtained by vendors from various sources. Some vendors apparently have a large enough supply of documents so that customers may be matched up to forms so closely that it is extremely difficult to detect the fraud. Hopefully, the decline of such cards during 1974 may indicate vendors' supplies are dwindling.

The popularity among imposters of the unaltered Form I-186 as a document to gain entry continues to grow with each passing year. As in the case of the unaltered Form I-151, large supplies in the hands of renters and vendors make it comparatively easy to find a card which matches the imposter.

The problem of Mexican credentials presented by imposters is ever present. It is believed many of these are obtained as favors from Mexican officials. Some are purchased and a few are allegedly found. Many imposters are easily unmasked when interrogation reveals that they are obviously unqualified for the positions they profess to hold. Examples are: illiterate "school teachers," "stenographers" who cannot type, and so on. These documents are used mostly to facilitate entry as an alleged temporary visitor. Although the use of fraudulent Forms I-186 is limited almost exclusively to Mexican nationals and they are predominant in the fraudulent use of the other two Service identity documents, aliens from almost every country employ the use of fraudulent Forms I-151. The following is a common example of this:

Officers of this Service in the New York, New York, area encountered counterfeit Alien Registration Receipt Cards in the possession of illegal aliens. These cards contained the illegal alien's name, photograph, date of birth, and an alien registration number usually found to relate to a file either in the New York district or in another district.

The alien in possession of the counterfeit card generally was found to be a visitor or student whose period of temporary stay in the United States had expired. The date of entry on the counterfeit card was invariably found to be the date on which the alien entered the United States for a temporary period. Several natives and citizens of Guyana who had been admitted to the United States on a temporary basis were found to be in possession of such counterfeit cards. Investigation led to the arrest of two sources of these fraudulent documents, one, a Guyanese who had sold the counterfeit cards to aliens of his own nationality after purchasing them from an alien from Columbia. Several of these counterfeit cards were used by Guyanese aliens in an attempt to effect entry into the United States as returning residents and one was used to obtain employment as a teller in a New York City bank. Based upon the testimony of the arrested Colombian alien above and a Guyanese alien who had purchased a counterfeit card directly from him, an indictment was obtained in the United States District Court, for the Southern District of New York, against a third source, a permanent resident alien from Columbia.

Use of fraudulent identity documents supporting a claim to United States citizenship is prevalent among almost every nationality. Fraudulent birth registrations from areas outside the continental United States are also employed. A prime example is the detection of false claims to United States citizenship at ports of entry by aliens presenting counterfeit or fraudulently obtained Puerto Rican birth certificates and United States voter's registration cards. This scheme is commonly used by natives of the Dominican Republic and other Spanish-speaking Latin Americans.

The acquisition of such documents to support a claim to United States citizenship may involve an individual acting alone, or conspiring with others in exchange for monetary gain. Aliens are motivated to enter the United States in this manner for a variety of reasons. An alien's ineligibility to receive a non-immigrant or an immigrant visa through legitimate State Department channels may be the root cause. Another and more virulent reason may stem from attempts by persons of the criminal classes to gain disguised entry into the United States with contraband or to engage in criminal activities.

For several years there has been widespread use of Puerto Rican birth certificates by aliens to claim United States citizenship. Generally, the alien is assuming a true identity and has merely purchased a copy of a valid Puerto Rican birth certificate. This has been a particularly favorite practice of Colombian pickpocket rings. Although the Demographic Office in Puerto Rico is supposed to maintain records of when a duplicate birth certificate is issued, investigations by this Service have established that in many instances, particularly when the fraudulent birth certificate was used to obtain a United States passport, there is no record of any duplicate having been issued. There is an apparently limitless supply of Puerto Rican birth certificates which may be purchased for \$30 and up in Puerto Rico and are sold by regular vendors in the Dominican Republic for \$50 and up. In one case developed through investigation, it was established that a shoeshine boy, born in 1912, in San Juan, Puerto Rico was selling Puerto Rican birth certificates to Dominicans and Cubans for \$40 and up in several instances for an extra fee would assist them in fraudulently obtaining United States passports. Fees for these birth certificates range from \$30 to \$75.

Many British West Indians, who are allowed to enter Puerto Rico or the United States Virgin Islands without obtaining a non-immigrant visa, procure fraudulent United States Virgin Islands birth certificates to establish a claim to United States citizenship. These frauds are difficult to detect because of the similarity of race, the fact they all speak the English language and that most of them spend some time in and obtain knowledge of the Virgin Islands before attempting to travel on to the mainland. In the early 1960's, possibly 10% of the British West Indians encountered claim to be United States citizens and a majority of these have some sort of documentation to establish citizenship. The birth certificates are relatively easy and inexpensive to obtain and while many of them relate to true individuals born in the Virgin Islands, the Service is encountering counterfeit certificates which reflect the true name and date of birth of the alien using it.

Since United States citizens need no passports when returning to the United States from Canada or Mexico, nor upon entry into Puerto Rico, the vast majority of United States citizens satisfy the inspectors and are admitted upon a declaration of citizenship. If a doubt arises, proof of citizenship may be required to convince the inspector. While the possibility of false claims always exists, the expertise developed by the immigration officers is invariably difficult to overcome. There are three principal sources available to Service investigators who are engaged in the detection of

schemes and violators involving the fraudulent use of Puerto Rican birth certificates and voters' registration cards. The first two sources are concerned with record information -- public and private. Public sources are those of government agencies, Federal, state, county and municipal bodies. Private records are those maintained in the ordinary course of business firms and social agencies not supported by informants. Frauds involving counterfeit non-immigrant visas appear to be conducive to both "ring-type" operation as well as individual activity. The counterfeiting or altering of passports is more conducive to a "ring-type" operation, although a travel agency could well operate in this field at a profit.

Usually, aliens who present these types of documents have been refused issuance of a valid non-immigrant visa because of criminal background, previous deportee history or the American Consul may have had reason to believe that the alien's only purpose in seeking entry into the United States was to work in violation of status. This type of alien then seeks the services of a vendor who usually works hand-in-hand with an unscrupulous travel agency. In such an operation, the cost to the alien may run from several hundred dollars to over a thousand dollars.

There are two common methods by which the fraud rings bring illegal aliens to the United States as imposters with non-immigrant visas. One method is to substitute the pictures affixed to passports containing valid United States B-2 visas, altering birth dates if necessary and renting these altered passports to clients. The other method is to remove the page from a passport which contains a valid United States B-2 visa and sew it into another passport to enable the bearer, fraudulently identified on the title page as the person to whom the valid visa was originally issued, to enter the United States. The second method is the most effective and most difficult to detect inasmuch as the only identifying data on the visa is the name of the person to whom it was issued. Therefore, when a passport is built around this, the name which appears on the visa is used in the passport but the remainder of the identifying data actually relates to the imposter who is using the passport.

The following list reflects the principal types of immigration frauds involving false identification commonly being encountered by INS officers:

1. Personations of United States citizens supported by the following documentation:

- a. Counterfeit, altered and fraudulently obtained United States birth and baptismal certificates;
 - b. Altered and fraudulently obtained United States Passports; and
 - c. Other counterfeit, altered and fraudulently obtained United States documents of identity i.e., Resident United States Citizen Identification Cards (Form I-179), Social Security Cards, driver's licenses, voter registration cards, etc.
2. Non-immigrant visa frauds:
- a. Counterfeit, altered or fraudulently obtained United States non-immigrant visas;
 - b. Altered foreign government passports containing authentic United States non-immigrant visas; and
 - c. Counterfeit, altered and fraudulently obtained non-immigrant Border Crossing Cards (Form I-186) and other documents in lieu of non-immigrant visas, i.e., Form I-94, etc.
3. Immigrant visa frauds (including applicants for adjustment of status to that of a lawful permanent resident under Section 245 of the Immigration and Nationality Act):
- a. Personations and fraudulently obtained immigrant visas with valid or fraudulent foreign passports;
 - b. Personations, counterfeit and altered Alien Registration Receipt Cards (Form I-151); and
 - c. Personations and fraudulently obtained United States birth certificates and baptismal certificates for use in support of relative visa petitions (Form I-130) and Section 245 applications.

The problem of counterfeit, altered or fraudulent identity documents is especially serious in the southwest. In 1967 a total of 4,455 Forms I-151, I-186 and I-179 were detected in that area. Since then overall fraudulent document activity continued at an alarming and increasing rate. The street value of fraudulent documents furnished by vendors actually demonstrated an overall decline in the price of supplied fraudulent documents, which can only be attributed to a high rate of competition among vendors. We must conclude that a high rate of competition in such sales evidences tremendous profit-taking in this criminal endeavor. Comparative figures for Fiscal Years 1967, 1973 and 1974 are as follows:

	I-151			I-186			I-179			TOTAL
	Ctf	Alt	Unalt	Ctf	Alt	Unalt	Ctf	Alt	Unalt	
FY 67	58	1135	475	0	830	1875	0	69	13	4455
FY 73	3711	1545	2302	904	1410	6536	2	46	31	16487
FY 74	4074	1361	2086	585	1623	6160	6	21	13	15929

Average Price Paid for Documents:

	I-151			I-186			I-179		
	Ctf	Alt	Unalt	Ctf	Alt	Unalt	Ctf	Alt	Unalt
FY 73	\$182	\$121	\$43	\$70	\$108	\$68	\$102	\$130	
FY 74	166	126	80	73	57	40	Unavailable		

False claims to United States citizenship remained relatively static in comparing Fiscal Years 1973 and 1974. There were, during the reporting period, 14,453 false claims to United States citizenship of which 5,010 were documented.

The above statistics reflect a sharp increase in the number of counterfeit Forms I-151 detected in 1974 as compared to 1973. Also, the total number of fraudulent documents detected is higher than in 1973.

There has been much improvement in the quality of both the counterfeit and altered documents over the years, leading to the conclusion that there may be many fraudulent documents which have gone undetected. Increased use of ultra-violet viewing equipment and stepped-up training programs have enabled us to detect the better quality products that may have avoided detection years ago.

The two most common techniques are the counterfeit birth certificate and the IDI method.

1. The counterfeit birth document follows the following process:
 - a. The purchase or the production of a counterfeit birth certificate. This is done by photographing the genuine form or the printing of a birth certificate form;
 - b. This form is then filled in by the user or the broker for the user; and
 - c. This counterfeit is then shown to obtain a genuine driver's license. Those two documents are used to obtain or attempt to obtain a U.S. Passport.
2. The IDI (Infant Death Identity) method, which is becoming more widespread, follows the following pattern:
 - a. Search of Vital records, tombstones, newspaper obituaries, morgues to locate the deaths of persons who died in infancy. Infancy in this situation is birth to 5 years;
 - b. From information obtained in death records, the genuine birth certificate is obtained from the Vital Registrar's Office;
 - c. The birth certificate is then used to obtain a social security number;
 - d. The birth certificate and the Social Security number are then used to obtain a driver's license;
 - e. With these genuine documents, the person applies for a U.S. Passport; and
 - f. A variation is to use an Identifying Witness rather than a driver's license.

In some cases persons use the birth certificates of deceased adults and follow above procedures to apply for U.S. Passports. This is not too frequent, but it is used.

In the past, affidavits of birth were used along with affidavits of Identifying Witnesses to create false identities. Procedures established by the Passport Office have made it impossible to use this technique.

The IDI method is becoming more prevalent because the documents used are genuine and the fraud is thereby harder to detect.

Another form of fraud technique is to use genuine blank birth certificate forms stolen from Vital Registrar's Office. The blanks are then filled in by the person desiring to assume another identity. In some cases, the blank forms have already been presigned by the Registrar. This same technique is used in the theft of blank driver's licenses.

The alteration of U.S. Passports after issue for use by imposters is accomplished by removing the photograph and replacing it with the photograph of the imposter. In most cases, some official entries regarding age or description are also altered. This practice is exclusively used abroad. It is viable because of the lack of expertise by foreign officials in detecting altered U.S. Passports. The expertise of INS officials generally prohibits this practice for entry into the United States.

False ID "User" Profiles

As reported by the Visa Office, INS, Customs and the Passport Office, users of false ID conform generally to the characteristics shown in Table VI below.

Additional comments indicate a trend for illegally entering aliens to move to the larger urban areas. There is some noted tendency for political or social unrest in the countries of origin to increase traffic. It is also noted that increasing westernization may be a factor in increasing a tendency to go to the U.S.

There appears no seasonal bias save drug trafficking where holiday and vacation periods are used because of the high load on Customs personnel at these times. Drug traffic is thought also to be affected by the supply and demand situation in its market.

Economic conditions in the U.S. may or may not have an effect on illegal alien traffic since the U.S. economy is invariably better than that of the country of origin.

In general, illegal alien traffic is higher in New York than elsewhere; illicit drug traffic is highest on the West Coast.

TABLE VI
FALSE ID USER PROFILES

Document or Activity	Age	Sex	Race or Nationality	Education Level	Criminal Record	Employment Status	Residence in U.S.	Motivation
Visa	18-40	90%M	Central and South American, Caribbean, African, Asian	Some -- Elementary Level	Rare	Unemployed or at low status and pay	Variable	Economic -- to improve standard of living and prospects
INS Documents	18-40	70%M	All	Limited to College Graduate	Generally none	Employed generally	Everywhere but trend toward urban areas	Varied
U.S. Passport	18-40*	78%M	All but predominantly Central and South Americans and U.S. citizens	All. Aliens less than citizens	80% have prior records	Generally employed	All areas	Varied
Narcotics Smuggling	Over 18	75%M	Latin American, European, Asian	Primary Level	Usually	Unemployed or low, menial work	Generally urban areas	Economic -- to make money

*Specific

	Male	Female
Illegal aliens	32	29
Narcotics	29	20
Swindlers	36	26
Fugitives	29	27
Militants	22	23

SECTION III
SOCIETAL IMPACT AND COSTS

General

The use of false identification to enter or remain illegally in the U.S. by large numbers of aliens has considerable impact on American society. Illegal aliens take jobs that could be held by American citizens or legal resident aliens; they consume welfare services and education funds; they often pay no taxes; they send much of the money that they earn outside the U.S.; they may be exploited by the unscrupulous and the greedy; they are occasionally a factor in crime; they, by their numbers, cause resentment often directed toward all foreign-looking persons, not just illegals; their detection and apprehension and the adjudication of their cases takes considerable time and money. The INS estimates that there are 4-12 million illegal aliens in the U.S. Even a conservative estimate of \$100 per week cost to the U.S. in job wages lost, taxes, welfare, and so on yields a staggering annual cost of their presence of \$21-62 BILLION.

If even 5%¹ of these illegals have entered the U.S. or remain in the U.S. by using false ID, this cost is in the range of 1 to 3 BILLION per year -- fairly assignable to false ID.

There is, in fact, no total nationwide estimate of the economic impact of the illegal alien on the American taxpayer but their impact on local communities follow as examples.

Welfare Costs

In 1973 the California State Social Welfare Board estimated the cost of welfare payments to illegal aliens to be at least \$100 million a year².

It was also reported in 1973 that \$100 million in welfare funds was paid to illegal aliens in New York City and that 65,000 illegal aliens were attending public schools in that city at a cost of \$78 million.

¹A conservative figure according to the Visa Office.

²State of California -- State Social Welfare Board Position Statement, January 1973. Los Angeles Times, 1/27/73.

Health Service Costs

In 1974, an \$8 million reimbursement claim was received from Los Angeles County for medical expenses incurred by illegal aliens. \$3 million was reportedly paid in 1974 to illegal aliens for medical and hospital expenses by Fresno County, California¹.

Income Tax Losses

Yearly loss, according to a Congressional Report, is \$100 million nationwide².

A three-month pilot project by INS and IRS produced \$168,000 tax collected from 1,700 illegal aliens.

Balance of Payment Losses

Wall Street Journal, September 29, 1971, estimated from \$3 to \$10 billion sent out of the United States by illegal aliens. In the State of Washington illegal aliens sent out of the United States \$7.5 million during the 1974 harvest. A small community post office sent \$35 thousand to Mexico in a five-week period³.

Illegal Aliens Occupy Jobs That Are Attractive to American Citizens

One alien found in Houston was employed at \$17,000 per year as a product development engineer. In Maine, an alien was found earning \$30,000 a year as a salesman and another earning \$900 a month as a computer salesman. In Boston, one was found earning \$6.00 per hour as a chemist and another earning \$10.00 an hour as a welder. In Providence, two were found earning \$8.65 an hour as painters, and in New York City one was found earning \$12.00 an hour as a plumber. These are only examples, but it has been estimated that there are more than 1 million illegal aliens occupying well-paid jobs that would be attractive to United States citizens.

¹Ibid.

²New York Times Magazine, 9/16/73. New York Times, 6/12/73.

³Investigative Study of the Immigration of Illegal Aliens and Farm Workers in the State of Washington. Study by the State of Washington Interagency Task Force for Agricultural Workers, December 1974.

CRIMINAL ACTIVITY

Smuggling

A smuggler of narcotics, jewelry, watches, arms and munitions, currency, or any other contraband, needs international mobility to operate effectively. False identification conceals his activity whether he is a principal, controller, or actual carrier of the contraband.

U.S. Customs investigations indicate that false identification is an absolute necessity for a successful international smuggling organization; that false identification is used by smugglers with extensive criminal backgrounds; that false identification conceals their criminal backgrounds and provides the organizations with the criminal expertise to evade law enforcement; that, when apprehended, false identification enables these criminals to obtain immediate bail and flee the U.S. before prosecution; that the overall smuggling organization continues to function without any disruption; and that Justice is frustrated until the fugitive can be relocated, apprehended and extradited for prosecution.

A survey conducted by one of the Customs areas involved primarily with the use of false identification in foreign passports disclosed that one of the most prevalent false ID areas of use was that of narcotics smuggling. False identification enables the narcotic smuggler to get into the U.S. as fast as he can with the narcotics, and to get out as fast as he can with the least likelihood of discovery.

In considering the societal impact of drug smuggling the street value of the drugs involved is a conservative measure of the larcenous activity it engenders. It is a conservative measure of the loss of goods and money to society because the fenced value of the goods (the return to the thief) is never close to the true value and generally less than the insurance value. Further, the monies transferred or raised by theft for drugs do not in general return to the economy in the productive way that proceeds of legitimate sales do. They go often to underworld receivers and are used to support other illicit activities which also cost the taxpayer money, decrease his freedom or compound his worry.

As an example, consider a review of arrests, seizures, and narcotic investigations effected by the U.S. Customs Service for the calendar years 1967 through 1974. This survey reveals a total of 416 narcotic seizures valued at \$833,849,126 on the illicit street.

It also showed that of the total 416 narcotic seizures reported that false identification was used by the smuggler in 143 seizures; that false identification was used by principals, controllers, or other associates connected with the defendant's arrest in 218 narcotic seizures; and that false identification may be involved in 55 narcotic seizures turned over since July 1, 1973, to the Drug Enforcement Administration for their investigation in which a Customs determination could not be made.

Table VII contains the following summaries for Customs cases involving the use of the false identification for narcotic smuggling during the calendar year 1967 through 1974. This data includes the total illicit street level value of \$1,672,802,000 for all of the narcotics known through investigation to have been successfully smuggled into the U.S. by these same traffickers or their associates.

TABLE VII
USE OF FALSE IDENTIFICATION -- NARCOTIC SMUGGLING

CALENDAR YEAR	VALUE OF NARCOTICS SEIZED	VALUE OF KNOWN NARCOTICS SMUGGLED	TOTAL
1967	\$ 18,500,000	\$ 32,537,500	\$ 51,037,500
1968	\$ 35,787,000	\$ 56,875,000	\$ 92,662,000
1969	\$ 24,381,492	\$ 40,050,000	\$ 64,431,492
1970	\$ 92,068,750	\$ 145,389,500	\$ 237,458,250
1971	\$296,074,500	\$ 384,900,000	\$ 680,974,500
1972	\$203,899,083	\$ 12,350,000	\$ 215,249,083
1973	\$ 97,257,551	\$1,001,700,000	\$1,098,957,551
1974	\$ 65,880,750		\$ 65,880,750
TOTAL	\$833,849,126	\$1,672,802,000	\$2,507,651,126

It should be noted that the Table V data are Customs Service data and accordingly reflect the Federal reorganization of July 1973 which vested investigatory responsibility with the DEA. Customs data following that date reflect only seizures by Customs officials presumably at the point of entry. This accounts largely for the drop in the figures for 1973 and 1974. Any implication that narcotics smuggling declined markedly in 1973 is false.

Of the narcotics seized, about 80% was in the hands of persons utilizing false ID.

It is thought by both DEA and Customs that the extent of drug traffic is closely related to both the economics of the trade and the ready availability of the supply. Seizures are thought to relate directly to the total amount of traffic.

The Passport Office states:

"The use of false identification for the purpose of trafficking in illegal drugs causes almost immeasurable dollar damage to our society as a whole. A person who fraudulently obtains a United States visa for the purpose of bringing illegal drugs into the United States is capable of bringing in, each time he uses that false identity, concentrated hard drugs (cocaine and heroin) which when diluted have a street value of almost a million dollars. For example, during the past two-and-a-half years 206 United States Passports were either applied for or obtained by persons involved in drug activities. The current potential of street value involved by this number of persons is in the neighborhood of 206 million dollars.

The subsequent impact of broken lives and deaths from overdoses of hard drugs brought in by these people is incalculable. This may be expanded to the crimes which drug addicts commit to obtain funds necessary to maintain their drug habit. This has been estimated to run into several hundreds of millions of dollars a year."

FUGITIVES

The impact of a fugitive on society depends to a great extent upon the nature of the criminal offense, the prosecution of which the person is fleeing. The range of such offenses covers all types of felonies. Some of the social impact may be caused by the recurrence of the offense in a false name plus the ability to escape

detection by law enforcement agencies. The dollar impact caused by law enforcement efforts to apprehend a fugitive using a false identity is considerable but impossible to determine with accuracy¹.

Of increasing concern in this context are the militant/radical groups. More traditional fugitive concerns lie with "con" men and espionage agents both of whom use false ID extensively.

The militant/radical impact has a wide scope since these individuals are involved in crimes of violence and terrorist activities. Examples are the Patricia Hearst episode and recent bombing of the State Department. All members of such groups are required to have 3-5 or more different sets of identification documents. One militant went so far as to enlist in the Army to create a false identity.

False ID Investigations & Prosecutions

False ID investigations and prosecutions are mainly the business of the INS, unless a visa fraud is detected overseas in the course of application and insurance. Once an alien is in the U.S., either the Department of Justice, INS, or a state or local authority has jurisdiction. The Customs Service is typically concerned with apprehending smugglers; false ID aspects of a typical Customs case would fall to the jurisdiction of INS. INS activity is discussed below.

INS completed a total of 16,676 investigations of suspected immigration frauds during Fiscal Year 1974. The following statistics indicate the number of Federal criminal violations detected and the sections of Federal law involved.

¹See Appendix A3, Report of the Fugitives Task Force.

	<u>Prosecution Waived by Blanket Waiver</u>	<u>Presented to U.S. Attorney</u>	<u>Thereafter Declined by U.S. Attorney</u>
18 USC 911 False representation as a U.S. citizen	11,373	2,381	2,263
18 USC 1001 False statements	1,347	1,862	1,767
18 USC 1015 False certifications	1	18	4
18 USC 1546 Fraud and misuse of visas and other documents	11,508	2,168	1,877

The Passport Office reports:

During FY 1974 there were 362 fraud cases opened and 341 closed by the Department of State office of Security. During the same period, the Passport Office granted investigative jurisdiction to the FBI in about 50 fraud cases involving matters of primary interest to the organization.

The following table gives figures on criminal prosecutions for passport frauds from July 1, 1973 to February 28, 1975. As of February 28, 1975, there were 136 cases still pending prosecution action.

Criminal Prosecutions

	<u>Opened</u>	<u>Closed</u>	<u>Declined</u>	<u>Dismissed</u>	<u>Convicted</u>	<u>Indicted Fugitive</u>
7-1-73 to 6-30-74	99	89	42	7	19	21
7-1-74 to 2-28-75	40	43	23	2	7	11
TOTAL	139	132	65	9	26	32

Pending

7-1-73	129
2-28-75	136

SECTION IV

COUNTERMEASURES TO CRIMINAL USE OF FALSE ID

General

Detection of an altered passport and non-immigrant visa is, first, visual and subsequently combatted through dissemination of information and intelligence.

Efforts to combat this type of fraud include an exchange of information between INS and the State Department. The interested American consular post is furnished information obtained from the alien relative to the identity of the vendor for transmittal to the foreign government authorities. In addition, new schemes and modus operandi detected through investigation are disseminated to the immigration officers at appropriate ports of entry for their use in identifying such documents during the inspection procedure.

Aliens intercepted at ports of entry or who are encountered after effecting entry with fraudulent passports and/or counterfeit non-immigrant visas have usually been advised by the vendor or travel agent to travel to the United States on weekends, when traffic is at its "peak", in order to escape detection at ports of entry by immigration inspectors. However, vigilant, well-trained immigration inspectors maintain a high detection rate of counterfeit entry documents of all varieties, despite the often overwhelming flow of traffic at ports of entry.

Cases involving fraudulent passports and/or visas are presented to the United States Attorney for criminal prosecution.

The use of false identification by natives of the Philippines has been a problem to the INS for many years. A large number of counterfeit, altered or otherwise fraudulent non-immigrant visas have been presented by imposters from that country. Most of them obtained the documents through unscrupulous travel agents in Manila, who also supply counterfeit airline tickets. Counterfeit non-immigrant visas showing issuance in Manila have been of fairly good quality and difficult to detect. A Philippine national, allegedly connected with a Manila travel bureau, together with an unlicensed travel agent have been identified as the counterfeit visa suppliers. Also, in another case, an employee of another Manila travel bureau supplied a counterfeit visa to an alien after she was denied a visa at the Manila Consulate. He was later arrested for selling a counterfeit airline ticket. A number of cases have been encountered

where a visa issued to a person other than the imposter has been utilized. In many of these instances, the imposter's name was similar to that of the person securing the visa. Passports containing the visas may be altered or the visa page may be substituted from one passport to another.

Detection of User Fraud

Considered here are two kinds of entry fraud to be detected with false alien documentation and by a citizen (presumably on illegal business) without a U.S. Passport. They are discussed below:

False Alien Documentation

False Visa Indicators - The following false visa indicators have been noted:

1. The applicant's use of a travel agency to obtain his visa without any appearance at the U.S. Consulate's Office;
2. The quality of the applicant's clothing indicates a lower working class and is not in agreement with his application;
3. The visa applicant is in possession of a foreign passport just recently issued;
4. The visa applicant is in possession of a foreign passport that was issued outside of his native country. Frequently, aliens with criminal records are denied foreign passports in their own country, and they will use their civilian identification cards for travel to an adjacent country to obtain the same passport from a consular office that for the same identification was previously denied to them;
5. The applicant is not a citizen or a resident of the country in which the issuing consulate office is located;
6. The applicant states in his visa application an occupation which does not normally warrant the expense of a trip to the U.S.;

7. The applicant is accompanied by an associate who may or may not be applying for a visa, but is totally familiar with the procedure required for the applicant;
8. The applicant's physical appearance indicates a lower working class than the prestigious title stated for his occupation, i.e., Sanitary Engineer instead of Garbage Man;
9. The applicant states he is married, yet at the same time the purpose of his visit to the U.S. is tourism;
10. The applicant's physical appearance indicates a lower working class but on his application he states his purpose is a tourist and neither his spouse nor his parents are in the U.S.;
11. The applicant's passport shows frequent travel to countries in Europe and South America with very short trips in each country visited;
12. The applicant states in his application an intended departure that is immediate;
13. The applicant omits to answer the visa question "What address do you wish your visa be mailed to?"; and
14. The applicant's language proficiency is not in agreement with his foreign passport identity and nationality.

False Entry Without a U.S. Passport

The U.S. Customs Service finds that the smuggler continually seeks new ways to enter the U.S. with false identification. The following method is also frequently utilized by the U.S. citizen.

The subject assumes an alias and then obtains the following credentials for the purpose of identification:

1. State driver's license;
2. Bank card and account;
3. Library card;
4. Social Security card;
5. Voter identification card; and
6. Various club membership I.D. cards.

Armed with the above credentials and falsely obtained U.S. Passport, the subject purchases a ticket to leave the United States for his destination. Upon arriving at his destination, the foreign entry is easily accomplished since a U.S. Passport makes entry into most foreign countries an easy matter.

In order to gain easy access back into the United States without a passport, the subject then purchases a ticket in the assumed name and returns to the U.S. via Nassau, Jamaica or other various locations from which the U.S. Immigration Service allows entry into the U.S. with the showing of any of the credentials in the absence of a U.S. Passport.

This method of entry evades detection by Federal law enforcement agencies and also enables the subject to keep his U.S. Passport clean of any entry stamps that would reveal his return to the U.S.

Application Phase

Visa Office

One of the most effective countermeasures that the Visa Office has used and continues to use against fraud is encouragement of alertness among consular officers abroad. An attempt is made to remind visa issuing officers that the incentives to gain entry to the U.S. are great, to point out techniques often used, to call attention to unusual trends in visa issuance at particular posts and to offer other support as needed.

Working with the Immigration and Naturalization Service, an attempt is being made to standardize certain forms that prospective providers of financial support and prospective employers are expected to file. The problem of false labor certifications is being attacked with the Department of Labor. But, since most of the documents submitted in the application phase are of foreign origin,

control over them is limited and individual officer alertness is the most effective weapon.

INS

The most effective countermeasures to combat the "application" phase of fraud is the training of all Service officers to increase their sensitivity to frauds. This is done through a formal training program at the Service Academy in Port Isabel, Texas, and also at local training sessions. Close cooperation at all levels with the Department of State and the Department of Labor are stressed.

Considerable success has also resulted from the following described Suspect Third Party Program.

The Service has always been concerned with the problem of combatting frauds engaged in by aliens in connection with attempts made to unlawfully effect entry and remain in the United States. In 1963, an increase was noted in the activity of unscrupulous individuals involved as third parties in the preparation and submission of visa petitions and other applications to the Service. These include applications for extension of temporary stay of non-immigrant visitors, change of status from one category of non-immigrant to another non-immigrant status and adjustment of status from a non-immigrant status to that of a permanent resident in the United States. The third parties take undue advantage of people who desire to do everything possible to aid in the immigration of relatives and friends and frequently engage in fraud, misrepresentation, furnishing false identity documents and other irregularities.

It has been the practice of some unscrupulous attorneys, travel agents, notaries public, employment agents and so-called "immigration consultants" to arrange marriages of convenience to assist aliens to obtain permanent residence in this country. If they are unable to locate a United States citizen to marry an alien for a fee, they often will supply an alien with false documentation as a citizen to go through the ceremony and file the necessary visa petition. There is an increasing trend of United States citizens to engage in multiple marriages for the purpose, using birth certificates or identity documents of various United States citizens. In furtherance of Service efforts to combat such unethical and unlawful practices and to aid in the identification and detection of the individuals concerned, the Suspect Third Party Program was initiated on November 4, 1963. Operating procedures, which included a vigorous prosecution policy, were established and field offices were directed to follow them closely.

Many of the investigations under this program disclosed criminal violations, including aliens and other persons who for substantial fees assisted them in their efforts to evade quota and other restrictions embodied in the immigration laws. The criminal statutes violated were 18 USC 371 (conspiracy), 18 USC 1001 (false statements) and 18 USC 1546 (fraud).

Passport Office

The most effective countermeasures to combat the "application" phase of fraud is the training of all officers to increase their ability to recognize frauds. This is done at fraud training seminars at our field Passport agencies as well as in Washington. In connection with these specialized seminars, conducted training seminars have been conducted for interested outside agencies in field areas. Representatives from the following agencies have attended these specialized seminars: FBI, DEA, FAA, Postal Service, Customs, Office of Security of the Department of State (SY) and INS.

Special seminars have been conducted by invitation to Customs officers and INS officers.

Fraud seminars are now being conducted for Postal and Clerk of Court Personnel who accept passport applications in the U.S.

Use Phase

Visa Office

Presentation of counterfeit immigrant visas for admission to the U.S. is virtually unknown. All the identity fraud appears to be in the application phase.

For the non-immigrant visa, reliance is primarily on the alertness of the INS primary inspectors at ports of entry to spot photo substitutions, page switching, or visa altering. Efforts to counter the attempted use of counterfeit visas include standardization of the visa plate, improvement of the special features of the ribbon, notation of visa refusals on passports, maintenance of a visa lookout system, and introduction of the counterfoil in high fraud areas. The counterfoil is a peel-off, paste-in paper wafer with a number and a finely printed design on it. The visa is printed in the passport partially over this wafer. Although attempts to counterfeit the counterfoil have surfaced (after a year of apparently trouble-free use), it is believed that it has been a useful addition in high fraud areas and has deterred some counterfeiters.

It should be pointed out that measures such as these may deter certain uses of false identification, but encourage other methods of circumventing the law -- false claims to American citizenship and increased efforts to enter the U.S. without visas and thus without inspection are likely to emerge.

One of the most promising recent steps in the area of counter-ing the use of false identification is a joint project being carried out by the Visa Office and the Immigration and Naturalization Service with the advice and assistance of a private consulting firm to develop fraud-proof non-immigrant visas and alien registration cards. Pilot tests of the recommended new system of non-immigrant visa issuance and control are to begin shortly.

INS

Again it is believed that education of Service officers is the most effective weapon to combat "use" frauds. INS officers must be adept at spotting photo substitution, page switching, visa altering, impersonations, etc. All officers also have available to them ultraviolet light equipment, including portable types for use in the field. Close cooperation between the Department of State consular officers and INS officers has proven effective. Suspect documents are checked by telephone to determine if they were issued by consular officers.

The Service's Fraudulent Document Center was established in 1958 to develop measures to combat false claims to United States citizenship by Mexican aliens using fraudulent documents. The Center furnishes information to assist Service officers in conducting investigations and obtaining evidence, compiles statistics to determine the scope of the problem and assembles and coordinates information pertaining to Mexican false claimants by indexing known and suspected violators as well as the fraudulent documents. The Chief Patrol Agent, Yuma, Arizona, has overall responsibility for the Fraudulent Document Center; 5,924 cases were added to the files during the Fiscal Year bringing the total number of files at the facility to almost 50,000. Service officers and officials of other agencies directed 6,128 inquiries to the facility for record checks in Fiscal Year 1974. One out of four of the inquiries resulted in the location of prior records relating to documented false claims to citizenship. The information available from the files proved invaluable in determination of the citizenship status of those attempting to perpetrate frauds.

Customs Service

The most effective countermeasure to false identification is the proper training of front-line personnel to alert them to profiles, methods of use, and other intelligence available concerning unusual techniques used by narcotic smugglers. In addition, close cooperation is stressed with the State Department, and the Immigration Service relative to ongoing investigations, so that all levels of the entry screening process can be fully aware of current trends and provide greater efficiency.

SECTION V
RECOMMENDATIONS FOR
AMELIORATION OF THE FALSE ID PROBLEM

General

This section sets forth the preliminary recommendations of the Task Force on Federal Documents for the substantial decrease and eventual elimination of the False ID Problem as a practical matter. The recommendations are intended both to make abuse of federal documents more difficult and to engender easier, surer, and more efficient detection of frauds perpetrated with false documents. It is understood that the issues involved here are, to some extent, international in character and that effective solutions will often require multi-national agreements and cooperation.

International Agreements

It is recommended that the Departments of Justice and State utilize their resources to obtain international acceptance of standards and uniform guidelines for passport control. The standards and guidelines should include consideration of issuance requirements, in general, ID required particularly, printing, photography and counterfeit, alteration and imposter countermeasures.

The acceptance of uniform guidelines of this sort would be an important step in the establishment of International Passport controls, a requisite for efficient address to the international false ID problem.

Such a program could be initiated as one of the law enforcement programs of Interpol and the International Association of Chiefs of Police. These two organizations have worldwide representation and are natural channels abroad. An international anti-fraud training program could be a part of a joint program.

Domestic Practices

Prosecution of Cases

It is recommended that guidelines be issued by the Department of Justice to all of their U.S. attorneys concerning the magnitude and importance of the false identification problem. This may provide a greater acceptance by the U.S. attorneys for the prosecution of selective cases involving false passports, non-immigrant visas, and Customs Baggage Declarations, particularly in narcotic smuggling.

In previous cases effected by the U.S. Customs Service, Assistant U.S. Attorneys have been reluctant to include these additional charges against the defendant. They felt it was superfluous; that it did not warrant the time and effort; and that the primary charge of narcotic smuggling was sufficient. However, these additional counts insure a prosecutor's chances to obtain a conviction, especially with an uncooperative defendant implicated in a narcotic smuggling conspiracy. Finally, principals, controllers and their associates who use false identification to enter the U.S. become highly vulnerable to Federal prosecution.

Inter-Agency Cooperation

The desirability of more intensive cooperation among the various agencies, bureaus, offices and departments having an interest in the false ID problem has been noted. There are several ways of effecting this and degrees of formality which might properly attach to these activities. They range from informal joint seminars on aspects of the problem such as have been conducted with success in the past, to the establishment of a national fraudulent document center patterned somewhat after the successful INS center at Yuma, but focused on the common needs of the member community.

In this vein, suggestions have been advanced concerning the establishment of "banks" to centralize state data such as Driver's License information, birth and death records and the like, from those states which have computerized or otherwise regularized their vital records activities.

Interstate Activities

Abuse of the birth certificate and driver's licenses through their uses as breeder documents impacts federal document control of concern to this Task Force. Accordingly, it is recommended that the states, singly or jointly, move to eliminate the IDI syndrome and better control both the birth certificate and the driver's license. Nevada law S.B. 391 (Attachment II of this report) is cited as a model in this regard.

At the very least, states should agree on a standard birth certificate form, materials and methods. The availability of facsimile documents should be prescribed and the use of legitimate forms controlled.

Training and Education

Extensive and intensive use of training programs for all officials having any connection with the false ID problem is recommended. Such training should be reviewed and updated as appropriate.

Legislation

Loopholes in existing legislation¹ have been noted from time to time which are not in the interest of society and every effort should be made to close them expeditiously.

¹Section 1546 of 18 USC relating to the possession of a fraudulent Alien Registration Receipt Card.

ATTACHMENT I

ORGANIZATIONAL COMPOSITION OF TASK FORCE¹

AGENCY	APPLICATION	DOCUMENT	USER	SUPPORT
Immigration & Naturalization Service	X	X	X	X
Visa Office	X	X	X	X
Dept. of Health, Education & Welfare	X	X	X	
Customs			X	X
Dept. of Defense	X	X	X	X
Passport Office	X	X	X	X
Selective Service	X	X	X	
Dept. of Transportation	X	X	X	X
Federal Aviation Admin.	X	X	X	X
Coast Guard	X	X	X	X
Bureau of Engraving & Printing			X	X
MITRE Corporation				X
Polaroid Corp.				X
American Bank Note Co.				X
Communications Consultants, Inc.				X
3M Company				X
Office of Security (State)			X	X
Justice Criminal Division				X
Electronic Data Processing				X
Drug Enforcement Admin.			X	X

¹Shows the function of the organization as, for example, the processor of applications and issuer of documents.

ATTACHMENT II
(REPRINTED WITH ADOPTED AMENDMENTS)
SECOND REPRINT

S. B. 391

SENATE BILL NO. 391—COMMITTEE ON JUDICIARY

March 25, 1975

Referred to Committee on Judiciary

SUMMARY—Prohibits certain acts respecting birth certificates.
Fiscal Note: No. (BDR 40-924)

EXPLANATION—Matter in *italics* is new; matter in brackets [] is
material to be omitted.

AN ACT relating to birth certificates; prohibiting their procurement and possession to establish a false identity; prohibiting their use in the commission of public offenses; providing penalties; and providing other matters properly relating thereto.

*The People of the State of Nevada, represented in Senate and Assembly,
do enact as follows:*

- 1 SECTION 1. Chapter 440 of NRS is hereby amended by adding
2 thereto a new section which shall read as follows:
3 1. *It is unlawful for any person to obtain or possess the birth certi-*
4 *ficat*e of another for the purpose of establishing a false identity for
5 *himself or any other person.*
6 2. *Every person who has in his possession the birth certificate of*
7 *another person without lawful reason for such possession or who uses*
8 *the birth certificate of another in the commission of a misdemeanor, is*
9 *guilty of a misdemeanor.*
10 3. *Every person who has in his possession two or more birth certi-*
11 *ficat*es of other persons without lawful reason for such possession or
12 *who uses the birth certificate of another person in the commission of*
13 *a gross misdemeanor is guilty of a gross misdemeanor.*
14 4. *Every person who uses the birth certificate of another person to*
15 *aid in the commission of a felony shall be punished by imprisonment*
16 *in the state prison for not less than 1 year nor more than 6 years, or*
17 *by a fine of not more than \$5,000, or by both fine and imprisonment.*
18 5. *The offenses described in this section are separate from the pri-*
19 *mary offense if any, and the unlawful possession of a birth certificate*
20 *is a separate offense from its unlawful use.*

Law becomes effective July 1, 1975.

APPENDIX A5

**REPORT OF THE STATE AND LOCAL IDENTIFICATION DOCUMENTS TASK FORCE
ON THE
SCOPE OF THE FALSE IDENTIFICATION PROBLEM AND
PRELIMINARY RECOMMENDATIONS FOR SOLUTIONS**

Submitted to

**Federal Advisory Committee On False Identification
David J. Muchow, Chairman**

May 1976

TABLE OF CONTENTS

	<u>Page</u>
SECTION I - INTRODUCTION	A-165
Purpose	A-165
Scope	A-165
Data Gathering	A-165
Evaluation of Data	A-165
SECTION II - THE FALSE ID PROBLEM	A-171
Application Phase	A-172
Application Patterns	A-173
Use Phase	A-173
Intended and Common Usage	A-173
Fraudulent Uses	A-174
Document Fraud	A-174
Counterfeit Documents	A-174
Altered Documents	A-175
False ID Users	A-175
False ID Victims	A-176
SECTION III - COUNTERMEASURES TO CRIMINAL USE OF FALSE ID	A-179
Countermeasures Presently Employed	A-179
Application Phase	A-179
Birth Certificates	A-179
Motor Vehicle Operator's Permits	A-180
"Use" Phase	A-181
SECTION IV - RECOMMENDATIONS	A-183
Birth Certificate	A-183
Driver's Licenses	A-186
Other Comments	A-187
ATTACHMENT I - COMPOSITION OF THE FACFI TASK FORCE ON STATE AND LOCAL DOCUMENTS	A-188
ATTACHMENT II - SYNOPSIS OF MATERIAL IN TASK FORCE FILES	A-190

Report of the State and Local Documents Task Force

on the

Scope of the False Identification Problem

Recommendations for Solutions

SECTION I

INTRODUCTION

Purpose

The State and Local Documents Task Force was to study the state and local documents commonly utilized in establishing false identities; to establish false identity use patterns for the subject documents; and to suggest practical solutions to this abuse.

Scope

While there are many documents which originate at a state or local office, it was determined as a result of survey, that the most frequently used documents for establishing false identities are the birth certificate and the driver's license. Therefore, the Task Force expended the bulk of its effort on studying the false identity problem as it relates to these important documents.

It is a fair statement that the potential use of the birth certificate as a "breeder" of other false documents and the universal acceptance of the driver's license as valid ID makes these two documents essential to the establishment of a full false identity. While a variety of imaginative frauds can be used to generate false identity documents, the possession of these two assuredly makes the process easier and the likelihood of apprehension less.

These two documents are similar in that both are issued by states under state control. There are no federal regulations relating to the issuance of either document.

The work of the Task Force was accordingly very broad in scope because there are more than fifty states and territories of interest with significant differences in procedures and standards. It was necessary to collect data from all the states to completely delineate

the problem. Even greater breadth was added by the fact that driver's licenses and copies of birth certificates may be issued within states and territories through scattered local offices. There are, for example, over 7,000 offices in the country authorized to issue certified copies of birth certificates. Because of the large numbers of issuing offices, procedures may, and often do vary from area to area within a state. Accordingly, statements made here relating to the system for issuance of birth certificate copies or for the issuance of drivers' licenses are representative common practice but do not necessarily reflect the procedures in every state or even in every part of a single state.

Data Gathering

Data was acquired through surveys and from existing reports and interviews. Task Force surveys are described as follows:

1. One survey questionnaire was sent to all fifty states and eight independent cities and territorial Vital Registration officials. The purpose of the survey was to secure information on the matching of infant death records to the corresponding birth certificates. The survey also requested the number of offices in each area that issue copies of vital records and solicited suggestions for reducing fraud in birth certificate issuance. All fifty-eight registration areas* responded.
2. A letter was also sent by Dr. E. B. Perrin (Director, National Center for Health Statistics) and Mr. Clarence M. Kelley (Director, Federal Bureau of Investigation) to each state and territorial health officer. The letter announced the formation of the Federal Advisory Committee on False Identification (FACFI), requested suggestions that would help to reduce the fraud problem as it relates to vital records, and enlisted their support for the work of the FACFI. Fifty-eight letters were sent and twenty-six responses were received.

*Fifty states and Washington, D.C., N.Y. City, Puerto Rico, American Samoa, Guam, Panama Canal Zone, Virgin Islands, Trust Territory of the Pacific Islands.

3. A survey was made of all state and provincial motor vehicle administrators and chiefs of enforcement by the American Association of Motor Vehicle Administrators to secure information on the automobile operator's license problem in false identification. One hundred and sixty questionnaires were mailed out and thirty-three responses were received.
4. A survey was conducted among the Department of Motor Vehicle District Directors in New York State by the Director of the Department of Motor Vehicles. This survey attempted to gather information regarding the extent of the false identity problem as it exists in New York State; a profile of those obtaining false driver's licenses; and recommendations for reducing the problem. The survey was sent to thirteen District Directors; all replied.
5. Data was also obtained from the Passport Office (PPO) and the Immigration and Naturalization Service (INS) regarding the extent of use of the birth certificate and operator's license in their operations. An estimate of the extent of fraud involved in the use of vital records and operator's licenses in matters of concern to INS and PPO was also obtained. The Passport Office additionally constructed a general profile of persons obtaining passports fraudulently.

Evaluation of Data

The total volume of fraudulent use, falsification, and counterfeiting of the birth certificate and operator's licenses is unknown for two reasons: first, because of the difficulties in detecting such use and, second because there is apparent inadequate reporting of those cases which are detected. The data available, however, though spotty and not precise, do suggest a problem of some magnitude. For example, the Yuma Fraudulent Document Center reported that at least 5,500 false fraudulent applications for U.S. entry certification are made annually.

More and reliable data is obviously needed to fully delineate the fraudulently obtained driver's licenses and birth certificates for criminal activities. Data is particularly sparse in estimating the number of times persons apprehended for other crimes are found to have false identification documents in their possession, a lack which would seem to be easily rectified by the application of uniform reporting standards.

A common method of establishing a false identity has surfaced, however, and its use is considered widespread by law enforcement officials although hard data have not been obtained. This method is known as the "Infant Death Identity" (IDI) Syndrome and is described as follows:

1. Through public sources, death records, tombstones, newspaper "morgues" and the like, an infant who died young is located who had about the same birthdate and sex of an individual seeking to establish a false identity.
2. The false identity seeker requests (sometimes by telegram) a certified copy of the dead infant's birth certificate. The fact of death is rarely noted on the birth certificate; birth and death records sections are commonly separate.
3. Using the birth certificate as his own, the individual acquires a driver's license, passport or whatever other credential can be so acquired.
4. The addition of a Social Security Registration card, bank accounts, credit accounts, and so on are now undertaken -- all legitimate and all based on the original fraudulent birth certificate.

That this method works quite well is beyond dispute. Cases are recorded by the Passport Office, the INS and the U.S. Customs Office documenting the widespread use and efficiency of the Infant Death Identity (IDI) Syndrome.

The social significance of this technique should not be underestimated since its use appears to be particularly common among drug traffickers, who require several alternate identities and passports for their activities¹. The use of IDI techniques by fugitives of one kind or another is verified by law enforcement officers across the country.

Directions for application of the IDI technique are given in exquisite detail in a current and popular "underground" book², and are commonly quoted in underground newspapers and other "specialty"

¹The Passport Office has discovered several IDI cases wherein an individual with an IDI obtained passport served as affiant for several others in obtaining their passports.

²The Paper Trip, publisher unknown, undated.

publications. The Paper Trip, in fact, advises against document theft and impersonation as a means of establishing identity since it is easier, surer and less risky to use the IDI method.

Cases have been reported to the Task Force in which fugitives have been apprehended with several complete sets of false identity documents in their possession - all apparently obtained by IDI methods.

Because they may be related to Welfare fraud and the IDI syndrome, additional investigation is thought warranted concerning the criminal use of marriage and death records. At this time, no hard data whatever are available relative to the abuse of these two records types. It is inferentially concluded that death records were sometimes used in establishing an IDI credential but it is noted that there are many public sources of death information (tombstones, for example) besides vital records data.

The data available suggest that a false ID potential of some magnitude exists for these two primary state and local documents. A fuller and more quantitative description of the problem is given in the following sections of this report.

SECTION II

THE FALSE ID PROBLEM

Of major concern is the abuse of the birth certificate and the driver's license, represented by the use of these documents to establish false identities. Both (particularly the birth certificate) are breeder documents, and both are important aids to the commission of crimes where a false identity is necessary for the criminal activity.

These documents can be either altered, counterfeited or used as the basis of an IDI process as previously described. The main thrust of this investigation was the fraudulent acquisition of valid documents, though alteration and counterfeiting are discussed also.

That this is an important matter is attested by the following statement by FBI Director, Clarence Kelley:¹

"During the course of recent FBI investigations, positive information has been developed which clearly indicates that subversive and criminal subjects are resorting to the use of counterfeit identification documents, as well as authentic documents of other persons in order to carry out their illegal endeavors. These criminal activities include narcotics, illegal immigration, insurance frauds, counterfeit checks, passport fraud, auto theft and many other crimes."

The problem for state and local authorities is to maintain a cost effective procedure for legitimate birth certificate and driver's license issuance while preventing illegal issuances and detecting the use of counterfeit documents.

The false ID problem can, in the context of this report, be broken down into two independent processes or phases. They are the "application" phase, in which a state or local agency is requested to supply a document (birth certificate or driver's license), and the "use" phase, in which the holder of the document displays it as proof of identity in the conduct of a transaction of one sort or another. These two phases are explored in more detail below.

¹As quoted in the FBI submission to the Task Force; Item 7, Attachment II.

Application Phase

Birth Certificate: Application for a certified copy of a birth certificate normally requires the submission of a written request to the appropriate state or local vital records office, providing information necessary to locate the birth certificate. Ordinarily, the information required consists of the name of the individual whose birth the certificate attests, the date and place of the birth, and the names of the parents. A fee is also required and this must be presented prior to issuance of the copy. Some copies are issued to applicants "in person," but these represent only about 20% of the total copies issued. No identification is usually required to obtain certified copies of birth certificates because of the high volume of requests and the fact that over 80% are requested by mail or by telegram.

Motor Vehicle Operator's License: Application for a motor vehicle operator's license must be made in person to an authorized official. Applicants must establish (usually with a birth certificate), that they meet the minimum age requirements, provide proof of driving ability, demonstrate knowledge of traffic laws, and adequately satisfy certain health requirements. The birth certificate is commonly accepted as proof of identity as well as age for driver's license application purposes. For interstate transfer of licenses, the old license itself is ordinarily the only ID required. Other or additional documents may be required to establish identity of the applicant. The usual documents accepted for identification, besides the birth certificate, are a social security card, driver's license from another state, military ID, U.S. Passport, or a foreign country's driver's license.

Non-driver's Identity Card: Thirty-four states have instituted issuance of a non-driver's identification card, the appearance of which is similar to the driver's license and which is issued by the same officials. The need for such a document derives from the widespread use of the driver's license for identification in check cashing and for other face-to-face business transactions.

Some form of identification is required before issuance of this card, but the requirements appear to be minimal. Usually the same types of documents required for a driver's license are required for this document. None of the documents presented for identification for the issuance of either a driver's license or a non-driver's license are verified prior to the issuance of the non-driver's ID.

The estimated number of applications for these documents is:

<u>Document</u>	<u>No. of Applications Per Year</u>
Birth Certificate (copies)	8 to 10 million
Driver's License	12 million
Non-Driver's ID Card	Unknown

It is not possible to estimate with surety the number of applications per year which are fraudulent. Certain figures are available, however, which are suggestive of a significant problem. The U.S. Immigration and Naturalization Service (INS) estimates that in 1974, for example, about 5100 of the birth certificates submitted to it were fraudulent - and the number is rising. Similar estimates from the Passport Office (PPO) suggest that their discovery of false birth certificates and driver's licenses was about 500 in 1974¹, up 25% over 1973.

Application Patterns

The Washington, D.C. registry reports that birth certificate requests for foreign travel and school admission show seasonal variations while job and social security related requests remain constant. Almost half the applications for birth certificates which were examined by the D.C. Registry stated vague reasons for their requests.

Use Phase

Intended and Common Usage

Each document is used in the following ways.

Birth Certificate: Used to establish age, citizenship, and parentage of the individual to whom the certificate pertains. The establishment of these facts are necessary for school entrance, to secure employment, to obtain a passport, to claim social security benefits, and for other commercial or business purposes where one or all of these facts must be verified. The total utilization of the birth certificate as a means of establishing the identity of the bearer is impossible to estimate.

¹Of about 2.5 million passports applied for.

Driver's License: Issued as an authorization to operate a motor vehicle. In the last several years, however, it has become the single most sought and accepted means of identification. Merchants accept it for identification in cashing checks or to validate the use of credit cards.

Non-driver's Identification Card: Intended as a means of identification for the cashing of checks, use of credit cards, and other instances where proof of ID is required; for all uses of a driver's license except the operation of a motor vehicle.

Fraudulent Uses

Complete information regarding the use of fraudulent or improperly obtained birth certificates for each of these purposes is not available. As noted, however, their use as false ID is thought considerable based on fragmentary and inferential data.

Substantiating ID is sometimes requested at "use points" but this is ordinarily a secondary matter, however. The Passport Office, for instance, requires documents to identify the individual in addition to a birth certificate which establishes citizenship. These additional documents would include driver's licenses, Social Security cards, military or industrial ID. However, in the majority of situations in which the birth certificate or the driver's license are used as primary ID, no additional documentation is required.

When a driver's license or non-driver's ID card is used for check cashing or using a credit card, other identification may or may not be required. In the majority of cases it is not.

Document Fraud

Counterfeit Documents

Counterfeit birth certificates and driver's licenses are used extensively in the establishment of false ID. Such documents are apparently available from many sources and the methods used to create them are varied. One method which has been utilized is to obtain a valid document, either driver's license or certified copy of a birth certificate, and blank out the information to be changed. Once this is done, the form can be reproduced still showing the signature of the official who issued the document and other information that should be retained and the new information is then entered on the document. This procedure produces a document which looks like a valid document and detection of the fraud is difficult.

Other methods used in counterfeiting documents include stealing of actual forms or printing false forms. When presented to untrained, uninformed persons these counterfeit documents may be, and often are, accepted without question as being authentic. With birth certificates, the counterfeit propensity is especially large for the following reasons: there are over 7000 local and state offices issuing birth certificates under their own laws and regulations. No federal control or unifying guidelines exist. The result is the issuance of hundreds of different sizes, shapes, and formats used for these documents. It is accordingly difficult for a document inspector to learn all the legal forms and recognize a counterfeit. Many certificates are issued on ordinary paper making counterfeiting and tampering with legitimate certificates easy for the experienced criminal or the clever amateur.

Altered Documents

Alterations of birth certificates or driver's licenses, while it does occur, appears to be a minor problem compared to counterfeiting or impersonation. The probable reason for this is that alterations are often detectable and are likely to raise questions. From surveys of motor vehicle registries in the state of New York and by the American Association of Motor Vehicle Administration (AAMVA), for example, it appears that the distribution of types of ID document frauds are typically:

	<u>NYS</u>	<u>AAMVA</u>
Altered	3%	80%
Counterfeit	36%	10%
Imposter	61%	10%

The large number of detected "altered" documents in the AAMVA study may be due to the fact that alterations are easier to spot. It is impossible to know how many counterfeits and imposters escaped. The most frequent use of the alterations is thought to be by persons wanting to appear older (to drink or to marry).

False ID Users

It is difficult to develop a profile of those using birth certificates and driver's licenses in establishing false identification. This may in itself suggest that no real pattern exists. Most of the persons and organizations affected by users of false

identities do not collect information of this type. The Passport Office, however, was able to provide some partial information relative to passport fraud. It is:

- Age - 18 to 26 years,
- Sex - male more often than female,
- Race - not available,
- Education - not available,
- Employment Status - unknown,
- Residence (rural, urban) - unknown, and
- Prior criminal record - not available.

The Passport Office indicates that the persons obtaining passports illegally fall into the following categories of criminal activity. These categories include: illegal aliens, narcotic dealers, fugitives, members of radical groups, espionage agents, confidence men and others.

Other data relating to false identity "use" is also minimal because of the lack of records.

Regarding variations of false identity use with geographical areas, the Passport Office also reports that most passport frauds are perpetrated in New York City and Los Angeles. The birth certificates used in passport fraud originate in many places, the most prevalent being California but many counterfeit documents have also been encountered in Illinois, primarily in Chicago. The Immigration and Naturalization Service experience is that the southwest and New York City appear to be the primary areas for illegal aliens. Their means of entry is from Mexico into the southwest or from the Caribbean through the Virgin Islands or Puerto Rico into New York City. Most have false identification, mainly birth certificates, obtained in Mexico, the Virgin Islands, Puerto Rico or in one or another of the Caribbean Islands.

No information is available to the Task Force to indicate whether false identity "use" activity varies with season of year but the economic climate appears to have some effect. There is a definite increase in alien traffic at times when economic conditions in neighboring countries are poor.

False ID Victims

The Task Force was able to obtain very little data from which to draw a profile of victims of the use of false identities. Everyone who is in any way affected by the criminal activity of someone

utilizing false identity is, in a sense, a victim. This would include victims of confidence men; anyone addicted to narcotics; any business establishment that is defrauded; any unemployed citizen who cannot find work because of illegal aliens filling available jobs; and the general taxpaying public.

Birth registries and motor vehicle bureaus receive little feedback on the social, psychological, political or other costs of false ID. Some of the social or psychological impact of false identification is indicated about victims by the above statement. The INS estimates that a significant number of illegal aliens hold jobs that might otherwise be filled by unemployed citizens or acquire unemployment benefits supported by the taxpayers.

False identification investigations, prosecutions, and declinations reported by the Passport Office for the year 1974 included 553 domestic and 238 foreign fraud cases completed with 99 criminal prosecutions closed. The Immigration and Naturalization Service apprehended 14,000 Mexicans fraudulently claiming U.S. Citizenship (5,000 were documented claims with most having valid birth certificates). No information was provided in regard to the number of prosecutions.

Total estimated costs or societal impact of the use of false identity cannot be estimated from information available to the Task Force. No cost information was available from either the INS or the Passport Office.

SECTION III

COUNTERMEASURES TO CRIMINAL USE OF FALSE ID

In this section the subject of countermeasures to creation and use of false identities is discussed. Those countermeasures now employed or about to be employed are described first, and following that, preliminary recommendations for additional countermeasures are given.

COUNTERMEASURES PRESENTLY EMPLOYED

The discussion of current countermeasures is divided by the "application" and "use" phase and by the two types of documents, birth certificates and motor vehicle operator's permits.

Application Phase

Birth Certificates

Matching of birth and infant death records: It is sometimes possible to detect birth certificate requests for a person who died before the age of one, because some states match the birth and death records and post the fact of death on the birth certificate. For those who die after the first year, there is no consistently used method at present which indicates the fact of death in the registry of births. Also, the infant death matching program is normally only carried out at the state Vital Records Office, and if the certified copy is requested from a local Vital Records Office, detection would not be possible, the information not being available to the local registry. This program has minimal impact in reducing fraudulent use of the birth record nationally since all states do not have such a program. Even in those states that do match, very few have a matching program in the local Vital Records Office. The effectiveness of the program even if broadly implemented may be short term because counterfeits could replace fraudulent applications of deceased persons.

Keeping track of the number of applications for particular birth certificates: Again this program has a minor impact on reducing the fraudulent use of birth certificates because of the small number of states doing it and the very few improper applications which could probably be detected in this manner.

Use of safety paper to prevent alteration of valid certified copies: Several states use safety paper which makes alterations obvious. If generally used, it would be harder to produce a passable counterfeit.

Motor Vehicle Operator's Permits

The National Highway Traffic Safety Administration (NHTSA) Highway Safety Program Standard No. 5, Driver Licensing, requires the states to seek positive proof of full name, date, and place of birth prior to issuance of an initial driver's license. Currently, 41 states claim to comply with this provision. This program is probably effective in dealing with persons in the 16 to 18 age range. These people probably have had driver's education in high school and the driver education certificate along with the birth certificate should identify the individual effectively. For persons applying for their first license at a later age, it becomes more difficult to confirm identity. Normally, a birth certificate is presented and this is accepted as proof of both age and identity.

The National Driver Register is designed to assist states in problems of interstate driver control: States participate on a voluntary basis, entering in the Register the names of drivers who have had their licenses suspended; and requesting a search of the Register files for records of applications prior to issuance of new licenses to those persons newly arrived in the state. The impact of this program on the false ID problem is expected to be minimal since its purpose and design is only to prevent persons with a suspended license in one state from going to another state and getting a license.

Another interstate control of licensed drivers available to the states is the Driver License Compact: Twenty-nine states are now members of the Compact. The Compact requires the member states to forward records of out-of-state traffic violation convictions to the driver records agency in the home state of the driver, and upon issuance of a driver license in any state it requires all previous current valid licenses to be surrendered to the new state of issuance.

Additionally, Section 6-101 (c) of the Uniform Vehicle Code (UVC), a model traffic code available to the states and endorsed by NHTSA, provides that out-of-state drivers surrender all licenses held by the applicant upon issuance of a new license, and that such licenses be returned to the issuing state. Twenty-nine states belong to the Compact and eight additional states have the UVC provision. However, not all of these states adhere to the provisions

of either the Compact or the statute.

Twenty-eight states now have licenses which they consider tamper proof. However, since alteration of licenses represents a small percentage of the total false ID problem, the impact in this area is limited. It would be advantageous, however, if all states were to develop such a program since it would aid in eliminating this portion of the problem. It would also make it more difficult to develop counterfeit licenses. Also, 36 states now have photos on their licenses which also aids in reducing the possibility of alteration and makes counterfeiting more difficult.

Use Phase

For the most part, countermeasures at the point of use are almost non-existent. The only organization found with an extensive program for investigating evidence presented is the Passport Office. Through a training program, PPO clerks have been sensitized to fraudulent practices. Accordingly, when confronted with suspicious documents, a verification of them is attempted. This procedure is principally responsible for the detection of passport frauds.

In the commercial sector, many businessmen do not examine a driver's license closely when it is presented for the cashing of a check. It is fair to conclude, therefore, that very few countermeasures are applied in the "Use" phase. Most detection of false ID occurs after the commission of a fraud.

SECTION IV

RECOMMENDATIONS

This section sets forth the recommendations of the Task Force for countering the false ID problem. Because of fundamental differences in the documents themselves, the methods for obtaining them, the standardization and control applied to their distribution and their differential viability in the conduct of frauds and other criminal activity, the recommended actions are grouped by document.

These recommendations derive not only from deliberations of the Task Force and examination of data and evidence made available to it; but also from careful consideration of the suggestions offered by officials in the field. Many of the suggestions represent the common thinking of many individuals considering the issues independently.

Birth Certificate

1. Match all deaths to the corresponding birth certificate. This would represent an extension of the infant death matching program. The cost of such a program would be very high because of the time required to manually match the records as well as the need to send copies of death certificates to other states when the birth and death do not occur in the same state. If this program was instituted, and if information was transmitted to the local Vital Records Offices, it would be an effective means of preventing persons from using a deceased person's birth record. The IDI syndrome would largely disappear.
2. Establish better lines of communication between the states and Federal Agencies. This would be a very helpful and inexpensive mechanism of dealing with the fraudulent ID problem. Many states have noted that while they cooperate with the Passport Office, INS, the FBI and other Federal Agencies, they are never informed of the outcome of cases on which they have been consulted. The states are not routinely notified when someone who is apprehended bears an improper birth certificate obtained from their state.

3. Increase the penalty provisions of the vital statistics law with regard to the possession and use of counterfeit, altered, or imposter certificates. This proposal is being given strong consideration now, and several states are already in the process of strengthening their laws. Also, the Model State Vital Statistics Act, model legislation recommended by HEW, is presently being revised and stronger penalty provisions are being considered for inclusion. This may have some effect on the use of false ID for relatively trivial offenses.
4. Vital records offices keep record of requests for certified copies. Often the same birth record is multiply used to establish false identities. If records are kept of the certified copy requests for each record, the possibility of false ID use would be raised and the matter could be investigated. Many states have kept such records by noting on the back of the certificates the date of each request and number of copies issued. With the use of microfilm, however, this practice is no longer practical. A new system would have to be developed with the microfilm record.
5. Institute better control over blank certificate forms and forms used for the issuance of certified copies. Most states already exercise some control over these forms, and it would not be costly for all states to tighten up. It will also be necessary for any procedures that are developed to also apply to all local Vital Records Offices.
6. Check the death index for all requests for certified copy in the 20-39 age group (the ages where most fraud activity appears to occur). This suggestion has merit, of course, only for those cases where birth and death occur in the same state but appears to be useful in dealing with the IDI syndrome where death shortly follows birth. This would involve a considerable expenditure of energy at issuing offices, however. A Kansas survey found that 25% of the requests processed were from the 20-40 age group. So the numbers involved may not be small. It is a partial alternative to the interstate birth/death matching scheme.

7. Establish a degree of Federal control over the vital registration system. This could be limited to the enactment of Federal legislation relative to the obtaining, use, possession, or sale of fraudulent or improperly obtained birth records and the establishment of penalties under Federal law. It is not thought that Federal assumption of the states' traditional prerogatives in the issuance of birth certificates would meet with general legislative approval. Voluntary cooperation among states is greatly preferable to Federal mandate.
8. Provide Federal funding for those states willing to adopt recommended procedures designed to curb the false ID problem. This funding would be used by the state in setting up and maintaining those programs. Since the cost of some of these programs would be quite high, it is thought necessary that some Federal support should be provided.
9. Adopt an Executive Order whereby Federal agencies will accept only certified copies issued by a state Vital Records Office. This would be a means of encouraging states to move toward a system of state certification and away from local certification. Many of the false ID problems originate in local Vital Records Offices. This recommendation does not appear costly.
10. States issue uniform certified copies. "Uniform," in this context, refers to format, information contained, signature and sealing characteristics, paper used, dimensions, color and other physical aspects of the document. Presently, the number of different types of certified copies issued in this country is very high. This makes it difficult to identify a valid certified copy format from an invalid format. Such a recommendation should also include considerations of alteration-proof paper and methods of control. The cost of the program, once the forms are developed, would not be exceptionally high.
11. Set up educational programs for persons issuing certified copies. These programs would concentrate on sensitizing these persons to possible fraud and the means for detecting it. This program would be modestly costly, but could be quite effective.

Driver's Licenses

1. States adopt tamper proof forms with pictures. This would aid in reducing alteration and counterfeit problems. It would be costly for those states (about 20) which have not already undertaken this process.
2. Encourage states to put more identifying information on the driver's license. Many states have recently dropped such items as race, sex, weight, height, color of eyes, or color of hair. These items do help in determining whether the person holding the license is in fact the person named on the certificate. A picture obviates the need for some but certainly not all of this information. The cost of putting this information on the license would be small and these could be of substantial benefit.
3. Establish an educational program for persons giving driver tests and issuing licenses. The program would emphasize the problem of false ID and train the officials in detecting false ID. Since many of the persons establishing false identification are above the age of first driver's permit, the older applicants should be checked more closely. Also, this training program would probably be costly but the results significant.
4. All states should require the applicant to present positive identification prior to issuance of a license.
5. Require the verification of the birth certificate prior to the issuance of any license. This could not be done at the application stage but would require that all licenses be issued through a central control office. Before the license would be mailed to the applicant, the birth facts would be verified through the state of birth. This procedure would be expensive but effective when coupled with other suggestions presented here relative to the birth certificate.
6. All states should enter into the Interstate Driver's License Compact and collect licenses held by an applicant from other states.

Other Comments

This Task Force has looked closely at the two documents emanating from state sources which are of fundamental importance to the commission of false ID crimes. There are many others which are sometimes utilized in establishing false ID and in the subsequent commission of crimes. It was strongly felt that the birth certificate and the driver's license are pivotal because of the "breeder" character of the former and the broad usage of the latter.

It should be reemphasized that neither the birth certificate nor the driver's license was ever intended to be used as an identification document. In modern commerce and business, they have become such to the extent that the overall false ID problem must be considered in that light. It would be useless at this point to say they shouldn't be considered identification documents because their use as such has become so extensive, a fact which illustrated a broad societal need for quick, compact, positive ID of some form.

While the birth certificate is sometimes used for identification, the driver's license is used much more extensively. The issuance by 25 states of non-drivers identification cards has caused the status of the driver's license as an identification document to become even more firmly entrenched. Accordingly, it would seem more logical to work on improving the procedures for issuing driver's licenses and strengthen that document's resistance to fraud and counterfeit than try to change attained public acceptance as an ID.

This would involve two processes: (1) Procedures relating to identifying the applicant would have to be strengthened; (2) The document would have to be made tamper proof and sufficient identifying information would have to appear on the license. In this way, the need for a license and an identification card would be met.

States issuing non-driver's ID cards should also implement stronger controls, as noted above. Since these documents are issued only for identification purposes, it is absolutely essential that their issuance be properly controlled.

Improve the response time of the National Driver Register, i.e., it should go on-line, rather than using the present system of mail response.

ATTACHMENT I

Composition of the FACFI Task Force on
State and Local Documents

The members of the State and Local Documents Task Force and their professional affiliations are as follows:

Loren E. Chancellor, Chairman	Registration Methods Chief, Division of Vital Statistics, U.S. Dept. of Health, Education and Welfare
George Gay	Division of Vital Statistics, U.S. Dept. of Health, Education and Welfare
Irvin G. Franzen, President	American Association for Vital Records and Public Health Sta- tistics
Charles Whitemire, Special Assistant	Council of State Governments
Frank Altobelli, Chief	Licensing and Adjudication Division, National Highway Traffic Safety Administration
James Latchaw	National Highway Traffic Safety Administration, Department of Transportation
John Crandall, Chief	Vital Records Section D.C. Department of Human Re- sources
Deane L. Huxtable	State Registrar, Vital Statis- tics, Virginia State Depart- ment of Health
C. R. Newhouser	International Association of Chiefs of Police

ATTACHMENT I
(Continued)

Arlie Schardt	American Civil Liberties Union
John O'Dowd	Passport Office U.S. Department of State
Joseph T. Kochanski	Law Enforcement Assistance Administration, U.S. Depart- ment of Justice
Michael T. Horkan	Immigration and Naturalization Service, U.S. Department of Justice
Arthur A. Tritsch, Director	Driver's Services Division American Association of Motor Vehicle Administrators
Roger Smith, Acting Chief	Vital Statistics Section California Department of Health
Lieutenant J. S. McKinnon, Asst. Supervisor	Investigations Florida Highway Patrol
Jack Pawley, County Clerk	Kanawha County, West Virginia
Robert J. Langling, Director	Department of Investigations New York Department of Motor Vehicles
Frank E. McCullion	New Product Manager American Bank Note Company

ATTACHMENT II

Synopsis of Material in
Task Force Files

1. Report of John J. O'Dowd, Acting Chief, Legal Enforcement Branch, U.S. Passport Office, (with Attachments).

This report focuses on the false ID problem and issues from the PPO's standpoint. It describes generic types of passport fraud, notes existing countermeasures, comments on PPO procedures, presents recent statistics on the number of detected frauds, presents a profile of passport applicants for FY's 1973 and 1974 and sets forth recommendations for ameliorative action. Also included is a statistical summary of fraudulent documents presented at passport offices and a number of interesting case histories.

2. Letter; Comments of Irving G. Franzen, President, American Association for Vital Records and Public Health Statistics.

This report contains the experience of the AAVRPHS regarding false ID, includes examples of criminal techniques used in obtaining false ID and proposes a number of suggestions for reducing the problem. Also submitted are a set of suggested goals for a Federal Advisory Committee on False ID.

3. Report by Michael T. Horkan, Immigration and Naturalization Service, U.S. Department of Justice.

This document outlines the general INS false ID problem, traces the background organization and activities of the Fraudulent Document Center and presents recent statistical exhibits and summaries of illegal alien and fraudulent document activity detected by the INS.

4. Report of John Crandall, Chief, Vital Records Section, D.C. Department of Human Resources.

This report treats the "application" and "use" phases of birth certificate processes. Information is given on extant countermeasures to abuse and recommendations for minimization of the problem.

5. Report of Deane Huxtable, State Registrar of Vital Statistics, Virginia State Department of Health.

ATTACHMENT II
(Concluded)

This document treats the issue of citizenship determination and discusses some measures to achieve protection of the birth certificate document. Some of the experience and plans of Virginia are cited.

6. Report from The National Highway Traffic Safety Administration.

"An Analysis and Report on State Laws Requiring Certain Information for Determining an Applicant's Identity and Eligibility when Applying for a Driver's License," prepared by the licensing and Regulations Branch, Driver Licensing and Adjudication Division, Office of Driver and Pedestrian Programs, Traffic Safety Programs.

7. Report from The Federal Bureau of Investigation, comprising discussion of Document Counterfeiting, Nature and Extent of Crimes Committed by Persons Utilizing False ID and Selected False ID Case Histories.

8. Questionnaire Sent to State Vital Registration Executives.

This paper, besides presenting the form sent by FACFI to solicit information on the status of an Infant Death Matching Program in each state and also includes a tabulation of responses. Information relative to access to records and the number of offices in each state issuing certified copies of birth certificates was also provided.

9. Summary of Responses from State and Territorial Health Offices.

This document tabulates the suggestions for improvement of the false ID problem. The request for recommendations was made by E. B. Perrin, NCHS and C. M. Kelley, FBI.

10. Submission by the American Association of Motor Vehicle Administrators.

The results of a survey on the fraudulent ID problem conducted by the AAMVA are given along with a report on the scope of the problem and recommendations for solution.

11. Report of Robert Langling, Director, Department of Investigations, New York Department of Motor Vehicles.

A survey conducted among New York State Motor Vehicle officials is summarized including statistical data, heuristic information and recommendations for solution of the false ID problem.

APPENDIX C

BACKGROUND PAPERS

As part of its support to the FACFI under a Department of Justice contract, the MITRE Corporation developed four papers which provide a broad background on technical subjects related to problems of personal identification. This Appendix presents the MITRE papers as modified by comments from FACFI members and other reviewers.

Appendix C1 provides an overview of Electronic Funds Transfer Systems (EFTS), which permit financial transactions to be accomplished with minimal transfer of negotiable documents. These systems have the potential to reduce counterfeiting and forgery of checks simply by reducing the amount of negotiable paper in circulation. However, they may be vulnerable to more sophisticated types of false ID fraud based on electronic manipulation of data.

Appendix C2 gives a general description of automated identification equipment, which assists or replaces human judgment in the identification of individuals seeking to accomplish financial transactions or to exercise privileges. Such machines verify identity through the recognition of special cards or passes, memorized "passwords", or by personal characteristics such as fingerprints, speech, or handwriting.

Appendix C3 gives vendor information on a variety of fraud-resistant identify verification devices. This information, which includes cost, applications, and operating principles, was assembled from vendor responses to an announcement placed by the FACFI in the Commerce Business Daily, a Federal newsletter widely distributed to industry.

Appendix C4 is a broad survey of the problem of false identification as it is perceived in several foreign nations. This Appendix is based on international surveys performed on behalf of the FACFI by the State Department and by Interpol and discusses national systems of personal identification that have been instituted through custom and law.

APPENDIX C1

**ELECTRONIC FUNDS TRANSFER SYSTEMS (EFTS):
AN OVERVIEW**

R.J. Ellis

**The MITRE Corporation
Bedford, Massachusetts**

March 1976

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
I INTRODUCTION	C-7
II TYPES OF ELECTRONIC FUNDS TRANSFER SYSTEMS	C-9
Check Truncation	C-9
Automatic Payroll Depositing	C-15
Preauthorized Debits	C-17
Point-of-Sale Terminal Systems	C-20
Automatic Teller Equipments	C-23
III ELECTRONIC FUNDS TRANSFER SYSTEM EQUIPMENTS	C-26
Check Truncation Systems	C-26
Automatic Payroll Depositing	C-27
Preauthorized Debits	C-28
Point-of-Sale Terminals (POS)	C-28
Automatic Teller Equipments	C-29
IV PROBLEMS AFFECTING EFT	C-31
Encouraging Acceptance of EFTS	C-31
Planning and Financing EFT Systems	C-33
Governmental Regulation	C-34
Legal Questions	C-34
V SECURITY	C-39
VI IMPACT OF EFTS UPON CRIMINAL USE OF FALSE IDENTIFICATION	C-43
Fraud Against Business	C-43
Fraud Against Government	C-43
VII CONCLUSIONS	C-45
REFERENCES	C-47

LIST OF ILLUSTRATIONS

<u>Figure Number</u>		<u>Page</u>
1	Check Truncation	C-12
2	Check Truncation Systems	C-13
3	Payroll Depositing	C-16
4	Preauthorized Debits	C-19
5	Point of Sale Terminal System	C-21
6	Automatic Teller Systems	C-24
7	Automated Clearing House Locations	C-35

SECTION I

INTRODUCTION

Since the mid 1960's, interest has grown in the possibility of conducting banking transactions without checks. Early journalistic efforts focused upon the possibility of utilizing electronic transmissions to replace checks and substantially reduce the amount of cash circulated within our society. In 1967, an article published in the Harvard Business Review reported that

"Technically speaking, the checkless society is virtually feasible now; the computer hardware is capable of handling it. But enormous problems remain, particularly in planning how the system will be instituted and financed, persuading the segments of the economic community to accept it, and showing them how to take advantage of it".¹

Five years later another special report stated

"Except for the increased proliferation of bank charge cards, the payments system of 1972 seems much like that of 1967 and few, if any, technological advances have occurred in the last half decade to affect it. Behind the scenes, however, the foundations and subbasements of a new plastic card society (not checkless but surely "less-check") have been put in place, and the superstructure will rise rapidly above ground level in the next few years".²

Systems which utilize electronic impulses, generated and interpreted by computers, to effect debits and credits in financial transactions are called Electronic Funds Transfer Systems (EFTS). What are the capabilities of electronic funds transfer systems? Are the "enormous problems" of planning such systems being resolved? Are there new problems which have surfaced? Why is electronic transfer being pursued? What does it offer the financial industry, the business community, the individual? This paper will examine electronic funds transfer in an attempt to answer these questions.

SECTION II

TYPES OF ELECTRONIC FUNDS TRANSFER SYSTEMS

Electronic funds transfer is not a new concept. It is an expansion and formalization of practices which have been utilized within the financial industry for many years. For example, Federal Home Loan banks make advances to their member banks by depositing funds to their demand deposit accounts; business firms transfer money by wire from city to city through the commercial bank wire system (Bank Wire) or the Federal Reserve funds transfer system (Fed Wire)³; many employees have their pay credited to their checking accounts; homeowners make mortgage payments through pre-authorized transfers from their checking accounts to the mortgage holder; and banks* make prearranged transfers from customers' checking accounts to their saving accounts. All of these transactions are electronic funds transfers and are common practice. Some take place within a bank, some between banks, and some between banks and customers. The capabilities of computers are substituted for human activity and physical transport of credit and debit instruments. EFT offers significant advantages to the banking industry since it will allow banks to expand the range of their services at the same time they reduce expenses.

Although there are a large number of services which can be classified as electronic funds transfer, five main categories have been receiving most attention. They are: check truncation, automatic payroll depositing, preauthorized debits, point-of-sale terminal systems, and automatic teller systems.

Check Truncation

Check truncation systems are intended to reduce the quantity of checks handled throughout the banking industry and the Federal Government. It is estimated that the number of checks written in the U.S. has increased from 12 billion in 1960 to 27 billion in 1973, with a current growth rate of 6 to 7%.⁴ This rate would place the 1975 volume at over 30 billion. Such a growth rate concerns representatives of both the financial industry and the Federal Government for several reasons. The first reason for concern is that such large volumes of checks could inundate

*Unless specifically stated, "bank" is used as a synonym for depository institution. See Section IV for discussion of different types of depository institutions.

the banking system with paper, causing decreased efficiency or worse, total collapse. The magnitude of this problem is better appreciated when it is recognized that the average check is handled a minimum of 26 times--10 times in the bank alone.⁵ Thus check processing is highly labor-intensive. The immediacy of this problem was addressed in a study performed by the A. D. Little Co. in 1971 for the American Bankers Association's Monetary and Payments System Planning Committee (MAPS). That study reported that

"the check-processing system for the nation's commercial and Federal Reserve banks is performing smoothly and, with only minor delays and inaccuracies, can be expected to handle the nearly 25 billion checks we are writing in 1972. Even at the predicted 7% annual increase... the present processing system can handle the load at least through the end of this decade".⁶

The problem is that the end of the decade is approaching at a faster rate than a solution to the otherwise inevitable result.

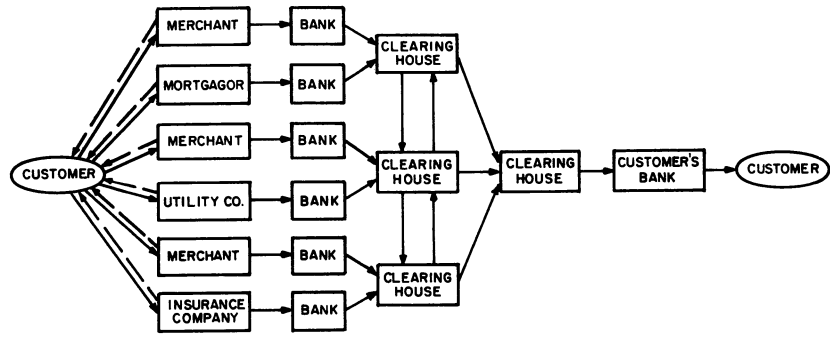
A second concern involves cost. No significant technological improvements have been made in the handling of paper documents in recent years. It continues to be labor intensive. Direct processing costs amount to approximately 16 cents per check, or \$4.8 billion annually at the 1975 volume rate. Feasibility studies indicate that this cost could be cut by as much as 50% through application of EFT methods.⁷ Banks will face accelerated increases in handling costs unless the process is converted from labor intensive to capital intensive. Increased labor costs will either reduce profits or require that the increased costs be passed on to the customers.

A third concern is the growth in float. Float may be defined as the value of all checks which have been issued but which have not yet cleared through the banking system. An individual utilizes float when he writes a check against funds which have not yet been deposited to his checking account but will be deposited before the check clears through the banking system. Corporations utilize float in the same way. Banks also utilize float, but in a slightly different manner. There is a relatively short time period (a few days) in a check's travels through the payment system when the check is between the bank which has accepted it and the bank upon which it is

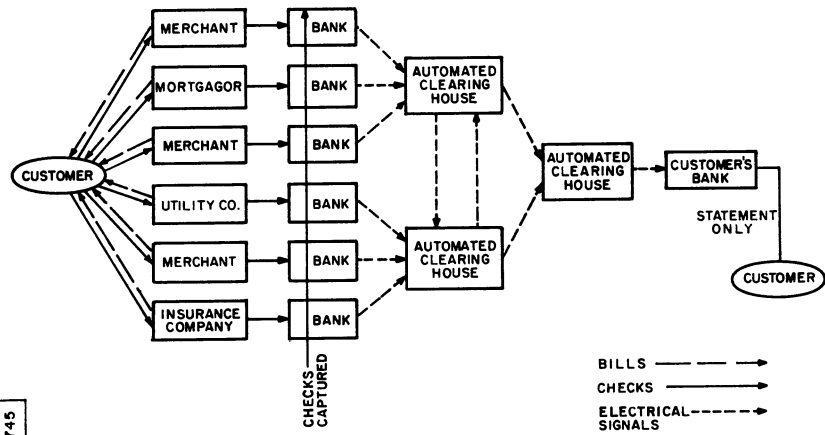
drawn. During that time period, the funds represented by the check are actually assets to both banks simultaneously; one bank because it has accepted it, the other because it has not yet paid it. At any time, the amount of money represented by all such checks equals several billion dollars, on which double interest may be earned. Individuals like float, merchants and corporations like float, and the banks like float, but the Federal Government does not. Float provides an elasticity to the money supply beyond the control of the Federal Reserve Board, which is responsible for providing such control. This float can be reduced only by greater speed in processing checks through the banking system.

For the above stated reasons, there are pressures from both the banking industry and the Federal Government to reduce the number of checks being used. Check truncation offers at least a partial solution. Although it does not reduce the number of checks written, it eliminates the flow of checks through the banking system by holding them at their point of entry. Further processing is accomplished electronically. A schematic representation of check payment, with and without truncation, is shown in Figure 1. A significant aspect of this type of system is that the cancelled checks are not returned to the writer. The customer's only direct exposure to check truncation is in his bank statement. This statement will not be accompanied by cancelled checks; therefore it must contain sufficient information for the customer to verify debits on the basis of receipts received at the time of purchase. Opponents argue that the public will not accept such statements. A further unresolved difficulty is the storage and final disposition of the checks captured at point of entry. Acceptability by the public is questioned on the basis of the above mentioned concerns. The Committee on Paperless Entries (COPE) in Atlanta concluded that such a scheme would reduce check processing costs to the banks by as much as 20%.⁹

Several variations of check truncation have been advocated. Among these are "bill check" and "giro" (from the Greek meaning to turn or transfer). "Bill check" and "giro" are represented in Figure 2. These schemes represent potential solutions to the "paper flood" in that fewer checks are actually written by the consumer. "Bill check" would allow a customer to pay routine bills, such as utility bills, by indicating on the bill the amount he wishes to pay, detaching a payment section, and returning this section to the company issuing the bill. The company



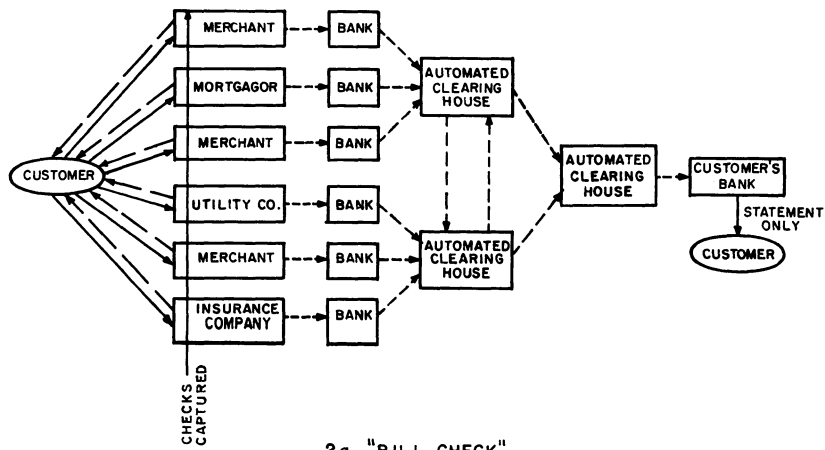
1a CONVENTIONAL CHECK MOVEMENT



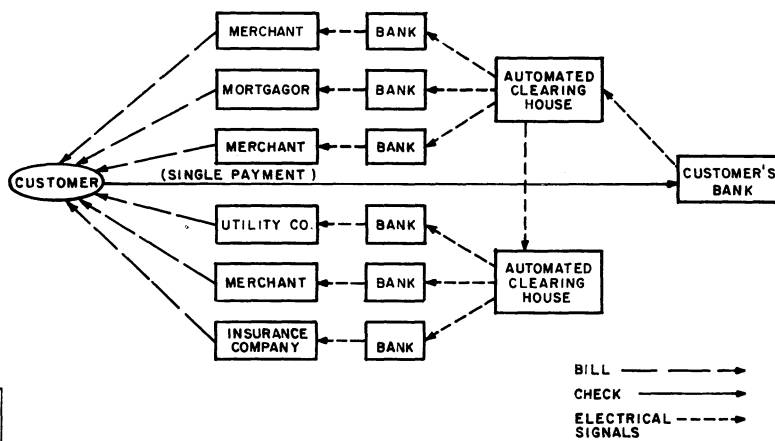
1b CHECK MOVEMENT WITH TRUNCATION

IA-47,745

Figure 1 CHECK TRUNCATION



2a "BILL CHECK"



2b "GIRO"

Figure 2 CHECK TRUNCATION SYSTEMS

IA-47,746

credits the customer's account and creates a magnetic tape containing bank and account numbers and the amount of the payment for each customer transaction. This tape is sent through the company's bank to an automated clearing house where individual tapes are compiled for each member bank. Upon receipt of this tape, the bank debits the customer's account. No check is returned to the customer since none was created. Paper capture is at the company rather than at the bank. "Bill check" promises substantial benefit to the bank. Estimates of bank savings through "bill check" range from 2¢ to 4¢ per item processed.¹⁰ Benefits to the customer are not readily apparent since he will have to prepare and mail the same number of items ("bill checks") as he would have if he had written checks. He suffers a disadvantage in that he loses the record of payment represented by his cancelled checks. Theoretically the proof of payment would be represented by his bank statement. A disadvantage accrues to the companies since they must prepare transaction tapes to be sent to their banks.

A second variation of check truncation is called "giro". Under this system a customer would receive bills on a combination invoice/payment authorization form containing all pertinent accounting and identification information for both customer and vendor accounts in machine readable language. The customer would detach the payment authorization section, enter the amount of the payment he wishes to make and send all of these authorization forms to his bank. His bank would then generate a magnetic tape and forward it to an automated clearing house for recompilation and distribution among its member banks.¹¹ Such a system would reduce the banking cycle since customer payments would go directly to banks. Benefits to banks would be less than with "bill check" since they would be required to prepare original magnetic tapes from machine readable authorization forms. Vendors would benefit since the tape preparation requirement would be transferred to the banks. However, vendors would be required to prepare machine readable bills. Customers would benefit since they could send a number of payment authorizations to their bank at one time. The customer's proof of payment is represented by a bank statement rather than individually drawn checks.

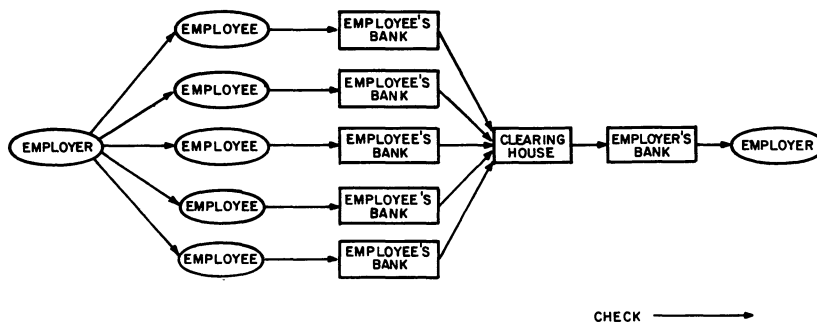
Bank truncation schemes appear to offer significant opportunities to overcome the paper flood being created by checks. However, most of the advantages accrue to the banking industry with potential detriment rather than benefit to the customer. Such systems as "bill check" and "giro" are being implemented, although the response seems to be less than encouraging at this time. Banks offering such services

have failed to merchandise these systems aggressively. Better merchandising may gain greater customer acceptance even though real advantage to the customer is questionable.

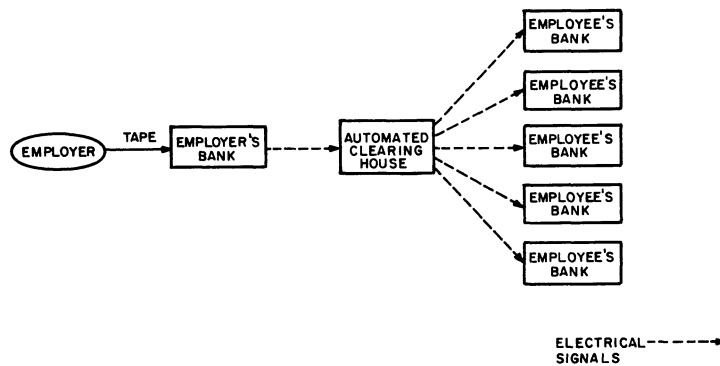
Automatic Payroll Depositing

For many years employers have sent employee paychecks directly to the employee's bank if so authorized by the employee. Some companies mail individual checks; some send a single check per bank accompanied by a list of the amounts to be deposited to each account. The first method, called direct depositing, saves the employee postage or a trip to the bank; the second method introduces the concept of automatic payroll depositing. In a fully developed system of automatic depositing, the company prepares a single magnetic tape, listing by bank, all of the deposits to be made. The taped information is transmitted to the company's bank where "on-us" transactions (transactions within that bank) are accomplished and the remaining information transmitted to an automated clearing house for distribution to the appropriate banks. Figure 3 illustrates automatic payroll depositing. Such a system of payment offers substantial opportunity to reduce the number of checks in circulation. For example, if the Federal Government were able to convert all of its payroll and benefits payments to automatic depositing, the number of checks written nationwide would be reduced by 44 million per month.¹² Such a conversion would save the Government approximately \$62 million per year in postage, printing and lost check costs. Substantial benefits would also accrue to many private employers from automatic payroll depositing. These benefits would take the form of reduced costs in preparing and distributing paychecks and replacing lost or stolen checks. However, if both the automatic payroll depositing system and the check distribution system must be maintained by the same employer, expenses could be increased. Advantages to be gained, therefore, appear to be strongly linked to employee (or payee, in the case of benefits) acceptance. Acceptance has been encouraging but not overwhelming to date. Reasons for lack of acceptance commonly stated by employees include:

1. Mistrust of computers.
2. Loss of control over personal finances.
3. Fear of loss of personal privacy.
4. Enhanced feeling of personal worth through direct receipt of a paycheck.



3 a CONVENTIONAL PAYROLL SYSTEM



3 b AUTOMATIC PAYROLL DEPOSIT SYSTEM

Figure 3 PAYROLL DEPOSITING

IA-47, 747

5. No direct benefit received--banks are only beneficiary.¹³

Within the banking industry itself there are reservations with respect to automatic payroll deposits. Although the Atlanta COPE project suggests savings of 5¢ to 10¢ per transaction,¹⁴ loss of bank float is of concern to many. Many bankers are disinclined to surrender their present ability to use employers' payroll funds until paychecks have been cashed and cleared. It is generally conceded, however, that as the check burden becomes increasingly intolerable, the banking industry will not only be forced into accepting automatic deposit schemes but they will be required to offer inducements to gain acceptance from both companies and individuals. One obvious advantage of automatic payroll depositing is that the paycheck and the pay envelope are removed as targets of crime. The dramatic increase in the use of credit cards suggests that the reasons for lack of acceptance listed above are being overcome, and as customer acceptance grows, the benefits of automatic payroll depositing will dictate its adoption. A strong factor affecting this acceptance is the Federal Government's use of automatic depositing. The Social Security Administration, which issues 43 million checks per month, is offering direct depositing now. The objective is automatic depositing for all such payments. The Air Force presently offers direct depositing and is experimenting with automatic depositing. The other services are expected to follow. Payments under the Railroad Retirement Program are also due to be converted to EFT.¹⁵

As more recipients of government payments accept automatic depositing, fears will be overcome, either by experience or through regulation controlling abuse (such as the Privacy Act), and other employers will be persuaded to join the program. Since automatic depositing requires the payee to have a bank account, banks will engage in heightened competition for this expanded market potential, thus benefiting the customer. Although acceptance of automatic payroll depositing seems to be slow in developing, the impetus provided by governmental programs in this area should insure the future of this type of EFT.

Preauthorized Debits

Like many other bank services presently being classified as EFT, preauthorized debiting is not an innovation to the banking industry. Although not all banks offer such services at this time, many banks have accepted authorizations from customers to

subtract funds from their accounts for mortgage or other types of loan payments. Some banks have extended this service to include life insurance premiums as well. It is estimated that 40% of the checks written each year in the U.S. (12 billion at the 1975 rate) are made payable to utilities and retail stores.¹⁶ Theoretically, all of these checks could be eliminated through debit preauthorizations. Figure 4 illustrates a preauthorized debit system. The ultimate preauthorized debit system would have the customer authorize his bank to pay any bill presented by any company he has specified. These companies would then prepare magnetic tapes which would be processed as discussed under check truncation above. Potential advantages to the customer include:

1. Assurance that bills are paid.
2. Convenience in paying recurring, identical bills.

Disadvantages include:

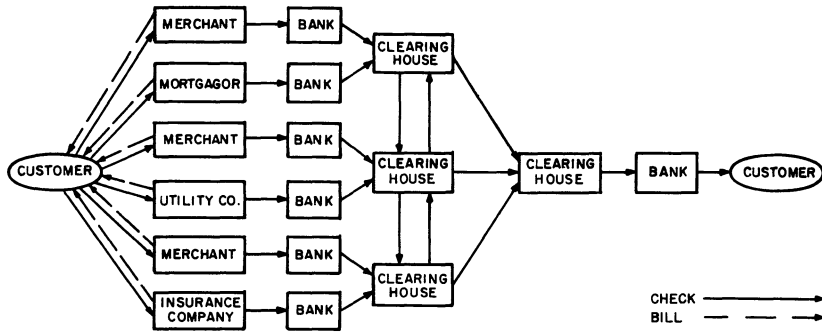
1. Loss of control over finances.
2. Inability to pay less than the full amount of the bill.
3. Loss of leverage against a company which has sold defective merchandise or services.
4. Loss of a cancelled check as proof of payment.
5. Fear of bank mistakes.
6. Loss of float.

Advantages to business include:

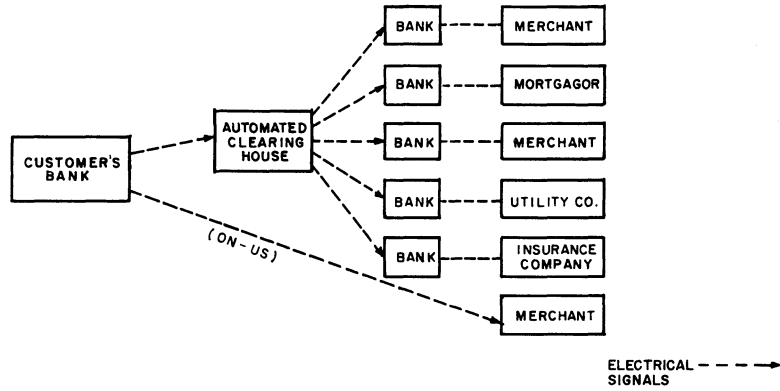
1. Greater assurance of payment in full on charge accounts.
2. Bills sent to one bank rather than to many customers.

Disadvantages to business include:

1. Requirement for equipment to compile billing information on magnetic tape.
2. Requirement for equipment to transmit electronic data to bank (hand carrying is a possible alternative).



4a WITHOUT PREAUTHORIZATION-NO EFT



4b WITH PREAUTHORIZATION-EFT

Figure 4 PREAUTHORIZED DEBITS

IA-47,748

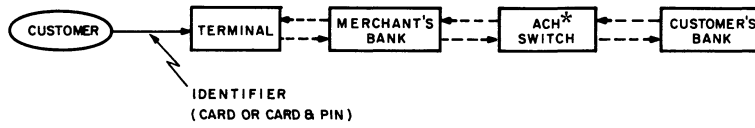
The principal advantage sought by banks would be a reduction in the number of checks written. Customers would probably use such a system for payments of established regularity in time and amount, such as mortgage payments, loan payments, budgeted utility payments, and insurance premiums, but they are unlikely to preauthorize payments to retail stores. It would appear then that a system of preauthorized debits might be offered by a bank as a customer service, but such a system would not find wide acceptance and would not significantly reduce the number of checks being written. It is doubtful such a system would be economical for the bank.

Point-of-Sale Terminal Systems

Point-of-sale terminal systems may be divided into two basic types: validation terminal systems and cash terminal systems. Validation terminal systems may accomplish a variety of functions depending upon the options built into the system, but their basic purpose is to provide the merchant with information about the customer's credit status. Cash terminal systems allow for the transfer of funds, thus completing the entire transaction. Figure 5 illustrates these two types of systems.

The basic types of validation terminal systems are: check verification terminals, which are utilized to ensure that a customer offering a check has sufficient funds in his account to cover the check; and credit authorization terminals, which allow a merchant to obtain credit authorization for a charge card purchase. The check verification terminal system must be connected on-line to the customer's bank to accomplish its purpose. Methods for accomplishing this connection and equipments required at both the merchant's location and at the bank are discussed in Section III. The credit authorization terminal system is connected to the credit institution for on-line credit checking. The credit institution may be either the merchant's own credit department (e.g., Sears, Montgomery Ward) or a bank system (e.g., Master Charge, Bank Americard). When the credit department is not collocated with the sales department, the terminal contains the capability to connect the two through the telephone system. Validation terminal systems are not a part of the collection process; therefore, current collection systems are unaffected by validation terminals.

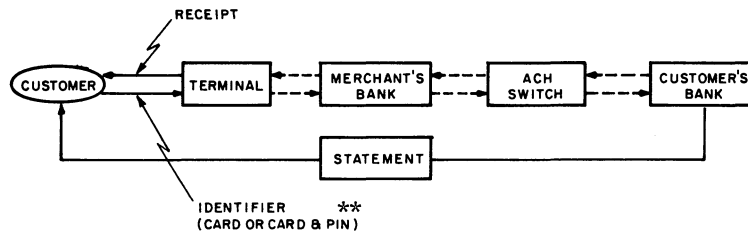
Cash terminal systems have the capability to conduct a complete cash transfer. Such systems supplement customary collection systems. Since cash terminal systems accomplish



*Automated Clearinghouse

ELECTRICAL - - - ->
SIGNALS

5a VALIDATION TERMINAL SYSTEM



**Personal Identification Number

ELECTRICAL - - - ->
SIGNALS

5b CASH TERMINAL SYSTEM

Figure 5 POINT OF SALE TERMINAL SYSTEM

the entire transaction, the terminals must connect the customer's bank to the merchant's bank. This is accomplished through a switching facility. A complete transaction would take place in the following way:

1. A customer initiates a purchase; the clerk enters the customer's ID which includes his bank and account number, the merchant's ID which includes his bank and account number, and the amount of the transaction.

2. The terminal queries the customer's bank to determine if his balance is adequate to accept the transaction.

3. If the balance is adequate, authorization is given, the customer's account is debited, and the transaction is transmitted through a switching facility to the merchant's bank for crediting to his account. If the balance is insufficient, the merchant's terminal is so notified.

4. After the merchant's account is credited, notification is sent to the merchant's terminal, and a sales slip is prepared for the customer.

The whole transaction is completed in a matter of seconds.

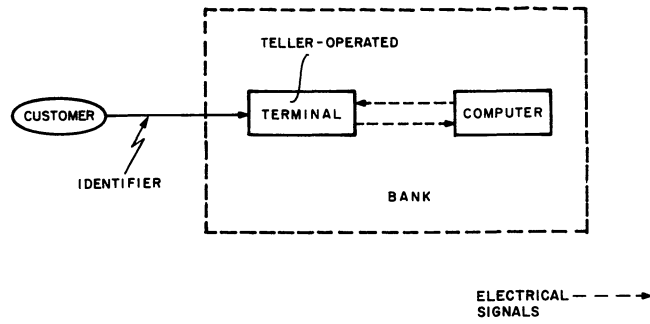
The major beneficiary from the use of point-of-sale terminals is the merchant, who saves expenses related to collection on returned checks, loss from bad checks, or loss from fraudulently used credit cards. Cash terminals protect the merchant from all but sophisticated electronic frauds since the transfer of funds is accomplished while the customer is on the premises. Electronic fraud is addressed in Section V. An additional benefit is provided by the cash terminal system since the merchant receives the funds immediately. The validation terminal provides little apparent benefit to the customer; in fact it could be argued that he suffers a detriment through privacy invasion and increased time required to consummate a purchase. The cash terminal system includes all of the disadvantages previously ascribed to the preauthorized debit system but does provide a degree of convenience to the customer. The bank gains a benefit from validation systems only in a reduction of returned check and bad check items. The cash terminal system benefits the bank through an increase in customers and the opportunity to provide other services to these customers. Offsetting detriments include increased costs associated with required equipments and operators

necessary to operate these systems. Tests conducted thus far have concluded that such systems are not economically feasible for a single bank to operate.¹⁷ It would seem that the economic disadvantage experienced by a single bank would be minimized in a large scale multiple bank program. These cost increases would require measurement against counterbalanced cost decreases associated with the current payments system and the gains achievable through an increase in customers before definitive conclusions could be stated.

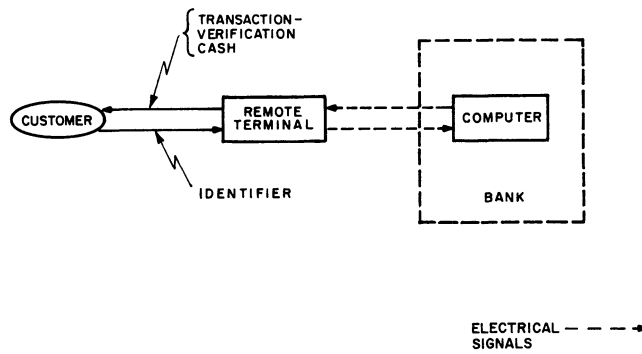
Automatic Teller Equipments

Business conducted at teller stations within a bank has until recently also been labor intensive. As the teller reaches a saturation level, efficiency suffers and customer waiting times begin to increase. One solution to this problem is to increase the number of tellers. EFT, however, offers the opportunity to change this banking function from labor intensive to capital intensive through the use of automatic teller equipments. Such equipments vary widely in capability and may operate either attended (to assist a teller to conduct transactions more rapidly) or unattended (to allow customers to conduct transactions on an around-the-clock basis). Figure 6 illustrates these two types of systems. Attended automatic teller equipments assist the teller basically through electronic verification of account status when a customer requests a withdrawal of funds. Such withdrawals may be activated by presentation of a check or a bank card, depending upon system characteristics. Deposits may be similarly accomplished. Unattended automatic teller systems, called Customer-Bank Communication Terminals (CBCT), can offer a variety of services. The least sophisticated only allow a customer to withdraw a specific amount from his account. The more sophisticated may allow cash advances, deposits, loan payments, withdrawals, and transfer of funds between savings and checking accounts. Such terminals may be installed within the bank or at any location to which appropriate communications are provided.

The primary advantage to the customer is convenience. Manned teller equipments speed up transactions, thus allowing the customer to avoid excessive waiting times in accomplishing banking transactions. The automated unmanned equipments allow access to the banking services around the clock, seven days a week. Banks benefit from such systems, by replacing manual labor with machine labor. One method of insuring sufficient volume to



6a ATTENDED



6b UNATTENDED

Figure 6 AUTOMATIC TELLER SYSTEMS

IA-47,750

warrant the investment in such equipments is for several banks to share an unmanned terminal. This can be accomplished by connecting the terminal to the banks through an appropriate switching arrangement. In at least one area of the country, merchants may rent unmanned terminals connected to central computers servicing bank cards.¹⁸ Such arrangements reduce the investment cost to the bank involved.

Legal problems have arisen lately over the use of unmanned terminals. A Federal court decision has banned two Chicago banks from operating remote terminals because such locations were considered branch banks. The terminals were determined to be in violation of the McFadden Act, which prohibits Federally chartered banks from establishing branch banks to a greater degree than state-regulated banks.¹⁹

SECTION III

ELECTRONIC FUNDS TRANSFER SYSTEM EQUIPMENT

At the heart of all EFT systems stands the digital computer. Such computers vary from general purpose machines to special purpose devices capable of only a single function. The controller may be the centroid of a large system including many computers, communications lines, and input devices in widely scattered locations or it may be contained within a desk-top instrument. Regardless of the configuration, the purpose is the same: to convert information into electrical impulses so that the information may be manipulated and transmitted rapidly. Each type of EFT system described in Section II is addressed below in terms of its component parts.

Check Truncation Systems

Check truncation systems require a computer at each bank, an Automated Clearing House (ACH), and a communications system to interconnect them. Each bank sends data to the ACH (either through hand delivery of magnetic tapes or electrical connection) containing information on all transactions initiated by the bank's customers. The ACH sorts this information by recipient bank, and retransmits the information. The receiving bank debits the customer's account, thus completing the transaction. Although a transaction could be accomplished in a matter of seconds, transmission would normally be accomplished between the close of business and the start of business the following day. Customer statements would be prepared periodically from the magnetically stored information.

Each bank utilizing check truncation will require a computer capable of connecting to an Automated Clearing House. The connection will be accomplished over telephone lines. The bank computer capability must include the following functions:

1. Conversion of information on checks--payer and payee identification information, date and amount of transaction--to electrical signals.
2. Storage of electronic signals, representing transactions, on magnetic tape.
3. Storage of identification information relevant to payee's bank.

4. Reading information from magnetic tapes.
5. Transmitting information to the communications system.
6. Preparing customer statements.

Under the "bill check" system, banks and the ACH would need the same types of equipments specified above. In addition, each participating company would require equipment to perform the following functions:

1. Preparing bills which contain machine readable entries.
2. Reading information from the payment section of returned bills.
3. Preparing magnetic tapes.
4. Transmitting information to the bank (this function may be performed manually).

The "giro" type system imposes the same requirements as does "bill check" except that functions 2 through 4 of the company's requirements are transferred to the bank.

Automatic Payroll Depositing

Automatic payroll depositing systems are in existence at the present time. Many employers send to their bank a single check and a list of employees' names, amounts and banks. The employer's bank credits employee accounts within the bank and transmits the remaining information to other employees' banks, thus completing the transaction. The bank-to-bank transfer is electronic. If the employer transmits the payroll information to his bank electronically, the system is a completely automatic payroll depositing system. Such systems are in use, and since most companies have access to computers capable of handling such transmissions, the spread of such practices poses few technical problems. Each company utilizing payroll depositing would require a computer capable of performing the following functions:

1. Preparation of magnetic tapes containing employees' names and bank account numbers, amount of net pay, and date.
2. Transmitting information to the communications system.

Preauthorized Debits

Since preauthorized debiting systems are basically only agreements between an individual and his bank, no special equipment is required to establish such systems.

Point-of-Sale Terminals (POS)

Point-of-sale terminal systems require special equipment which can access a computer immediately. Although personal identification technology offers several possibilities for establishing identity of the customer, most current point-of-sale terminals utilize plastic cards. A wide variety of point-of-sale terminals exists at this time, and the functions they perform vary among terminal types. Basic terminals (not strictly POS) are designed only for customer identification. Such terminals are used as part of check cashing services or credit sales. To establish his identity, the customer places his card into the terminal; the terminal "reads" either embossed or magnetically stored information from the card; and compares this information against information stored in its memory. If a match is made, identity of the customer is verified. The problem with this type of verification is that the card is verified rather than the customer. More advanced verification terminals utilize techniques such as personal identification numbers (PIN). PIN's are theoretically known only to the customer (who should memorize the number) and the computer (which can establish a relationship between the information on the card and the PIN). In this way, the customer, rather than the card, is identified. Still more advanced verification terminals check the credit status of the customer with either the customer's bank or a credit extending organization. The most advanced systems (truly POS) perform the following functions:

1. Identify the customer.
2. Check the customer's credit status with his bank.
3. Cause the computer at the customer's bank to transfer funds from the customer's account to the merchant's account.
4. Provide a receipt to the customer.
5. Provide inventory control information to the merchant.

All of these functions are completed in a matter of seconds while the customer is in the vendor's establishment. In these advanced

POS systems, a "payment card" replaces both the credit card and the checkbook. Some terminals operate with payment cards or passbooks. Advanced POS terminals have been used in experimental systems with a high degree of success. Such systems have been installed both in banks and merchant's locations. A fully automated POS system would include a switching facility.

Automatic Teller Equipments

Automatic teller equipments may be located anywhere customer convenience dictates. They are unmanned and therefore provide banking services around the clock, 7 days a week. To operate such a terminal, the customer establishes his identity with a card and usually some system such as a PIN to link him to the card; and initiates the transaction he wishes to make through a keyboard. Such terminals are capable of performing the following transactions:

1. Accepting funds or checks for deposit.
2. Accepting mortgage and loan payments.
3. Executing withdrawals and dispensing cash.
4. Making loans.
5. Making transfers between savings and checking accounts.

Although transactions 1 and 2 above are similar to night depository functions, the other transactions are possible because the terminal can be automatically connected to the bank's computer.

SECTION IV

PROBLEMS AFFECTING EFT

As stated in Section I, several extremely significant problems must be solved before EFT can reach its full potential. These problems include persuading all segments of the economic community (including the customer) to accept it, the planning and financing of such systems, solving of some legal questions, and developing of methods to protect EFT systems from fraud. The last topic is discussed in Section V. EFT is seen by members of the banking industry as offering two significant opportunities: increased profits and increased numbers of new accounts. Costs would be reduced through a move from labor intensive activities to capital intensive activities. However, competition among financial institutions, which the Federal Reserve Board of Governors and the Congress²⁰ seem to be encouraging, is reducing profits, thereby substantially off-setting the benefits derived from reduced costs. As a bank offers increased services, it has the potential of attracting more accounts. This was evidenced in the "Hinky-Dinky experiment" conducted in Lincoln, Nebraska in 1974. In this experiment, the First Federal Savings and Loan Assn. installed automatic teller terminals at five Hinky-Dinky supermarkets. Within 45 days, the bank had opened 650 new accounts with total deposits of \$640,000.²¹ The competitive advantage of new services for any individual bank exists only until its competition also provides such services. Thus, opportunities offered by EFTS to the financial institutions in the long run tend to benefit the customer through increased services and lower costs, while the competitive advantage gained by the financial institution disappears.

Encouraging Acceptance of EFTS

Persuading the customer to accept EFTS is not going to be an easy task. Several significant issues are involved. First, it should be recognized that a significant segment of the population, numbering "tens of millions of potential customers..."²² do not presently even use checking accounts. The Bank Marketing Association stated, in its research report A Qualitative Analysis of Why People Do Not Have Checking Accounts reports

"... their primary reasons for not having a checking account are psychological, imagined, even based on misconceptions about the mechanics of checking account usage, the rules and corrective procedures imposed by a bank, and the motives for seeking them as customers".²³

If so many people reject checking accounts for unfounded reasons, many more will hesitate to accept services which, at least for the present, contain real disadvantages as described in Section II above. A case in point is Mr. Greg Collier, a Pillsbury Company computer shift manager, who in 1975 reported that although paycheck direct deposit was offered by Pillsbury and had been accepted by a third of its 1500 eligible employees, only 2 of the 35 employees in his department had enrolled. He stated, "It could take months to unscramble something that was messed up. That shows you how much we trust computers".²⁴ Another commonly held viewpoint is that electronic banking would benefit the bank more than the customer. Such attitudes make it clear that the financial community must stress direct benefits to the customer in designing EFT systems and in "selling" them to the general public.

Acceptance by financial institutions is equally critical to the development of EFT. Although EFT systems may work on a limited scale, their full benefit can be realized only with widespread participation throughout the financial community. Such participation is necessary to allow fully automatic interbank transactions to be accomplished. These transactions require automated clearing houses and switching facilities so that any two banks can be connected together at any time. Banks have joined together in several locations throughout the Country to initiate EFT systems. In October 1972, the California Automated Clearing House (CACH) was established by several banks to speed up interbank exchanges. Where ACH associations have been established, acceptance appears to be proceeding slowly, which is quite understandable considering the changes that EFT requires. In Minneapolis, for example, "Apex", the local ACH system, has concentrated initially on encouraging electronic payroll deposits. After 1½ years of operation, approximately 10% of the area's major employers offer the service to their employees, and within these companies about 40% of the eligible workers are enrolled.²⁵ This rate of acceptance might appear to be discouragingly slow, but it should be remembered that acceptance of such a system requires substantial time, investment and expense on the part of the new participant. Time is required to hire, instruct, and train operators in the new procedures; to inform employees of the availability and benefits of the new program; to enroll applicants and to insure proper operation of the new procedures. All of these activities must be accomplished in conjunction with the conduct of normal business. The new participant must invest in capital equipment since his system must be compatible with the Automated Clearing House. New computer programs may be required to prepare payroll

information compatible with ACH requirements. Expense is incurred in retraining of operators and operating the new system. These disadvantages must be weighed against advantages known only from limited experience and therefore difficult to evaluate. If the ACH service proves to be cost effective, the rate of acceptance will improve rapidly.

Planning and Financing EFT Systems

The establishment of large scale EFT systems is an expensive and complex undertaking. Since the benefits of such systems would be shared by all participants, it stands to reason that all should share in the planning, development and implementation costs associated with such systems. Further reasons for broad participation in the early stages of such systems are the requirements for compatible, if not common, equipment and the recognition that future subscribers will be constrained by present decisions. This requirement for compatibility not only guides the system planner, it also constrains equipment manufacturers since future developments should also be compatible with the EFT system developed.

Broad-based EFT systems are organized around the Automated Clearing House (ACH). In an operational EFT system, a member bank would receive debit and credit authorizations from its customers. If the authorizations lead to transactions within the bank, appropriate actions would be taken immediately. If these authorizations affected customers' accounts in other banks, the data would be transmitted to the Automated Clearing House for retransmission to the affected banks. These transmissions could be accomplished instantly by the ACH serving as an electronic switching center, or periodically with the ACH serving as a center for gathering of data from all member banks and retransmitting the data daily or every other day, after working hours. Data on delayed transactions would be recorded at the member bank and either transmitted by telephone lines or hand carried to the ACH. The ACH would return data in the same form as received. Since most, if not all, member banks would ultimately service merchants utilizing POS terminals, the capability for instant data transmission between the bank and the ACH would be required. This same capability could be used for the transmission of delayed data, and therefore hand transporting of magnetic tapes between a bank and the ACH would be rare.

Financing of common facilities and requirements, such as the ACH and common programming, should be shared among those

utilizing these elements of the EFT system. This will present problems since all ultimate users may not be prepared to join into initial activities, new banks may be incorporated after the implementation of the EFT system, and the distribution of ACH utilization among the member banks may be unknown and changeable over time. In spite of the above recognized difficulties in the establishment of ACH's, the growth of such facilities has progressed from the formation of the California Automated Clearing House in October 1972. By 1975, the National Automated Clearing House Association (NACHA) included 7 operational ACH associations and 13 other ACH groups in various stages of organization.²⁶ A total of 35 ACH's are currently planned. Figure 7 shows their location.²⁷

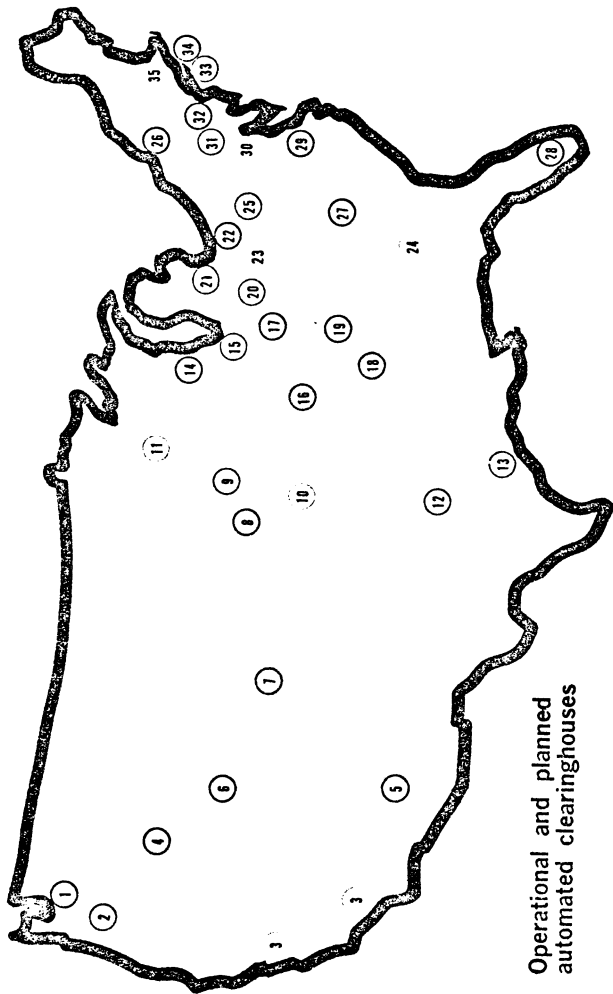
Governmental Regulation

The financial industry contains many types of institutions each with different purposes, forms, privileges, capabilities, limitations and regulatory restrictions. The institutions of primary concern here are depository institutions. Depository institutions are classified as commercial banks and thrift institutions. Normally only commercial banks may offer checking account service. They may not pay interest on these accounts. Allowable interest rates vary between commercial banks and thrift institutions. The ability of a commercial bank to operate branch offices is normally controlled by state regulations whereas thrift institution branching is Federally regulated. The industry is complex enough without EFT; with EFT, existing regulations may be inadequate, inapplicable, and capable of accomplishing little more than complete confusion. A major problem is that EFT systems eliminate most of the differences between services offered by thrift institutions and commercial banks. In an attempt to solve some of the problems created by the advent of EFTS, a National Commission on Electronic Funds Transfers was authorized in 1974, but over a year elapsed between authorization and appointment of the committee.²⁹ Fortunately, a new bill has been signed into law delaying the committee's reporting dates by a similar period. The committee held its first meeting on February 6, 1976³⁰. Regulatory problems posed by EFTS have not been solved; in fact, they are just beginning to be addressed.

Legal Questions

Many legal questions will require resolution before the future of EFT can be resolved. Because of limited experience with EFT systems, all of the legal questions may not yet be

(Source "Checking on EFTS", Computer Decision
 May 1975)



Operational and planned automated clearinghouses

- | | | | |
|--|------------------------------------|------------------------|--------------------------|
| NACHA ACHS operational by end of 1975 | 2 Portland | Non-NACHA ACHs | 5 Phoenix |
| 15 Chicago | 24 Atlanta | 4 Boise | 29 Richmond |
| 12 Dallas | 30 Baltimore | 27 Charlotte | Rochester |
| 20 Dayton | 35 Boston | 17 Cleveland | 6 Salt Lake City |
| 9 Des Moines | 23 Columbus | 34 Indianapolis | 1 Seattle |
| 21 Detroit | 10 Kansas City | 28 Long Island | Future NACHA ACHs |
| 33 New York | 3 Los Angeles/San Francisco | 14 Milwaukee | 7 Denver |
| 31 Philadelphia | 11 Minneapolis | 19 Nashville | 13 Houston |
| 25 Pittsburgh | | 32 New Jersey | 18 Memphis |
| | | 8 Omaha | 16 St. Louis |

Figure 7 Automated Clearing House Locations

known, but a substantial number have been raised. Some of these questions relate to specific aspects, others address the overall area of EFT. Some critical questions are addressed below.

1. Proof of Payment - Each of the EFT systems discussed in Section II has a problem in providing proof of payment to its customers. Checks, deposit slips, or sales receipts serve as proof of purchase in our present payments system. In the absence of these paper proofs, what will be available to demonstrate proof of payment? In many states, legal codes do not make explicit provisions for the admissibility of computer generated business records.³¹ Unless this point is clarified, EFT users may have no legal proof of payments made. This problem will be further complicated in cases involving liability for errors made either by users of the system or by the computer itself. An additional legal concern over proof of payment involves the impact of EFT upon attachment procedures.

2. System Security - In many respects, the opposite question to proof of payments involves the security of EFT systems against electronic fraud. Although system security is addressed in Section V, the legal question of liability for loss through breach of system security will require legal consideration since all elements of the system may not be under the control of a single party; exact points of transfer of responsibility may be indeterminate; and exact point of electronic intrusion may be difficult to determine.

3. Privacy - EFT systems could conceivably be abused to obtain a great deal of information about an individual--his salary, buying habits, and his location at the time of any electronic transaction. The Privacy Act of 1974 will require review in the light of the potential privacy issues raised by EFTS. At least one state has already recognized some of the problems of automated financial records of individuals. The California Right of Financial Privacy Act permits access of state and local government to such records only if disclosure is authorized by (1) customer consent, (2) administrative subpoena or summons; (3) court order; or (4) judicial subpoena.³²

4. Shared Facilities - The issue of control over EFT facilities is not at all clear. Mr. Donald Baker, an official in the Antitrust Division of the Department of Justice, has warned that the ACH's may not be used to restrict competition between commercial banks and thrift institutions. The first ACH's in California are being operated by the Federal Reserve

Board. Involvement of the "Fed" in systems utilizing point-of-sale terminals, however, may be determined to be a violation of statutory limitations which forbid this agency from dealing directly with non-banking businesses.³³ Although sharing of terminals would seem to hold promise for reducing the cost of capital equipments, the Justice Department has been reported to be concerned about such cooperation since it could lead to anti-trust suits.³⁴ On the other hand, some states have mandated that off-premises terminals must be made available for sharing.³⁵ The issue seems to rest upon whether the sharing is determined by the courts to improve or restrict the competitive environment.

In June of 1974, the Federal Home Loan Bank Board (FHLBB) adopted regulations allowing Federal Savings and Loan Associations (S&L's) to operate experimental EFT systems. This was the first instance of a Federal financial regulatory agency issuing rules in the EFTS area.³⁶ This regulation allows Federal S&L's to establish, maintain or use one or more remote terminals located anywhere in the state of its home office or within the primary service area of any branch located outside the state. A Federal S&L may share remote terminals with other financial institutions, including other Federal S&L's, commercial banks or mutual banks. In addition, the FHLBB may require sharing of the terminal with another financial institution insured by the Federal Savings & Loan Insurance Corporation whose home office or any branch office is located within the same primary service area or Standard Metropolitan Statistical Area.

5. Rights of Third Parties in Credit Transactions - If a merchant extends credit to a customer on the basis of an EFT credit check and later finds that information received from the bank was in error, what are his legal rights against the bank verifying the status of the customer? What are the customer's rights in such a case? Again the present legal framework cannot clearly resolve such issues.

6. Automatic Payroll Deposits - The Federal Government is moving deliberately toward direct deposits of payroll checks and benefit payments. The Air Force currently offers this option to employees; the Social Security Administration offers direct deposit to beneficiaries of its programs. Substantial savings are realized through such payments as opposed to check payments. To maximize savings all such payments should be made through automatic direct depositing. Can automatic direct depositing be legally required for such recipients? This question must be resolved if the full potential of EFT is to be

realized in this area. If the Federal Government is able to require automatic direct depositing, state and local governments and private industry, recognizing the cost efficiency of this payment method, will be quick to follow. Again liability for errors is a significant concern.

7. Branch Banking - As previously stated, the FHLBB has promulgated regulations with regard to remote terminals. Such terminals, if considered branch banks, would be subject to restrictions of the Federal Reserve Board with regard to branch banks. The Comptroller of the Currency has stated that remote terminals should not be considered branch banks but has limited the allowable distance between a home office and an individually operated terminal to 50 miles. He also authorized the sharing of terminals. This decision was challenged by the banking commissioner of Illinois, a state which does not allow branch banking, in a suit against Continental Illinois National Bank and Trust Company of Chicago which wanted to install a network of 125 remote terminals.³⁷ Federal District Judge Herbert L. Mills prohibited the bank from operating remote terminals, declaring them to be branch banks.³⁸ Judge Mills did, however, express his belief in EFT by encouraging the bank to seek revision of the Federal law (McFadden Act) that limits branch banking to the extent limited by state law.

The legal questions discussed herein are not intended to be an exhaustive analysis of all legal questions raised by EFT. It has been stated "the different types of legal implications that might flow from (such a system) are as varied as the many sources of legal rules out of which they might arise".³⁹ The intent here is to indicate the nature of legal issues which must be resolved before EFT can reach its full potential, or even survive.

SECTION V

SECURITY

Although technology is presently available to implement all of the types of EFT systems discussed in Section II, protecting such systems from electronic invasion and fraudulent manipulation remains a substantial problem. The problem involves security against both internal fraud and external invasion. It should also be recognized that security is an on-going concern; yesterday's problems may be solved today, but new problems will continue to surface. Potential losses to electronic theft are enormous, and as long as the potential remains high, the battles between the innovative thief and the protector will continue.

The threat of internal fraud is created by those who have legal access to the system. This includes clerical personnel in retail establishments and financial institutions, tellers, computer operators, various employees of the telephone companies providing the communications links, and the customer. The seriousness of this threat can be judged by the comparable statistics from the non-EFT environment. The Department of Commerce reported in 1974 that the estimated retail losses due to ordinary business crime (ordinary crimes include burglary, robbery, vandalism, shoplifting, employee theft, bad checks, 40 credit card fraud, and arson) would be \$5.77 billion in 1974. Of this total, employee theft would account for 13%⁴¹, or \$750 million. This figure does not include white collar crimes such as embezzlement, which was reported at \$188 million by financial institutions alone in 1975.⁴² Some internal fraud such as clerks who overcharge and pocket the overcharged amount will be favorably impacted by EFT since cash will not be readily available for pocketing. Careless use of an identification card, however, would enable clerks to make bogus charges against customer's accounts. Specific threats are addressed by system below.

The threat of external fraud is created mainly through the use of false identification. Depending upon the sophistication of the identification used, system security can be very good or very bad. The basic identification item involved in most EFT systems is the plastic card. Unless more sophisticated card systems are utilized, EFT systems will be as vulnerable to fraud as present card systems are. The Department of Commerce reported that losses from fraudulent credit cards cost banks about \$420 million in 1973.⁴³ Bad check losses, estimated to be approximately \$750 million in 1974⁴⁴, could be expected to become card losses in a "cashless" society. Therefore the

potential loss, at the 1974 rate could be in the order of \$1.2 billion unless identification cards are made more secure. Fortunately more secure identification techniques are being developed to cope with this challenge.*

Check Truncation

The major security problem in check truncation systems is internal. The possibility exists for non-existent charges to be made against a customer's account since payments made are reported to him only as debits on a monthly statement. Careful review of limited data will be required to assure the validity of all charges reported. The possibility for external fraud also exists in that a thief could send bogus payment authorizations to a bank in someone else's name, authorizing the transfer of funds to his account or to a phony account established to accept such transfers.

Automatic Payroll Depositing

The possibility of fraud in automatic payroll depositing exists primarily at the point where the magnetic tape is prepared. Payment authorizations to a dummy account could be set up for receipt of funds diverted from legitimate accounts. This tape preparation could take place at the paying company, at the paying company's bank, at the clearinghouse, or at the receiving bank. Such diversions could be discovered, but it would probably take several days for the diversion to be recognized by the payee and the system to be traced to discover the exact diversion made. By that time, an adroit criminal could have acquired the funds and disappeared. Such diversions could also be accomplished by wire tapping if the depositing is accomplished by electronic transmission.

Preauthorized Debiting

Preauthorized debiting transfers a great degree of control over financial matters from the account holder to the bank. This creates the possibility for the bank to accept bogus authorizations which would allow funds to be fraudulently siphoned

*Identification techniques are discussed in Appendix C3.

from accounts. Since account statements would probably be prepared on a monthly basis, plenty of time would be available to the criminal to accomplish the fraud and disappear before it could be discovered. The possibility exists for internal fraud both from the company which has been preauthorized and from the bank handling the account. Personnel at either location could inflate charges and divert the overcharge to dummy accounts. Such schemes could only be detected through careful checking of the bank statements by the account holder. Time delays in discovery and checking would benefit the criminal.

Point of Sale Terminals

The principal threat to POS systems is through false identification. If a false identity is accepted to such a terminal, the criminal would be able to accomplish any transaction within the capability of that terminal. Compromise of such systems could be the result of legitimate customer action. For example, a system utilizing a PIN card combination could be defeated by a customer who records his PIN either on the card itself or elsewhere within his wallet and subsequently loses the card and the wallet. Counterfeit cards also pose a significant threat. Internal threats could stem from an operator of a manned terminal who acquires identification information on legitimate customers and uses it for his own purposes. Overcharging customers and diverting the overcharged amount also constitutes a hazard specially in a part-cash part-electronic system where the diverted funds could be stolen from the cash drawer.

Automatic Teller Equipments

The threat to automatic teller equipment systems is through false identification and is similar to that described for unmanned POS terminals above.

It should be recognized that unauthorized access to EFT systems can benefit a thief in a number of ways. The most obvious way is through the transfer of money to the thief's own account. Although this method offers immediate financial reward it may not be the most profitable for the criminal. Since such transfer includes a victim, the crime may be discovered within a relatively short period of time. The theft of information rather than of money poses a problem because personal data within the EFT files also has monetary value. Such thefts could go undetected for long periods of time since

the victim's loss is not readily identifiable. As legal access to such information is further restricted by provisions of the privacy acts at both National and State levels, the value of illegally acquired information will increase, making the crime more profitable.

A third type of security problem which should concern users of EFTS is akin to industrial espionage. If a company could obtain a competitor's records of accounts receivable and accounts payable, for example, it could learn supplier identities and prices, discover proprietary secrets, time its own new product releases or special sales more advantageously, or even enter false information into these records thus completely destroying the validity of the competitor's financial records.

Again, as with Section IV, the intent of this section is not to treat exhaustively the subject of EFTS security. Rather it is to identify some of the problems inherent in EFT. A detailed analysis of card security is contained in the study "Security Aspects of Electronic Bank Card Systems" performed by the MITRE Corporation for the American Bankers Association in 1974.

SECTION VI

IMPACT OF EFTS UPON CRIMINAL USE OF FALSE IDENTIFICATION

The concern over the use of false identification in the commission of crimes was the motivational force behind the establishment of the Federal Advisory Committee on False Identification. The major types of crimes investigated by the FACFI were: drug smuggling, illegal immigration, fugitives from justice, fraud against business, and fraud against government. Of these general areas, EFTS has direct applicability to the areas of fraud against business and fraud against government. In addition to these areas of direct concern to FACFI, EFTS holds promise for reducing types of crimes involving theft of money or negotiable checks since the quantity of these items being circulated would be reduced.

Fraud Against Business

The types of frauds against business which would be directly impacted by EFTS are check fraud and credit card fraud. It obviously follows that if the number of checks being written is substantially reduced, those that are written can be subjected to closer inspection before being accepted. Automated terminals would provide cash, and POS terminals would allow direct electronic payment. These new options would allow more merchants to refuse to accept checks without fear of alienating customers. Automated depositing would remove the pressure to cash payroll checks. Therefore forgeries (which require impersonation) would be substantially reduced. The capability of EFTS to reduce credit card fraud would be directly related to the degree of security provided by the card system used.

Fraud Against Government

EFTS offers several opportunities for the government to reduce its losses due to false ID fraud. Automated depositing would eliminate loss or theft of payroll and benefit checks. It would eliminate reissue of checks claimed to be lost or stolen but subsequently cashed. It would also save the costs associated with investigation and legal actions related to such fraud. If the methods used to identify recipients of government benefits contained unique personal identifiers, security measures could also be developed to ensure against a claimant using more than one identity. This possibility would, of course, require careful consideration to avoid privacy invasion.

Overall Impact

The overall impact of EFT upon the use of false identification should be substantial. Although there will be a direct impact upon the two areas discussed above, other areas should also be favorably impacted. Improvements in identification technology will be required to protect EFT systems from fraud. These improvements will be carried over to other areas in which false identification is being used to commit crime. Criminal users of false identification will have to be more sophisticated to overcome improved system capabilities. The net result should be the commission of fewer crimes because of the greater degree of sophistication required. It would be hoped that the number of violent crimes would be reduced also because less cash would be available for theft. On the other hand, the payoff for an individual criminal act would be expected to increase if the electronic protections could be defeated.

SECTION VII

CONCLUSION

The consensus among banking industry, government, and retail industry representatives appears to be that EFT systems will be the payments systems of the future. The technology of EFT terminals is progressing rapidly; installation of such systems is also increasing. Adverse legal decisions are being appealed, regulatory agencies are restructuring their thinking to account for EFT, banks and thrift institutions are looking to EFT as a means to gain competitive advantages, and EFT customers are increasing rapidly. The opportunities available to merchants and financial institutions are indeed substantial. EFT also offers opportunities to reduce crime through the reduction of negotiable paper in circulation. Specific crimes affected include purse snatchings, muggings, robberies, burglaries, and crimes involving the use of false identification. Crimes in the latter category include check fraud and credit card fraud--crimes which presently net criminals over \$1 billion per year. Yet all is not without concern and problems. Some of these have been addressed above. There are risks involved in the utilization of EFT systems, and these risks are substantial. Conversely, the benefits to be gained are also substantial. Most attention to the benefits, however, has centered on benefits to the financial institutions. Results so far show that EFT systems do increase deposits, that new deposits are substantially greater than withdrawals, that bad check losses are reduced, and the volume of check cashing decreases.⁴⁵ Benefits to the customer need more attention. The customer needs a realistic appraisal of benefits to be gained and risks to be taken. Security of EFT systems is a very real concern and presents significant problems. It would be unrealistic to assume that EFT systems can be made invulnerable to the risks addressed above. If the risks are recognized and means are found to provide reasonable protection from these risks, EFT can realize the potential it offers and become a significant part of the future payments system.

REFERENCES

1. Kramer, Robert L. and Livingston, W. Putnam, "Cashing in on the Checkless Society", Harvard Business Review, Sept.-Oct. 1967, p 141.
2. Cox, Edwin B. and Giese, Paul E., "Now it's the 'Less-Check Society'", Harvard Business Review, Nov.-Dec. 1972, p 6.
3. Ford, William F., "Less Check, Less Cash Society", National Business, Oct. 1973, p 45.
4. Knight, Robert E., "Electronic Funds Transfer Needs Laws for Equal Bank, Thrift Rules", American Banker, June 4, 1974, p 4.
5. Walker, Gerald M., "Electronic Funds Transfer Systems", Electronics, July 24, 1975, p 80.
6. Cox, Edwin B. and Giese, Paul E., op cit, p 7.
7. Ford, William F., op cit, p 45.
8. Knight, Robert E., op cit, p 1.
9. Knight, Robert E., op cit, p 2.
10. Brooke, Phillip, "Atlanta Research Produces Advanced Electronic Funds Transfer System Plan", American Banker, Dec. 5, 1972, p 1.
11. Waage, Thomas O., "Giro Credit-Transfer Plan Could be EFTS Alternative", Bank Automation Annual, American Banker, Oct. 29, 1973, p 7.
12. Lublin, Joann S., "'Checkless' Banking is Available, but Public Sees Few Advantages", The Wall Street Journal, Nov. 18, 1975, p 1.
13. "Young Affluent Consumers Most Likely EFT Customers", Computerworld, Dec. 24, 1975, p 2.
14. Knight, Robert E., op cit, p 4.
15. Walker, Gerald M., op cit, p 83.

16. Knight, Robert E., op cit, p 4.
17. Ibid, p 4.
18. "Digits Move Fast in the Teller's Cage", Electronics, Nov. 8, 1973, p 31.
19. "Two Chicago Banks Told to Withdraw Electronic Tellers", The Wall Street Journal, Dec. 11, 1975, p 20.
20. Cox, Edwin B., and Giese, Paul E., op cit, p 10.
21. Flato, Linda, "Checking on EFTS", Computer Decision, May 1975, p 22.
22. "BMA Survey Finds Why Many Avoid Checks, Suggests Ways of Changing Their Minds", American Banker, March 1, 1972, p 1.
23. Ibid, p 1.
24. Lublin, Joann S., op cit, p 23.
25. Ibid, p 23.
26. Flato, op cit, p 22.
27. Ibid, p 25.
28. Morton, Anton S. and Ernst, Martin L., "The Social Impacts of Electronic Funds Transfer", IEEE Transactions on Communications, Vol. Com.-23, #10, Oct. 1975, p 1151.
29. "Too Little Too Late", Datamation, Dec. 1975, p 49.
30. Leavitt, Don, "Delays Frustrate Head of EFTS Commission", Computerworld, Jan. 12, 1976, p 1.
31. Fischer, L. Richard, "Legal Implication of a Cashless Society", Computer, Dec. 1973, p 23.
32. Ibid, p 23.
33. "The Quickened Pace of Electronic Banking", Business Week, Sept. 15, 1973, p 124.

34. Knight, Robert E., op cit, p 4.
35. Asher, Joe, "Bankcards", Banking-Journal of the American Bankers Association, Sept. 1975, p 30.
36. Brooke, Phillip, "FHLBB Insures Formal Rules for EFTS, First by Any Agency; ABA Raps Move", American Banker, June 28, 1974, p 1.
37. Walker, Gerald M., "Electronic Funds Transfer Systems", Electronics, July 24, 1975, p 81.
38. "Two Chicago Banks Told to Withdraw Electronic Tellers", The Wall Street Journal, Dec. 11, 1975, p 20.
39. Freed, "Some Legal Implications of the Use of Computers in the Banking Business", 19 Bus. Law. 355, 358 (1964).
40. U.S. Department of Commerce, "The Cost of Crimes Against Business", November 1974, p 17.
41. Ibid, p 18.
42. Congressional Record, September 15, 1975, p S15926-27.
43. U.S. Department of Commerce, op cit, p 4.
44. Ibid, p 18.
45. Asher, Joe, op cit, p 82.

11

APPENDIX C2

AUTOMATED IDENTIFICATION TECHNOLOGY

R.J. Ellis

**The MITRE Corporation
Bedford, Massachusetts**

May 1976

C-51

U

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
LIST OF ILLUSTRATIONS	C-54
I INTRODUCTION	C-55
II INTERACTION TYPES	C-57
Transaction	C-57
Access Control	C-58
III IDENTIFICATION TECHNIQUES	C-59
Manual Identification	C-59
Semi-automatic Identification	C-59
Automatic Identification	C-59
IV EQUIPMENT REQUIREMENTS	C-67
Manual Operation	C-67
Semi-automatic Operation	C-67
Automatic Operation	C-68
V SECURITY ASPECTS OF AUTOMATED IDENTIFICATION	C-77
Manual Identification	C-77
Semi-automatic Identification	C-78
Automatic Identification	C-79
VI APPLICABILITY TO THE FALSE IDENTIFICATION PROBLEM	C-81
VII CONCLUSIONS	C-83
REFERENCES	C-85

LIST OF ILLUSTRATIONS

<u>Figure Number</u>		<u>Page</u>
1	Interpersonal and Intrapersonal Data Variability	C-62
2	System Performance	C-64
3	Semi-Automatic Transaction System	C-69
4	Closed-Circuit TV Access Control System	C-70
5	Automatic Identity Verification	C-73

SECTION I

INTRODUCTION

The ever increasing complexity of society is creating a problem which affects us all. We are ever more frequently required to prove to others whom we do not know that we are who we claim to be. Since we are not known by all of the people with whom we interact, it is important that they know our identity (identity is defined as "the condition or fact of being some specific person..")¹. How do we identify ourselves to others? Under what circumstances should we be required to identify ourselves? Can modern technology assist in this identification process? In order to answer these questions, it is necessary to examine the ways in which we interact with each other and why it is necessary that identity be established. Two types of interactions are addressed in this paper: transactions and access control. Transactions are those situations which involve the exchange of items of value; for example, the exchange of goods or services for cash. Access control involves the controlled admission of an individual into an area which is not available to everyone; for example, the entry of a person into a secret government building. Three types of interactions will be investigated: manual, semi-automated, and automated. Manual interactions involve the use of no special equipment. Semi-automatic techniques utilize special equipment to assist in the identification process, but the decisions are made by individuals. Automated techniques involve the use of special equipment which performs the identification process, makes the decision, and completes the desired action, either the transaction or the admission, without human intervention. Characteristics of special equipment capable of performing the semi-automated and automated interactions will be examined to establish capabilities and susceptibilities to two kinds of errors:

- Type 1 - failure to recognize a legitimate identity
- Type 2 - failure to reject a false identity

Security problems associated with this special equipment will be addressed, and the effect of such equipment on the false identification problem will be explored.

SECTION II

INTERACTION TYPES

To an increasing extent, interactions in our society are becoming depersonalized. Formerly a merchant knew his customers. He not only knew their names, he also knew their families, their reputations, and their financial status. This was possible because the number of his customers was small, they came from a small geographical area, and their assets were readily visible. Recently, however, a merchant's customers have become far less well known to him. He has more customers; they are more mobile; and, therefore, come from a much larger geographical area; he has less contact with them, both as customers and neighbors; and their assets are no longer visible enough to allow evaluation of financial status. This lack of knowledge of his customers has made the extension of trust, or credit, more risky for the merchant and has increased his potential for loss. Yet, the extension of credit has become so widespread that few merchants feel that they can afford not to offer this service. Acceptance of checks poses a similar problem to the merchant since their use is so widespread. For example, the typical food store receives checks for 85% to 90% of its total sales. Although losses from bad checks cashed by food stores are reported to have exceeded \$450 million in 1974², competition almost requires provision of this service. The same loss of personal knowledge is occurring between employer and employee. As a company grows, personal recognition can no longer be used to assure the identity of employees. More rapid turnover in recent times has also contributed to the problem. Although there are many reasons why a business needs to be able to distinguish between employees and non-employees, the principal one involves protection of the property of the employer from theft. Such theft may involve merchandise, cash, or documents. In order to protect against the additional threats created by the loss of personal knowledge between the parties of an interaction, systems of identification verification must be adopted to replace personal recognition.

Transaction

A transaction has been defined as a situation which involves the exchange of items of value. The most common example of a transaction is the purchase of goods or services for cash (checks and credit cards are included since these instruments merely delay the consummation of the cash transfer).

Access Control

Access control is defined as a situation which involves admission or exclusion of a person from a specific location or area. Access control would include entry of persons into industrial or secure governmental facilities, entry of foreign nationals into the country, and entry of persons into private facilities (e.g., club houses, parking lots, safe deposit areas and boxes, etc.). Such access must be controlled to protect the rights and privileges of those who are legitimately authorized such access and of those who authorize the access, while restricting unauthorized individuals from these privileges and rights.

SECTION III

IDENTIFICATION TECHNIQUES

Adequate identification is a necessary part of any interaction. Identification may be accomplished in any of the following ways:

Manual Identification

Manual identification may be accomplished by personal recognition, visual comparison, or information comparison. The corner grocer uses personal recognition to identify most of his customers. From long association, he recognizes his customers on sight. He requires no other proof of identity. A new or unknown customer may be requested to show his driver license to establish his identity before the grocer accepts a personal check. The grocer will use visual comparison of the customer's appearance with the picture on the license. If no picture is included on the license, verification might be accomplished by comparing information on the check and license; such as name, address and signature. These are all manual identification procedures since the merchant uses no equipment to assist him.

Semi-automatic Identification

A merchant who uses equipment to assist himself in making identifications, but reserves the final decision for himself is using semi-automatic procedures. Such procedures may include document recognition, data comparison, and data retrieval. Document recognition is accomplished by a device which examines a specific characteristic of the document itself (such as thickness, size, or material). A device which reads a number from a plastic card and compares that number with information stored in its data base is using data comparison. A device which has the capability to contact a remote computer, such as one at a customer's bank, to verify the existence of an account and its current balance or the acceptability of a transaction is using data retrieval.

Automatic Identification

Devices which have the capability of accomplishing the identification function without human assistance are performing automatic identification. Such devices utilize either document recognition or data comparison or both to accomplish identification. Document recognition is accomplished as described under semi-automatic identification above. Complete reliance on this method

of accomplishing automatic identification is risky, however, since it establishes only the validity of the card and does not establish a relationship between the card and its bearer. Thus a system utilizing only document recognition would be subject to defeat by the fraudulent use of lost or stolen cards. Devices utilizing data comparison techniques seek to establish identity through the comparison of information provided by an individual with data either stored in the device or in a location accessible to the device. Data used by such devices are of two types: personal knowledge and personal characteristics. Personal knowledge data are entered into the device through a keyboard. Secret numbers or passwords are examples of such data. Devices using personal characteristics measure such attributes as weight, speech patterns, or signature characteristics.

Systems utilizing personal knowledge seem to be favored in transaction control because:

1. They are, at least at present, less expensive.
2. They require less storage of data per individual, and are therefore more applicable for systems serving large populations.
3. They are less dependent upon the manufacturer of the equipment, therefore terminals supplied by more than one manufacturer may be used in the same system.
4. Initial identification is accomplished by the use of a card similar to a credit card and therefore the systems appear to be a natural extension of current systems already familiar to a large segment of the population.

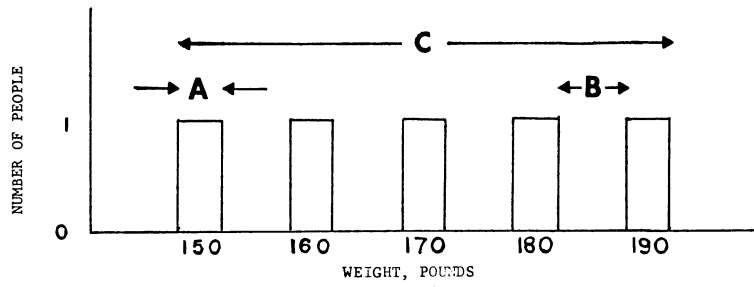
Systems utilizing personal characteristics appear to be favored in access control applications because:

1. There is no need to remember a personal characteristic.
2. Personal characteristics are far less susceptible to compromise than personal knowledge and therefore a higher degree of security can be attained.

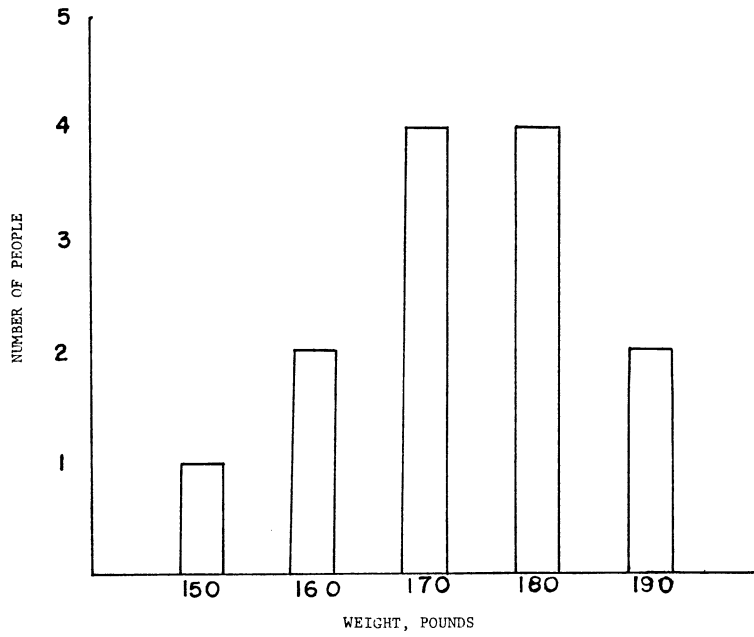
Personal knowledge systems recognize a unique code corresponding to a specific individual. Systems which measure personal characteristics, however, measure data which vary from time to time.³ This variance is called "intrapersonal measurement variability". A desirable characteristic for measurement is one

which has a small intrapersonal variation and a large interpersonal variation because data associated with such a characteristic tend to be more readily associated with a given person. Figure 1 illustrates "interpersonal" and "intrapersonal" data variability. For purposes of illustration, assume a population of 5 people whose weights are 150, 160, 170, 180, and 190 pounds respectively. If, during the course of a normal day, each person's weight fluctuates 2 pounds, centered around the specified (nominal) weight, the intrapersonal weight variability would be 2 pounds (see "a", Figure 1a). The interpersonal weight variability would be a minimum of 8 pounds (e.g., 181 to 189, see "b", Figure 1a) and a maximum of 42 pounds (e.g., 149 to 191, see "c", Figure 1a). In this sample population, weight would be an acceptable characteristic for identification because the intrapersonal variability is small compared to the interpersonal variability. This population is unrealistic because of its small size and its weight distribution. A second population is illustrated in Figure 1b. This population includes 13 people whose weights are distributed as follows: 1 at 150, 2 at 160, 4 at 170, 4 at 180, and 2 at 190 pounds. In this case, assuming the same daily weight fluctuation as stated above, the intrapersonal weight variability would still be 2 pounds and the maximum interpersonal weight variability would still be 42 pounds, but the minimum interpersonal weight variability would be 0 since there are several people who have the same nominal weight. In such a population, weight would not be an acceptable characteristic for identification. A "normal" population, of course, would contain a very large number of individuals whose nominal weights would not be concentrated at values which are multiples of 10 but would be distributed more or less continuously across the weight scale. Such a normal population would exhibit the same values of intrapersonal and interpersonal weight variability as shown in Figure 1b. In order to meet the requirement for small intrapersonal variability and large interpersonal variability, therefore, characteristics far more complex than weight are required.

When an individual is enrolled in a personal characteristic measurement system, a set of measurements is taken of each characteristic utilized. The average value of each set is calculated and stored in the system's computer memory with the individual's assigned identification number. When a person enters an identification number, the characteristics being used by the system are again measured and compared against the values stored in the computer for that identification number. Because of the variability in this data mentioned above, personal characteristic measurement systems are subject to two types of errors:



(a)



(b)

Figure 1 INTERPERSONAL AND INTRAPERSONAL DATA VARIABILITY

Type 1 - failure to recognize a legitimate identity
Type 2 - failure to reject a false identity

A type 1 error occurs when the difference between the stored value and the measured value is larger than the deviation allowed by the system design. This situation occurs because of intrapersonal measurement variability. It may be caused by the lack of due care on the part of the individual (if, for example, handwriting or voice characteristics are measured), different circumstances between the taking of the stored data and the test data (extra clothing or a carried parcel if weight is the characteristic), or by criteria which are too exacting (not enough allowance for intrapersonal measurement variability). This type of error is also known as a false alarm or an insult. A type 2 error occurs when an imposter challenges the system and is not discovered. Such an error may be caused by an imposter who knows not only how the system works but can also approximate very closely the measured characteristic of the impersonated individual (e.g., by mimicry or forgery), by criteria which are too loose, or by reliance upon a characteristic which has a small interpersonal variability. A properly designed system must consider both types of errors. Criteria which establish acceptance levels for one type of error without similarly controlling the other will not effectively solve the identification problem. Figure 2 illustrates system performance as defined by type 1 and type 2 error rates. The type 1 error rate curve is constructed by taking two measurements each from a large population of subjects and plotting the differences. It should be anticipated that the differences would be small most of the time, i.e., the intrapersonal variation is small. The type 2 error rate curve is constructed by taking a large number of measurement pairs, one each from two different subjects. This curve shows that most of the time there is a relatively large difference, i.e., the interpersonal variation is large. If a decision is made to accept all persons who demonstrate a difference of 3 or less between the measured value and the stored value, the decision will result in a type 1 error rate of 12% (12% of the time a valid identity will be rejected) and a type 2 error rate of 12% (12% of the time an imposter will be admitted). If, however, the threshold is set at 4, the type 1 error rate will be reduced to 3%; but the type 2 error rate will be increased to 22%. A single threshold value is not a desirable strategy for this reason. Normally two thresholds are established. The decision will be reached in the following manner:

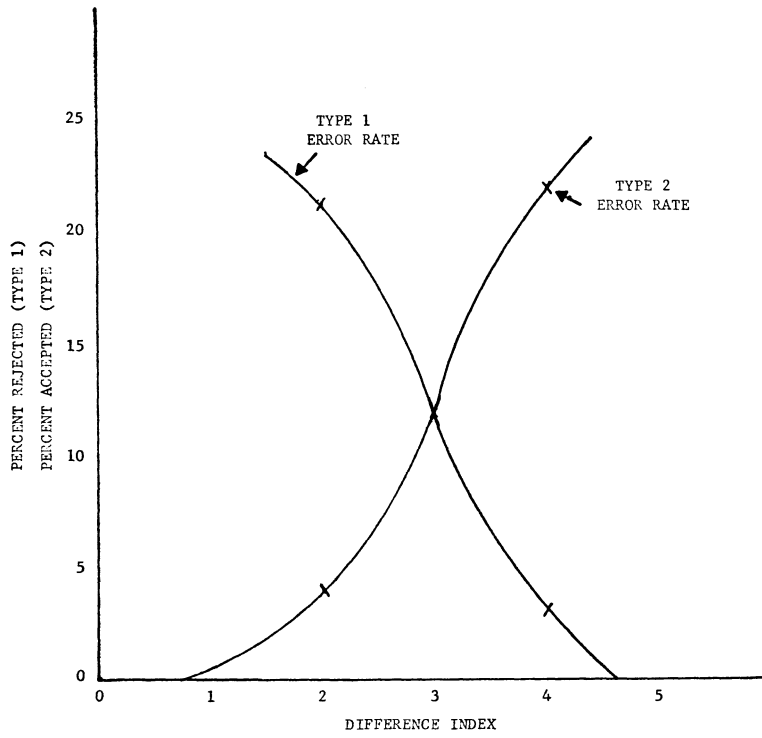


Figure 2 SYSTEM PERFORMANCE

1. If the difference is 2 or less (type 2 error rate of 4%), the applicant's identity will be assumed to be validated.
2. If the difference is 4 or greater (type 1 error rate of 3%), the applicant will be assumed to be an imposter.
3. If the difference is between 2 and 4, no decision is made on that measurement.

SECTION IV
EQUIPMENT REQUIREMENTS

This section discusses the requirements for devices which assist in or accomplish identification. Manual, semi-automatic, and automatic operation is discussed for both transactions and access control. Emphasis is on the actions accomplished by the equipment.

Manual Operation

As defined, manual identification is accomplished without the assistance of special equipment. There are, however, some devices which may be used to assist in the establishment of identity. Identification documents are examples of such devices. An example of this would be a customer identification card, which authorizes the bearer to cash checks. It could also be a driver license which contains a signature, which could be used for comparison with the signature on a check. A special case of the use of a signature is the traveler's check which requires the purchaser to sign it at the time of purchase and again when it is cashed. Manual access control may be assisted by a picture badge, which a guard compares against the physical appearance of the one seeking admission. Passports and border crossing cards are also used to assist manual access control.

Semi-automatic Operation

Semi-automatic identification utilizes equipment to assist in the identification function but leaves the decision to a person. Transactions may be assisted by terminals which allow a clerk or teller to access a computer data base to determine the status of the customer's account. Such terminals are common parts of electronic funds transfer systems (EFTS).* These terminals read plastic cards which contain the customer's account number (the number embossed on the card and recorded on a stripe of magnetic film), transmit inquiries to the computer which stores account status information (either the store's own system or that of the customer's bank), receive information back from the

*EFT Systems are discussed in Appendix C1.

computer, and display data before the clerk or teller so that the transaction may be approved. Figure 3 illustrates such a system. Semi-automatic access control normally involves the transmission of images from several entry areas to a single remotely located guard station where admission decisions are made. Images transmitted normally include a closed-circuit TV picture of a person and a picture badge, which are used by the guard to verify the identity of the person seeking admission. A separate camera covers the area immediately adjacent to the door or a "holding" area to allow the guard to ascertain how many people are seeking admission simultaneously. Although there are many types of TV assisted access control systems, a typical system might operate as follows:

1. The applicant approaches the entrance and rings a bell to alert a guard at a remote location that someone wishes to enter.
2. The guard illuminates the area and activates the closed-circuit TV camera.
3. The applicant places his identification card or badge into a terminal.
4. The applicant's image and that of his card are displayed at the guard's position, and
5. The guard decides to admit the applicant.

Figure 4 illustrates a typical closed-circuit TV access control system.

Automatic Operation

Identification which is accomplished by a device without human assistance is considered automatic. Automatic identification systems utilized in transactions normally utilize cards as part of the identification process. Such systems must perform two functions:

1. validate the card, and
2. link the card to its authorized user.

Several schemes have been devised to enable automatic equipment to distinguish between valid and counterfeit cards. These schemes are based upon the addition of special substances or printing which can be detected by an appropriate device. The

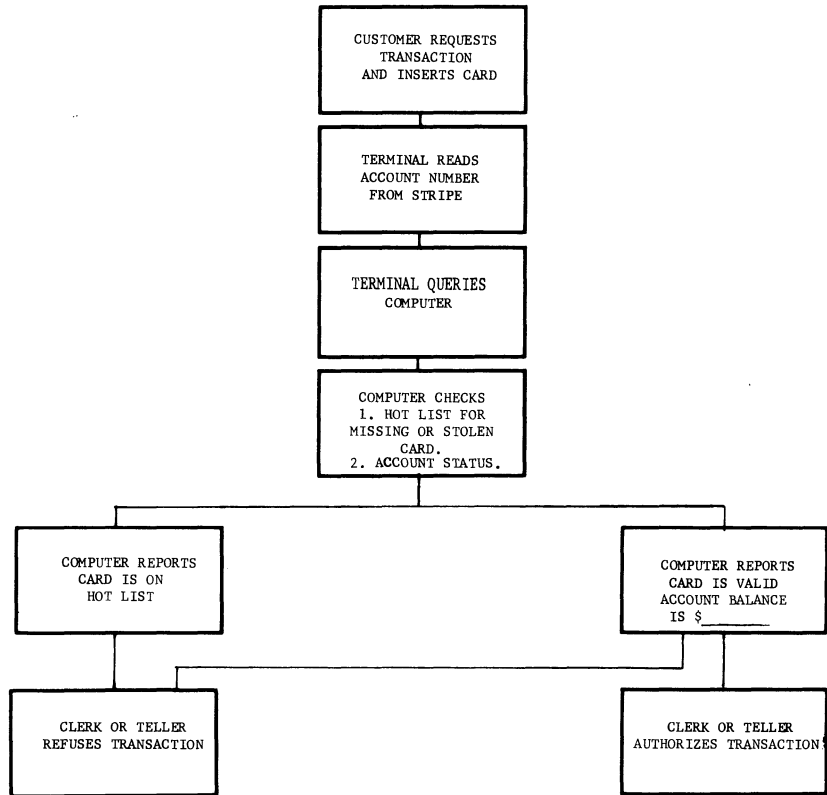


Figure 3 SEMI-AUTOMATIC TRANSACTION SYSTEM

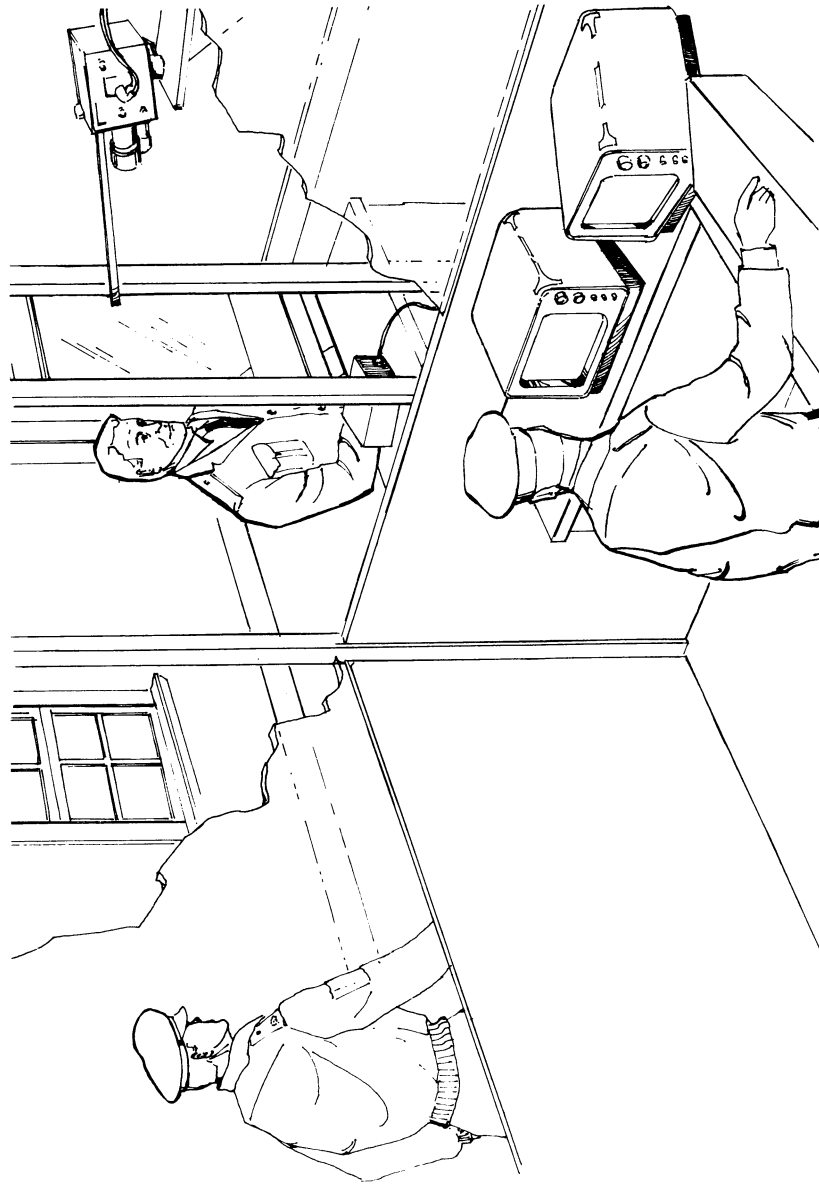


Figure 4 Closed-Circuit TV Access Control System

effectiveness of the particular scheme used is measured in terms of the difficulty required to detect and duplicate that scheme. Examples of some schemes used are discussed below.

1. Reflector implants - This technique involves the location of small infrared reflectors, or a reflectorized film containing encoded holes, in the core material of the card. The reflectors are randomly located, but their position is precisely measured. The card also contains a magnetic stripe upon which has been recorded identification information. The position of this information in relation to the reflectors is also precisely measured and encoded on the magnetic stripe. When a potential customer places this type of a card into a "reader", the following actions are accomplished:

- the information recorded on the magnetic stripe is decoded,
- the type of reflectors is ascertained,
- the distance between the reflectors and the initial bit of data stored on the magnetic stripe is measured,
- the measured distance is compared with the recorded distance,
- if the distances match, the card is accepted as valid.

In order to defeat such a technique, a counterfeiter would need to produce a card containing the appropriate holes or reflectors of the right size and position. Then he would have to record appropriate information on the magnetic stripe in exactly the same position as on the genuine card. Such a technique is relatively inexpensive to produce but extremely difficult to duplicate.⁴

2. Microcircuit implants - This technique is similar to reflector implants except that the implant consists of a tiny electrical circuit. The terminal device measures the electrical characteristics of the circuit instead of the distance mentioned above. This information is recorded on the magnetic stripe.⁵

3. Surface printing - This technique imprints a unique code upon the card. The code is then encrypted and recorded upon the magnetic stripe. The code may be a design, a series of carefully located stripes, magnetic ink, or some other characteristic. The terminal reads the recorded data,

measures the critical feature of the imprint, and compares the two to establish card validity.⁶

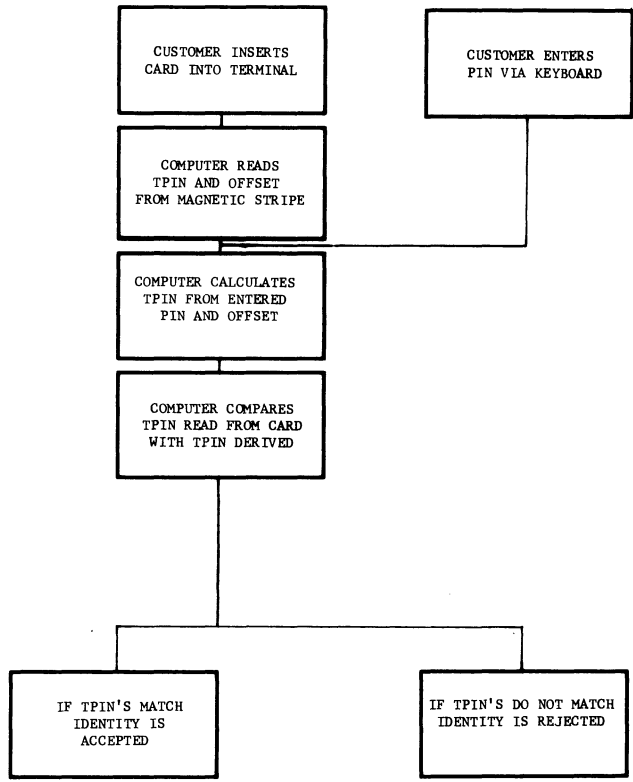
4. Other features - Other features may be used to validate a card. One such feature is physical measurement, such as the thickness of a card at a specific point. Usually such measurements would be taken over the magnetic stripe to insure that the stripe has not been covered by another layer. Radioactive substances have also been used as implants.

All of the features discussed above are designed to protect cards against counterfeiting. They do not attempt to validate the user. Features described below are designed to assure that the user of the card is the one to whom the card was issued. The most common method used to verify a card user's identity is through the use of a personal identification number (PIN). The PIN is a unique number assigned to a customer when he is issued a card. Some systems allow the customer to select his own PIN which may not be unique. In such cases, an algorithm links this PIN to another number, assigned by the system and called TPIN (true PIN) which is unique. Some systems encode and record the PIN on the magnetic stripe while other systems also store an "offset", which is a number used to relate the PIN selected by the customer to the TPIN. In order to establish his identity, a customer places his card into the terminal and enters his PIN through the terminal's keyboard or an associated entry device. The terminal:

1. Reads the information recorded on the magnetic stripe.
2. Decodes the information and determines the customer's PIN (either directly or through the offset).
3. Compares the PIN derived from the coded information with the PIN entered by the customer.

If the derived PIN and the entered PIN match, the terminal accepts the customer for the transaction of business. Figure 5 illustrates this procedure.

Access control systems could also use the type of identity verification described above. Such systems could be used to control access to parking areas or to clubhouses where the facilities are used by the members of a restricted group at non-standard hours. A reasonable degree of protection and control may be provided at a cost less than that of a guard or attendant. Where a higher degree of control is required, more sophisticated systems, which measure personal characteristics, may be required.



PIN = PERSONAL IDENTIFICATION NUMBER
 TPIN = "TRUE PIN"

Figure 5 AUTOMATIC IDENTITY VERIFICATION

The sophistication of the technique used should, for economy as well as convenience, depend upon the degree of control required. This degree of control is usually based upon the consequences of system error. It should also be recognized that the significance of errors differs not only between applications but also between type of error. For example, a higher rate of type 2 errors (failure to reject a false identity) would have less consequences for a system controlling access to a parking lot than for one controlling access to a storage facility for secret material. Similarly, a higher rate of type 1 errors (failure to recognize a legitimate identity) could be more acceptable at a manned access control station than at an unmanned one since an attendant could assist in resolving the error.

Automated access control equipment which utilize personal characteristics to establish identity operate in the following manner:

1. Measure some personal characteristic of the person seeking to be recognized (unknown person). This is usually accomplished by converting the measured characteristic to an electrical signal.
2. Compare the measured value with a reference value obtained at an earlier time from a known person (the one the unknown person claims to be). This is accomplished by taking the difference between the measured value and the stored value.
3. Decide, on the basis of the value comparison, whether the unknown person probably is, or probably is not, the known person.

This decision is based upon a set of constraints designed into the decision logic of the system. This logic usually contains two threshold values for the difference between measured and stored values. If the measured difference is less than the lower threshold value, a match is assumed and the claimed identity is accepted. If the measured difference is greater than the higher threshold value, a mismatch is assumed and the claimed identity is rejected. If the measured difference falls between the two threshold values, identity is questionable. The decision logic provides instructions to the system on the basis of decisions made. Usually an applicant is given a number of attempts to have his claimed identity accepted. If he is unsuccessful after this number of attempts (if the system rejects or questions), he is rejected and must resort to other means to be identified.⁷

Systems which utilize a characteristic which is subject to change over time usually contain the capability to update the stored value on the basis of each new set of accepted measurements. Characteristics which are currently being used in automated identification systems include: fingerprints, finger length, voice, and signature.⁸

● Fingerprints - Systems which utilize fingerprints as the personal characteristic are currently in production. The system requires the applicant to enter an identification number through a keyboard and then position his finger on a special surface where it is scanned by the terminal. The relative locations of ridge endings and ridge branches, the "minutiae" of the fingerprint, are encoded and compared against the reference file stored under the identification number entered by the applicant.⁹

● Finger length - Finger length measurement is accomplished by a terminal much like that used for the fingerprint. The applicant enters his identification number, permitting the terminal to access the stored data, and places his hand in a prescribed position on the viewing surface. The technique is reported to be receiving favorable acceptance in systems with relatively small populations, such as employees seeking admission to stock brokerage firms or students entering school cafeterias.¹⁰

● Voice - Voice measurement systems encounter a problem not present in fingerprint or finger length systems: the measurement data derived from a given speaker saying the same words two times are not identical.¹¹ Therefore, it is necessary that several speech samples of the key statements (those to be used to determine identity) be evaluated by the computer during the establishment of the file data to insure reliable comparisons during the control function. It is also necessary that the data file be refreshed with each successful use to compensate for any variation over a period of time.

● Signature - Like voice patterns, no two signatures by the same person are ever identical. In fact, two identical signatures constitute legal evidence of forgery by tracing.¹² It is also true, however, that once initiated, the act of producing one's natural signature is not a deliberate act. The actions are predetermined and are not under direct eye-to-brain-to-hand control.¹³ Again, because no two signatures are identical, the computer data file must be built up on the basis of several sets of entered data and constantly refreshed over time. Various

aspects of the signature may be utilized in the construction of the data file. For example, elapsed time to complete the signature shows striking consistency. Successive signatures of most individuals show a time deviation of less than 10 msec.¹⁴ Pressures and pen acceleration patterns exhibited during corresponding pen strokes likewise are quite consistent. Therefore, the signature provides a useful source of measurements for automated personal identification.

SECTION V

SECURITY ASPECTS OF AUTOMATED IDENTIFICATION

Thus far automated identification has been addressed from the aspect of how a person proves his identity. Although this is a valid concern of people in a complex society, another aspect of the identification problem may be of more practical, if not philosophical, concern: how does one protect himself against fraud based upon the use of false identification or imposture in his dealings with other people? The security aspects of each type of identification technique described in Section III are addressed below.

Manual Identification

In very small, static populations like the customers of the corner grocer referred to above, manual identification usually proves to be very effective. As the size of the population and its rate of turnover increases, however, manual identification (or personal recognition) becomes increasingly ineffective. A merchant might attempt to assist his employees in the identification function by supplying "courtesy cards" to his established customers. These cards are usually the first visible evidence of the establishment of a trust (credit) relationship. They also represent the first opportunity for the use of fraud through the use of false identification. It is common practice for businesses to request credentials from strangers to verify their identity. Driver licenses, social security cards, passports, company identification badges, or law enforcement credentials would appear to provide proof of identity, but all have been used to commit frauds. The American Bankers Association, recognizing the seriousness of this problem, has advised its members... "know your endorser. Be cautious with strangers. Remember--no credential is foolproof".¹⁵ Neither is personal recognition foolproof. Humans are capable of making both types of errors defined in Section I even when using personal recognition. The error rates are dependent upon such factors as length of time the individual has been known, frequency of contact, similarity of the circumstances of the contacts, consistency in clothing and personal appearance, and degree of attentiveness. Humans also suffer from a weakness unknown to machines. They are capable of being "conned". Since the probability of human error cannot be readily measured, nor can the frequency of human error be easily controlled, the identification function is being increasingly assisted by automation.

Semi-automatic Identification

Cards used in semi-automated identification systems contain magnetic stripes upon which identification information is stored. The information on this stripe can be easily read and electronically recorded on another piece of magnetic tape. The act of fraudulently obtaining information stored on the magnetic stripe of a card in this manner is called "skimming".¹⁶ There is no known way to prevent skimming. The information stored on the card is intended to be read by any of a variety of terminals; thus a card which relies solely on the information on the stripe to identify a customer is highly vulnerable to fraud. Protection is provided by linking the information on the stripe to other information, either on (or in) the card itself or memorized by the person to whom the card is issued. Other information on the card could be any of the types described in Section IV. Information memorized by the issuer would be represented by the PIN discussed previously. One of the problems inherent in the use of memorized information is that people have a tendency to mistrust their memories and record the PIN, sometimes on the card itself or elsewhere in the wallet. If the card is lost, the wallet is usually lost also, and the PIN is susceptible to compromise. Although this tendency seems to be more prevalent when the system assigns the PIN than when the customer does, PINs selected by the customer are not random and therefore offer less security than ones which are assigned. (For example, the tendency of people to choose holidays and birthdays as "secret code numbers" is well known.)

It should be recognized that a counterfeiter is not concerned with exact duplication of a card. He is interested only in producing a card which will satisfy the terminal being used. The security of a card system, then, may be evaluated in terms of the accessibility of secret codes on or in the card, the difficulty of altering information on a card or transferring the information to another card, and the cost and technological complexity involved in creating a successful counterfeit.¹⁷

In addition to the card security features discussed above, access control systems utilizing closed-circuit TV must be designed so that the indirect means of viewing the applicant for entry is not used to the benefit of the intruder. Fields of view must be large enough to insure visibility of the total area immediately adjoining the entrance. Many applications use an entry booth rather than direct access from uncontrolled space. Such booths provide greater assurance that the number of persons entering is controlled by the remotely located guard. Minimum-distortion optics and proper lighting are required to minimize

identification errors. Color is also valuable since it creates another dimension for the intruder to duplicate.

Automatic Identification

In addition to the security considerations discussed for semi-automatic identification, two additional problems are present in automatic identification. The first of these is encountered in transaction terminals having both read and write capabilities. Such systems utilize terminals which read information (e.g., account balance) from the magnetic stripe on the card to authorize a transaction (withdrawal) and then write new information (new balance) on the stripe following completion of the transaction. Stripes with special features, such as multiple tracks or response to multiple recording levels, provide a degree of security against counterfeit cards because of the difficulty of matching the read/write characteristics of the system. Cards utilizing imbedded materials or sophisticated patterns (such as those produced through holography) provide security because the methods used to produce these cards are very expensive. The second security consideration in automatic transactions is encountered in systems which transmit the information read from the card to a central computer which performs the identification function. In such systems, the communications link may be the most vulnerable part of the system since this link may be tapped, jammed, or "spoofed" with false information.

Automated access control systems utilize one of four basic concepts: a card, a memorized number, a personal characteristic, or a combination of the first three. The first two of these by themselves are group identification techniques rather than personal identification techniques. The first, the card, is representative of the type of system which would control access to a parking lot. Authorized users of the lot are issued cards which activate the entry gate. Anyone having possession of a card may use the facility. Since the risk of loss through counterfeit or use of a lost or stolen card is small, security provisions of such a system are minimal. They would probably be restricted to periodic reissue or rerecording of the cards. The second, a memorized number, is again a group identification technique. A door key is replaced by a lock which responds to a punched-in number. The same number is used by everyone. Although such a system is not subject to compromise through counterfeit or fraudulent use of a stolen or lost item, the system is easily compromised through user negligence and intruder observation. Security is provided through observation by legitimate entrants. If they

see and report an unknown individual within the secure area, and investigation shows that the system has been compromised, the number can be changed. What little security such a system provides depends upon initiative of the legitimate entrants. The third concept, personal characteristics, has several security features which are different from the two previously discussed. First, systems utilizing this concept are personalized, that is, they seek to identify a specific person; and second, error rates may be modified to suit the requirements of the application. These error rates are a function of the thresholds established, but may be further modified by allowance of multiple attempts (to reduce type 1 errors) and the measurement of two independent characteristics (to reduce type 2 errors).

This discussion has not attempted to resolve all security issues involved in automated personal identification systems. Rather it was intended only to point out that there are different types of systems which require different types of design considerations to achieve optimum performance.

It is significant to note that in a trial conducted before U. S. District Court Judge Alexander Harvey in June 1976, Bertran E. Seidlitz was convicted of stealing computer information from the Federal Energy Administration. Seidlitz was able to access the computer by punching secret passwords into a keyboard attached to his telephone, thus establishing apparent authority to access the records. As a result of his conviction of "fraud by wire", Seidlitz could be fined up to \$1000 and imprisoned for five years on each of two counts. The conviction has been called a "landmark" in legal efforts to protect computer data systems from such frauds.¹⁸

SECTION VI

APPLICABILITY TO THE FALSE IDENTIFICATION PROBLEM

The concern over the use of false identification in the commission of crimes was the motivation for the establishment of the Federal Advisory Committee on False Identification. The major types of crimes investigated by the FACFI were: drug smuggling, illegal immigration, fugitives from justice, fraud against business, and fraud against government. Automated personal identification technology can be applied to all of these areas since it provides a means for verifying an individual's identity. The type of system utilized must be based upon several considerations. Among these are:

- the degree of security required
- the frequency of use by a specific individual and by all users
- cost
- acceptability to the users of the system

Not all considerations are applicable to all systems, however. For example, the use of automated identification techniques may not be as applicable for customs utilization to reduce drug smuggling as it would be for access control to a secret facility since customs officers are required for other entry control functions. Similarly, a personal characteristics measurement system could be too time consuming for use at a busy border crossing station. Although the individual use anticipated will necessarily alter the type of identification system utilized, automated identification systems offer capabilities which can improve crime prevention efforts in all of these areas. At the same time, greater reliance upon such systems could lead to potentially greater losses. The sophistication of such systems should make them immune to defeat by all but the most clever criminals, but successful defeat, particularly in business applications, could lead to huge losses since direct access to the total assets of a business could be gained through its computer. Although this possibility must be considered, it at least presents law enforcement officials with a challenge they can address. Sophisticated identification systems can greatly reduce the number of crimes committed through the use of false identification. This will allow concentration of efforts against the limited number of criminals who are able to defeat these systems.

SECTION VII

CONCLUSIONS

The extent to which trust and credit are used within our society is constantly increasing. Their use can be broadly divided into two types of interactions between people: transactions and access control. In transactions, the extension of credit to a customer exposes a merchant to two types of risk: default by a valid debtor and default by a fraudulent debtor. Automated personal identification holds substantial promise for reducing the second type of risk. Access control also involves two types of risk; risk that the one seeking access is not who he says he is and that access is sought for illegal purposes. Automated personal identification techniques hold promise for reducing the first type of risk. The risks associated with both extension of credit and trust, therefore, may be reduced through the use of automated identification techniques.

It should not be assumed that the installation of automated personal identification equipment will eliminate the risks identified above. None of these systems is foolproof. The best techniques associated with card manufacture and coding can be reproduced or defeated. The most secure technique can be compromised. Communications links can be tapped. Transmitted data can be intercepted and modified. Personal characteristics recognition systems are subject to error. The two types of errors are interrelated. This means that if not everyone is to be rejected, it must be recognized that some unauthorized individuals will be accepted. All of the techniques discussed have merit by themselves, but greater capabilities can be achieved by combining techniques, for example, by using an anti-counterfeiting feature and a PIN in a card system, or by using two independent personal characteristics. Various degrees of security can be achieved, but the criminal element will be constantly attempting to defeat these systems because the potential for gain is high. Therefore, constant vigilance must be maintained to insure that the degree of security desired from a system is achieved.

REFERENCES

1. Webster's New World Dictionary, College Edition, 1968, p 721.
2. U.S. Department of Commerce, "Crime in Retailing", August 1975, p 6.
3. Raphael, David E. and Young, James R., "Automated Personal Identification", Report Number 539, Stanford Research Institute, December 1974, p 3.
4. Ferdman, Mauro, Letter to James Booth, ABA, dated 6/20/75, The MITRE Corporation, D72-140, p 2+.
5. Ferdman, Lambert, Snow, "Security Aspects of Bank Card Systems", The MITRE Corporation, MTR-2971, Vol. II, p 50+.
6. "New Secure Card Properties (SCP) Brochure", Burroughs Corporation, November 24, 1975.
7. Raphael and Young, op cit, p 3.
8. Ibid, p 5.
9. Muerle, J. L., et al, "EDP Security Through Positive Personal Identification", Proceedings, 1974 Carnahan and International Crime Countermeasures Conference, April 16-18, 1974, p 252.
10. Raphael and Young, op cit, p 7.
11. Bunge, E., "Automatic Speaker Recognition by Computers", Proceedings 1975 Carnahan Conference on Crime Countermeasures, May 7-9, 1975, p 24.
12. Herbst, N. M. and Liu, C. N., "Automatic Signature Verification", IBM Research Report RC 5810, November 7, 1975, p 2.
13. Ibid, p 5.
14. Ibid, p 6.
15. American Bankers Association, Identification With and Without Credentials, 1950, p 44.

REFERENCES (concluded)

16. Ferdman, Lambert, Snow, op cit, p 29.
17. Ibid, p 55.
18. Donald P. Baker, "Theft by Computer", The Washington Post, June 16, 1976, p. A1.

APPENDIX C3

**SOME COMMERCIALY AVAILABLE
IDENTIFICATION PRODUCTS**

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	C-91
I FINGERPRINT DEVICES	C-94
Curtis-Levantine and Associates: Finger-Inking and Palm-Inking Device	C-95
Indenticator Corporation: "Thumb Signature" Endorsement System	C-96
IDENTISEAL-A Division of Infra-Print, Inc.: Fingerprint Reproduction Technique	C-97
William M. Riggles, Jr.: Fingerprint Photography and Viewing Device	C-99
Veriprint Systems Corp.: Fingerprint Printer and Automatic Optical Correlator (comparator)	C-101
RCF Systems, Inc.: Electro-optical Fingerprint- Taking Device	C-103
II DOCUMENT SECURITY TECHNIQUES	C-104
American Magnetics Corporation/Bond ID Company: Magnetic Stripe Card Security System	C-105
Applied Optomechanical Kinetics: Coding and decoding of information	C-107
DEK/ELECTRO Identification Systems Division: Photo Identification Card System	C-109
IData, Incorporated: Photo Identification Card System	C-111

TABLE OF CONTENTS (concluded)

	<u>Page</u>
Identocard Limited: Optical thin-film coatings	C-113
3M Company: Transparent retro-reflective film and viewer ("3M" Brand IF-100).	C-115
N-YINGLING Associates: Imaging line and continuous tone data on presensitized metal	C-117
Optronic International, Inc.: Holographic Identification System	C-119
Ralph C. Wicker: Hidden half-tone image printing and viewing	C-120
III PERSONAL IDENTIFICATION TECHNIQUES	C-122
Alden Electronic & Impulse Recording Equipment Co., Inc.: Signature, fingerprint, photo or document transmission and reception system	C-123
International Business Machines Corporation: Automatic Signature Verification Technique	C-125
Wen C. Lin: Speech and signature computer-aided recognition and verification	C-126
Peerless Printing Company, Inc.: Signature comparison display	C-127
George H. Warfel: Dynamic Digital Signature Data in Magnetic Stripe, in central file, or partially in each	C-128
Westinghouse Electric Corporation: Speaker identification technique	C-130

INTRODUCTION

As part of its charter to "educate the public regarding steps which may be taken to reduce the criminal use of false identification,"¹ the FACFI wishes to present information on commercially available products and methods that could reduce false ID fraud. Appendices C1 and C2 were designed to provide an overview of some of the technology available. We recognize that the community or a businessman faced with increasing levels of false ID crime may well need information on specific products and their potential to solve particular problems. However, any attempt by the FACFI or its staff to produce a comprehensive list of such products would probably err by omission. Therefore, an effort was made to elicit product information from the sources themselves.

The advertisement shown as Exhibit I was placed in the Commerce Business Daily, a Federal newsletter in which government solicitations and announcements to private industry are frequently made. The item appeared on January 6, 1976. Information was requested on any product or method having a proven potential for reducing false identification fraud; respondents were asked to address such points as initial and operating costs of the system offered, probability of defeat by counterfeiting, alteration, or imposture, and the impact of the system on the public, especially with regard to convenience and privacy.

A wide variety of initial responses to this announcement was received by the Department of Justice; replies ranged from standard sales brochures to detailed analyses. The respondents themselves included a number of independent inventors and small business, as well as a few large corporations.

The responses were examined by the FACFI's technical staff (the MITRE Corporation) and rewritten in the form of condensed, standardized "information briefs". However, the staff did not analyze or comment on any claims made by the respondents. The information

1. Notice of Establishment of Federal Advisory Committee on False Identification, Federal Register, vol. 39, no. 205, p. 37516, October 22, 1974.

briefs were returned to their respective sources for amendment and public release. They have been reproduced in this Appendix with the exact wording used by each respondent in the released version of the information brief.

The responses have been grouped for the convenience of the reader into three categories: fingerprinting devices, document security techniques, and personal identification techniques. Within each category, product descriptions are listed by source in alphabetical order. Where a particular item of information was not supplied by the respondent, the product description contains the phrase "not contained in CBD (i.e., Commerce Business Daily) response".

Because of the method used to gather the information, the list of products described in this appendix represents only a sampling of commercial techniques to reduce false identification fraud. We must also stress that the product descriptions and claims are the responsibility of the individual offerors of these products. The appearance of these product descriptions in the FACFI report does not constitute endorsement of these products by the FACFI, its staff, or the Department of Justice. We have not verified any claims made on behalf of these products by their offerors, and are not responsible for the accuracy of these claims.

Exhibit I

Announcement in Commerce Business Daily*

FRAUD RESISTANT IDENTITY VERIFICATION DEVICES. The Federal Advisory Committee (FACFI) of the Dept of Justice is currently studying the problem of the criminal use of false identification and its potential impact upon government, commercial, and private sectors. As a part of this mission, FACFI is seeking source information from firms which market devices, or methods with proven potential, for reducing fraud based on counterfeiting, alteration, or imposter use of identification documents. "Identification documents" may be construed as official Federal, state, or local documents such as birth certificates, and driver's licenses, or privately issued identification such as credit and courtesy cards. Respondents should provide the following information as a minimum: —

- a) Intended use of device or method
- b) Principle of operation
- c) Initial and operating cost to user per unit or other measure
- d) Detailed estimates probability of defeat by alteration, counterfeit, imposture, or other technique
- e) Impact on public, especially with respect to privacy and convenience and
- f) Number currently in use or planned

Replies must be received not later than twenty calendar days (from the date of publication of this notice. Telephonic or telegraphic replies are not acceptable.

This is not a Request for Proposal. No other information is available at this time, and respondents will not be notified of the results of this evaluation. However, since the FACFI intends, initially, to present relevant responses with full credit to sources as part of a report to be furnished the Attorney General, all information should be suitable for public release. Those responses containing proprietary information not for public release must be so marked. (R002)

**David Muchow, Chairman
Federal Advisory Committee on
False Identification Dept. of Justice
Criminal Div., 315 - 9th St., N.W.
Washington, DC 20530**

*Issue No. PSA-6482, January 6, 1976, p. 9.

I. FINGERPRINT DEVICES

The devices and techniques described in this section are intended to transfer the impressions of one or more fingers to a document of some type. The conventional method of taking fingerprints involves rolling or pressing the fingers against an inked surface; a technician is usually required to assist the person being fingerprinted. This standard technique can serve as a basis for comparison of the methods offered here. Identification of an individual through fingerprints requires a careful comparison of prints taken at different times; this comparison usually requires the services of a skilled analyst. The products listed here do not generally overcome the need for such an analyst; the sole exception is an automatic comparator offered by Veriprint Systems Corporation.

NOTE: Product descriptions and claims made herein are the sole responsibility of the offerors. The FACFI, its staff, and the Department of Justice have not endorsed these products or verified the claims made for them.

PRODUCT INFORMATION BRIEF

- I. FIRM: Curtis-LeVantine & Associates
18225 Rancho Street
Tarzana, Calif. 91356
(213)987-1928 & 545-6320
(Allan D. LeVantine)
- II. PROFILE: Company formed as a partnership in 1972. Engaged primarily in Research & Development. Now adding manufacturing and marketing capability.
- III. TECHNIQUE OFFERED: Finger-Inking Device and Palm Inking Device
- IV. STATUS: Operational--in manufacture. In use at the Santa Monica Police Dept. Has been displayed at technical conferences.
- V. APPLICATION: "This unit would be a beneficial adjunct to any system that uses fingerprints as a means of identification."
- VI. HOW USED: This technique is offered as the inking method to complement an unpostulated total system. Inking is accomplished by simply pressing the finger onto the cushion. A uniform coat of ink is applied. The resultant rolled print has an amazing high-contrast quality not normally obtained by standard inking methods. Makes palm prints also.
- VII. COST: Initial: The Print-Master costs \$295.00
Operational: Dependent upon operational system. "It is economical in its spartan use of ink."
- VIII. PROBABILITY OF DEFEAT: Dependent upon postulated entire system for which this technique is offered to complement.
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: Dependent upon postulated entire system.
Convenience: Dependent upon postulated entire system.
- X. PRINCIPLE OF OPERATION: Electrically operated device automatically coats a foam supported elastic surfaced cushion with a uniform film of ink.
- XI. UNIQUE FEATURES: "A new method of applying ink to the fingers produces exceptional quality prints every time."

PRODUCT INFORMATION BRIEF

- I. FIRM: Identicator Corporation
The Hearst Building
Market Street at Third
San Francisco, Calif. 94103
(Oscar R. Pieper)
- II. PROFILE: Not contained in CBD response
- III. TECHNIQUE OFFERED: "Thumb Signature" Endorsement System
- IV. STATUS: System fully developed and available. Approximately 9000 systems in operation. Majority of present systems installed in banks and other financial institutions.
- V. APPLICATION: Recording customer thumbprints on checks and other documents.
- VI. HOW USED: As deterrent to fraud
- VII. COST: Initial: Not contained in CBD response
Operational: Less than one cent per impression.
- VIII. PROBABILITY OF DEFEAT: Not contained in CBD response
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: Customer required to "endorse" check with thumbprint before acceptance by user of system.
Convenience: System is inkless and requires less than 10 seconds for recording of print. User of system may choose to substitute thumbprint for slower ID checks.
- X. PRINCIPLE OF OPERATION: Proprietary device develops visible print from natural skin oils and moisture.
- XI. UNIQUE FEATURES: Patented developing process requires no ink or chemicals to be applied to customer's skin.

PRODUCT INFORMATION BRIEF

- I. FIRM: IDENTISEAL - A Division of Infra-Print, Inc.
1212 Home Savings Bldg.
1006 Grand Avenue
Kansas City, MO 64106
(816)471-5252
(Jay N. Gutelius)
- II. PROFILE: Not contained in CBD response
- III. TECHNIQUE OFFERED: Fingerprint Reproduction
- IV. STATUS: Operational--"Millions of Identiseals have been used by all types of businesses..." Providing service for over 4 years. Used by Tennessee in selective counties to reduce food stamp fraud. Bureau of Prisons application.
- V. APPLICATION: Check cashing, legal documents, securities, credit applications, policies, safety deposit box records, notes, credit cards for use in supermarkets, motels and hotels, banks and financial institutions, auto and airplane leasing, equipment rentals, drug and liquor stores, department and discount stores, and many others.
- VI. HOW USED: At the time of desired identification, a transaction fingerprint is registered on an Identiseal tab which is affixed to the appropriate document. This requires person to only touch "pad" and then Identiseal "tab". Print then develops. Actual verification depends upon comparisons by Identiseal operating personnel. Additional assistance in tracing criminal actions can be provided by the Identiseal Secure Center where prints are compared with a data bank of stored prints from fraudulent documents. Center supplies prints and fraudulent document data to local and national law enforcement agencies.
- VII. COST: Initial: Identiseals cost three to five cents each. Pads fifteen cents each. (Good for use on 500 Identiseals.)
Operational: Dependent upon operational system.
- VIII. PROBABILITY OF DEFEAT: Alteration
Counterfeit
Impostor
Dependent upon postulated entire system. "Identiseal is a positive legal identification system..." Not specifically addressed in CBD response.

- IX. IMPACT ON PUBLIC: Privacy: "Millions of Identiseals have been used by all types of businesses with virtually no adverse customer reaction. Customer soon understands that an Identiseal endorsement stops forgers from stealing their money and damaging their credit."
- Convenience: "Customers like the 'touch and go' system because it means fast checkout with virtually no fuss or delay."
- X. PRINCIPLE OF OPERATION: The Identiseal tab contains one "chemical". A pad contains a second colorless, odorless, non-toxic "chemical". When the finger is first pressed on the pad and then onto the Identiseal tab this causes the "chemicals" to interact to produce a dark area in those places where contact is made--thus creating a fingerprint.
- XI. UNIQUE FEATURES: Psychologically powerful in deterring attempted crime by requiring individuals to identify themselves, by fingerprint, at the point of a transaction. The Identiseal system is especially designed to give maximum protection with minimum effort. "... without the use of complicated, expensive equipment."

PRODUCT INFORMATION BRIEF

- I. FIRM: William M. Riggles, Jr.
7400 Miami Lakes Drive, West
Apt. 107D
Miami Lakes, Florida 33014
- II. PROFILE: 18 years research in fingerprint impressions including dermatoglyphic program with Univ. of Miami Medical School.
- III. TECHNIQUE OFFERED: Fingerprint photography and viewing device.
- IV. STATUS: One fully developed model exists and some number of viewers have been manufactured (to study birth defects of infants based upon hand prints).
- V. APPLICATION: Personal identification for check cashing and credit card and auto license verification. Retail sales and access to secured areas. Increases efficiency of ID card production where both photo and fingerprint are included. Obtaining prints of newborns and criminal suspects.
- VI. HOW USED: At time of desired identification, a transaction print is obtained by placing thumb on prism and depressing. This causes print to be viewable and allows for photographically recording print, face of identified individual, and transaction document (check, ID card, etc.). Actual verification depends upon comparisons by operational personnel. Additional assistance in tracing criminal actions can be accomplished from photographic record.
- VII. COST: Initial: Viewing device could be produced for about \$100.00; combined photo recording/viewing model for about \$650.00 and up (depending on camera).
Operational: Not contained in CBD response. (Dependent upon total operational system.)
- VIII. PROBABILITY OF DEFEAT: Dependent upon postulated entire system. "As far as we have determined in six years, if the viewer checks the print through the viewing portion, there is no way to defeat its intended use."
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: "... very little public resentment to invasion of privacy after explaining that non-violator's prints would not be disclosed and would be destroyed after a period of time."
Convenience: Not contained in CBD response but would appear to minimize personal inconvenience in that it should be quick and simple.

- X. PRINCIPLE OF OPERATION: The device works with a dark image prism. When the finger is placed on top of the device, the ridges interrupt the surface and are illuminated by side light projecting a negative fingerprint image of sufficient contrast to the viewer and/or camera.
- XI. UNIQUE FEATURES: Provides means for viewing fingerprint at time of photograph to assure print is usable and not camouflaged. Simultaneous photographic record of print, document (check) and face. Psychologically powerful in deterring attempted crime by virtue of requiring print at time of transaction.

PRODUCT INFORMATION BRIEF

- I. FIRM: Veriprint Systems Corp.
20747 Dearborn Street
Chatsworth, Calif. 91311
(213)789-6476
(Louis B. Meadows)
- II. PROFILE: Corporation with distributors throughout the nation.
- III. TECHNIQUE OFFERED: Fingerprint Printer and Automatic Optical Correlator (comparator).
- IV. STATUS: Operational--Extensively field tested. Starting a production manufacturing operation. Developing a central file for reference prints.
- V. APPLICATION: Controlled access to security environments. Confirmation of identification for credit card and check cashing. Transportation and warehousing. Drug Control. Law Enforcement. Other high risk industrial, institutional and governmental security environments.
- VI. HOW USED: At time of desired identification, a transaction fingerprint is registered on appropriate document. Registered print is then developed using either Veriprint 1 or 10 desk top unit. A master or file fingerprint, such as obtained from a standard identification card, data processing card, etc., is used in the desk top Vericom to provide an automatic comparison with the transaction print within four seconds. Identification is confirmed or not confirmed as indicated by green or red lights, and the transaction can be completed or rejected. In the future, Vericom terminals may be electronically linked to a central file to aid in the verification process.
- VII. COST: Initial: Veriprint 1 machine costs \$125.00. Vericom unit is \$5770.00. Modified to accept Alien ID cards.
Operational: Dependent upon operational system. "... less than a cent to Veriprint." "... little other costs involved..." for Vericom.
- VIII. PROBABILITY OF DEFEAT: Dependent upon postulated entire system. "Vericom is virtually error free on legible fingerprints. More simply-- Vericom provides a foolproof personal identification system." "... Veriprint 1 fingerprints are smudge and smear proof and the fingerprint is an identification that is always carried with a person and cannot be altered to match another person's print." "... Vericom has been shown to be statistically better than 99% correct in making a print match identification."
- Alteration
Counterfeit
Imposture

- IX. IMPACT ON PUBLIC: Privacy: "... the taking of a fingerprint does not appear to be a normal invasion of privacy."
Convenience: Appears quick and simple. "The Vericomp identification system imposes no inconvenience to the public. The inkless system for taking fingerprints leaves no perceptible or harmful residue on the fingers."
- X. PRINCIPLE OF OPERATION: Printing uses an exclusive non-ink process that dries on contact together with desk top Veriprint to produce print. Smudge and smear proof. Desk top Veriprint is a unique and ingenious combination of physical and graphic reproduction. Correlation is accomplished by Vericomp which employs a unique electro-optical scanning correlation technique. Correlation is indicated automatically by colored lights.
- XI. UNIQUE FEATURES: Quick and economical method of providing positive, accurate fingerprint comparison and verification. Psychologically powerful in deterring attempted crime by requiring individuals to identify themselves, by fingerprint, at the point of a transaction.

PRODUCT INFORMATION BRIEF

- I. FIRM: RCF Systems, Inc.
429 Los Miradores
Redondo Beach, Calif. 90277
(213)378-0704
(Randall C. Fowler)
- II. PROFILE: Not given in CBD response
- III. TECHNIQUE OFFERED: Electro-optical Fingerprint-Taking Device
- IV. STATUS: Working prototype units have been constructed and tested.
- V. APPLICATION: Collection of fingerprints for law enforcement or commercial applications.
- VI. HOW USED: Portable equipment that produces instant copies of fingerprints without ink.
- VII. COST: Initial: Not given in CBD response
Operational: Not given in CBD response
- VIII. PROBABILITY OF DEFEAT: Believed low, but no detailed figures available.
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: Personal verification requires comparison of fingerprints with those on document or in computer file.
Convenience: Print-taking requires holding finger stationary for less than 1 second.
- X. PRINCIPLE OF OPERATION: Optical projection of fingerprint is intercepted by an intermediate surface and transferred to a standard fingerprint card or other document using plain paper copier technology.
- XI. UNIQUE FEATURES: No ink or other liquids applied to finger. Device produces "rolled" prints from stationary finger.

II. DOCUMENT SECURITY TECHNIQUES

The devices and techniques described in this section are intended to secure identification cards or other documents against counterfeit and alteration. In general, these techniques cannot guarantee that the documents so secured cannot be used by an imposter. However, some of the techniques described provide for the use of photographs, personalized code words, or other data that could be used to verify that the person using the document is authorized to do so.

NOTE: Product descriptions and claims made herein are the sole responsibility of the offerors. The FACFI, its staff, and the Department of Justice have not endorsed these products or verified the claims made for them.

PRODUCT INFORMATION BRIEF

- I. FIRM: American Magnetics Corporation/Bond ID Company
2424 West Carson Street
Torrance, Calif. 90501
(213)775-8651
(Glen G. Magnuson)
- II. PROFILE: American Magnetics Corporation is a leading supplier of Digital Magnetic Heads in the United States. They also manufacture magnetic stripe card readers.
- III. TECHNIQUE OFFERED: Magnetic Stripe Card Security System
- IV. STATUS: Working prototypes of AMS Card Reader; feasibility model of Bond ID equipment. Patent proceedings initiated on AMS reader.
- V. APPLICATION: Validation of card and cardholder in financial transaction and security systems.
- VI. HOW USED: As part of credit, cash dispensing, automatic teller systems, or security access systems. In general, Bond ID and AMS Card Reader requires access to central data file of such systems. However, both can be used in combination in a stand-alone terminal--access to a central data file is not necessarily required.
- VII. COST: Initial: Estimated as less than \$250.00 per terminal for both AMS and Bond ID equipment.
Operational: Line charges for access to central data base, if required.
- VIII. PROBABILITY OF DEFEAT: "Virtually non-existent" for alterations and counterfeit. Bond ID "secret number" could be compromised by customer carelessness and subsequently used by imposter using customer's card.
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: "No such effect."
Convenience: Customer required to memorize "secret word" (PIN) and key in same at each transaction. AMS system contains safeguards against false rejection of legitimate card.
- X. PRINCIPLE OF OPERATION: AMS system verifies card by simultaneous reading of embossed account number and magnetic stripe data on standard credit card and by developing security code based on relative distance between embossed and magnetic data. Bond ID system verifies customer by computing unique "offset number" derived from account number and customer-selected "secret word" (PIN).

XI. UNIQUE FEATURES: AMS system can be used with any existing credit card that contains both embossed and magnetic data; Bond ID system derives "offset number" through proprietary algorithm.

PRODUCT INFORMATION BRIEF

- I. FIRM: Applied Optomechanical Kinetics
Box 71
Stow, Mass. 01775
(617)562-9870
(Alfred O. Kuhnel)
- II. PROFILE: Design engineers and builders of mechanical, hydraulic, electronic and optical systems; supported by a photographic and reproduction group for the special coding and decoding work and elements.
- III. TECHNIQUE OFFERED: Coding and decoding of information by use of simple masking patterns and lenses.
- IV. STATUS: Patent exists and coded and decoding elements have been produced that demonstrate the use and security.
- V. APPLICATION: Whenever printed information is used such as credit cards, drivers licenses, bank-books, travelers checks, and credit cards that require fully camouflaged coded or uncoded information not visible to the eye.
- VI. HOW USED: A laminated film with an opaque masking pattern is applied via adhesive to credential. Printed (or written) information is placed on credential. A transparent lenticular decoding sheet, matched to the masking pattern, is used for viewing the coded information. If repetitive information is to be mass applied then a photographic plate can be prepared and normal printing techniques used.
- VII. COST: Initial: Low cost comparable with that involved in credit card or credential production.
Operational: Once the credential and decoding optical plastic reader has been produced, there is no operational cost in use except replacement of worn out credentials or plastic readers.
- VIII. PROBABILITY OF DEFEAT: Any attempt to alter the encoded information will destroy the area being modified and render the attempt immediately detectable. Counterfeiting is not possible unless access has been gained to the original production equipment and the records system of the facility issuing the credentials.
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: Complete since the only person involved in encoding and removing the cover material can be the user for written or self printed information.

Convenience: "This invention provides a very simple and practical means for the solution..." "... does not require special lighting." (1) No special lighting required.
(2) Hand written encoding by means of a ball point pen.
(3) Self typed information can be applied by typewriters that can accept stiff materials.

- X. PRINCIPLE OF OPERATION: Writing, removing cover mask and readout are the three steps in the process. Conventional writing or printing is used. Material containing opaque masking lines with or without camouflaging means has previously been applied. An optical decoding plate allows viewing of the writing or printing by placing the cylindrical lens elements parallel with the opaque masking lines.
- XI. UNIQUE FEATURES: Photograph of a card holder is not necessary but can be added at extra cost for security. This technique permits readout in any readily available visible light. Descriptor information can be written along with a signature.
- Electro-optical sensor heads can be applied for decoding and reading in systems requiring interfacing with magnetic tapes or digital computers.

PRODUCT INFORMATION BRIEF

- I. FIRM: DEK/ELECTRO
Identification Systems Division
The Scott & Fetzer Company
1530 Progress Road
Fort Wayne, Indiana 46808
(219)484-8611
(William E. Barager)
- II. PROFILE: World producer of photo identification equipment and credentials (cards). Offers design, development, implementation and operational services.
- III. TECHNIQUE OFFERED: Photo Identification Card System
- IV. STATUS: Operational--largest single producer of color photo drivers licenses in the United States.
- V. APPLICATION: Wherever ID cards may be used--drivers licenses, banks, security access control, etc.
- VI. HOW USED: Identification and user information data obtained through subject application. Data is placed on card and verified by subject. Subject is then seated in a DEK/ELECTRO identification photography system, such as the System 10, a photograph taken, and the system then automatically produces the card. The card is finished and provided to subject. Film negative of card becomes permanent record for re-issue or law enforcement purposes. "Security plate" may be used to photographically place all validations and security data unique to a program on the I.D. card. Verification is accomplished visually and for special purposes by aids such as a Detectron manufactured by DEK/ELECTRO Systems, Inc.
- VII. COST: Initial: Initial costs vary in relation to system employed--central issue or over-the-counter.
- Central Issue: Cameras are capitalized at \$2,500 per camera plus construction of a central processing laboratory. Basic equipment costs for a central processing laboratory approximately \$150,000. Total initial cost includes laboratory processing and fabrication equipment such as film processors, paper processors, lamination plus the number of cameras utilized in the field.
- Over-the-Counter: The basic System 10 retails for \$7,500. These are installed in high volume locations. The Mini 10, which is transportable, is \$3,995 and is installed in low volume locations or employed by travel teams. The photo

print configurations are identical. A small central office and maintenance facility is required and costs approximately \$25,000 to establish. This includes necessary spare parts and chemical mixing equipment.

Operational:

Central Issue: On-going costs are predicated on the volume of cards being produced annually which establishes the level of manpower required to maintain the facility, provide camera maintenance and fabricate the cards. The facility can be operated by as few as two or three people and as many as six or more. The annual volume and degree of sophistication of the card are the major determinants.

Over-the-Counter: Operational costs vary directly with the number of camera units in the field and the geography of the area. The number of service and maintenance personnel can be as few as one or two in a relatively small area to four or five in a state as large as Florida with a requirement to service and maintain in excess of 100 units.

- VIII. PROBABILITY OF DEFEAT:
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC:
- X. PRINCIPLE OF OPERATION:
- XI. UNIQUE FEATURES:
- Need to postulate an entire system (including verification technique(s)). "... card is virtually impossible to alter without detection." "Card validation and security markings are applied by special techniques that prevent the making of valid I.D. cards by unauthorized persons."
- Privacy: In general, no objection by the public. Data on file is only a photographic duplication of that which is already in the data base plus the portrait of the individual. Only utilized upon request of competent authority at state or federal level.
- Convenience: Quite often sought by the general public because of ease of identification for check cashing, credit card utilization and general identification usage.
- Photographic system. Card validation and security markings are applied by special techniques. Equipment and materials utilized in the DEK/ELECTRO System are not available to the general consumer market. DEK-A-CHROME, the color print material, is exclusive to DEK/ELECTRO and not available through consumer outlets. Special security markings can be applied to aid in verification (interface with 3M to produce a color photo identification card with their IF-100 security material). Positive I.D. enhanced and assured dependent upon wide range of verification options employed by user.
- Nearly automatic system produces a secure card.

PRODUCT INFORMATION BRIEF

- I. FIRM: IData, Incorporated U. S. Licensee of
1120 Goffle Road AB ID-Kort
Hawthorne, N.J. 07506 Stockholm, Sweden
(201)423-3335
(Bernard Van Emden)
- II. PROFILE: Designer and manufacturer of photo identification credentials
(cards) and verification aids. Offers design, development,
implementation and operational services.
- III. TECHNIQUE OFFERED: Photo Identification Card System
- IV. STATUS: Operational--over seven million cards (2200 types) in use
in 49 states and internationally.
- V. APPLICATION: Drivers licenses; Bank, Police, Public Official, Disaster
Service, Utility Service, Armored Delivery, Medical,
Transit and Airport Identification, Security Access Control;
etc.
- VI. HOW USED: Identification and user information data obtained through
sponsor application. Data is verified and the credential
(card) is then manufactured and finished by IData.
Finished card then delivered to applicant or to sponsor
organization.
- VII. COST: Initial: Credential (card) manufacture ranges from \$0.30
to \$3.00 per document. Single purpose verification aid
runs from \$2.00 to \$250.00
Operational: Dependent on wide range of operational
systems--credential should be replaced every 5/10 years.
- VIII. PROBABILITY OF DEFEAT: No known successful counterfeit. Need to postulate an
entire system (including verification technique(s)).
Alteration Identification confidence may range from 10% to close to
Counterfeit 100%.
Imposture
- IX. IMPACT ON PUBLIC: Privacy: "... any identification system in the U.S. will be
immediately suspect..."
Convenience: "... have minimized the personal inconvenience
by allowing maximum individual flexibility..."

- X. PRINCIPLE OF OPERATION: Identification credential (card) is difficult to counterfeit or alter because it is made of unique scarce material (special paper, special markings, coating, etc.), manufactured by scarce and expensive machines using special technologies. Card is easily recognized, uniform and distinctive. Positive identification is thus enhanced and further assured dependent upon wide verification options employed by user.

- XI. UNIQUE FEATURES: High forgery resistance (highly resistant to alteration and counterfeiting).

PRODUCT INFORMATION BRIEF

- I. FIRM: Identocard Limited
12-16 Berryman Street
Toronto, Ontario M5R 1M6
(416)962-1134
(J. C. Tait)
- II. PROFILE: Identocard is engaged in manufacturing photo identification and security systems. The Company has been in business since 1968 and has offices in Spain and Mexico.
- III. TECHNIQUE OFFERED: Optical thin-film coatings.
- IV. STATUS: Prototype machine is now under construction. Full production will be in 12 to 14 months.
- V. APPLICATION: Passports, bank notes, credit cards, passes, etc.
- VI. HOW USED: Identification document assembled in usual manner. Special coating is then applied to the document. Verification is aided by unique colors, etc. visible at different viewing angles.
- VII. COST: Initial: Cost of full production machine and ancillary equipment.
Operational: Projected costs without custom seals, logos, etc., \$1.00 per sq. ft.
- VIII. PROBABILITY OF DEFEAT: Dependent upon postulated entire system. "... almost impossible to forge successfully." "The system permits rapid detection of counterfeit attempts."
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: Since coating is visible to public, there is no hidden code that would threaten privacy. Would seemingly have negligible impact.
Convenience: Without additional readers card can be verified by the man in the street. Coatings can be customized with seals, etc. Color change can be predetermined to one of green, blue or red.
- X. PRINCIPLE OF OPERATION: Identification document is coated with a number of thin layers of rather common materials, such as zinc sulfide, cryolite, and aluminum. When these coatings are viewed from different angles, the color of the light reflected or transmitted by them is seen to change. Colors differ

essentially from all known types of dyes, inks, pigments and paints. Special materials and processes are beyond the means and capabilities of most counterfeiters. Resulting document is easily recognized and distinctive.

XI. UNIQUE FEATURES: Could be used while keeping present document forms.

PRODUCT INFORMATION BRIEF

- I. FIRM: 3M Company
Safety Systems Division
3M Center
St. Paul, Minnesota 55101
(612) 733-1110
(R.J. LaValle)
- II. PROFILE: Large company with design, development, and manufacturing capability in diverse areas.
- III. TECHNIQUE OFFERED: Transparent retro-reflective film and viewer ("3M" Brand IF-100).
- IV. STATUS: Operational - in use for almost four years. Approximately 18,000,000 drivers licenses and non-driver I.D. cards in Calif. Other markets contacted at the Federal and state level.
- V. APPLICATION: Personal identification document, birth or death certification, driver license, deed, passport, credit card, stock certificate or other important document, depending on substrate.
- VI. HOW USED: Identification and user information obtained in standard manner and placed on identification document. Retro-reflective transparent film is then laminated to face of document. When document is viewed through a compatible viewer, indications of alterations become visible by viewing the hidden, continuous legend pattern.
- VII. COST: Initial: Quotations based on information from St. Paul.

Operational: Cost will vary according to volume, size of document, etc.
- VIII. PROBABILITY OF DEFEAT: Need to postulate an entire system. "...counterfeiting capabilities to duplicate this material would be almost non-existent". "In almost four years of use in the State of California there have been no known instances where an exact duplicate has ever been passed." "...Verification of documents is the key..." "To the best of our knowledge no product has ever gotten into the hands of unauthorized personnel."

- IX. IMPACT ON PUBLIC: Privacy: "Since no fingerprint is required, no interrogation of the document holder need be made, nor any additional photograph taken, we do not feel that we are impinging on the privacy of the individual possessing the document in question."
- Convenience: "We feel that the economic benefits of the use of our system of document security will not be an inconvenience to the public." "To a quickly trained person, the verification of a secured document will be quick and efficient."
- X. PRINCIPLE OF OPERATION: The application of IF-100 document security film to a document protects against alteration by the use of an optical system. After application, the material provides a bright reflex-reflecting legend when viewed through a compatible viewer, hidden from normal vision, designed to user specifications, unique to each user. The material shows some shift in specular and reflex-reflecting color. This shift may aid in detecting alterations. Production of film is highly complex and conducted under rigid security procedures.
- XI. UNIQUE FEATURES: Secure document produced using standard techniques.

PRODUCT INFORMATION BRIEF

- I. FIRM: N-YINGLING Associates
4430 Willow Run Drive
Dayton, Ohio 45430
(513)429-0544
Neil P. Yingling, Sr. Associate
- II. PROFILE: Small team of consulting-engineering associates
- III. TECHNIQUE OFFERED: Imaging line and continuous tone data on presensitized metal of pliable characteristics.
- IV. STATUS: Pre-pilot technique development test program
- V. APPLICATION: Drivers licenses, I.D. cards, birth certificates, diplomas, credit cards, etc., i.e., any item or data that is "imaged" or from any article that can be photographically reproduced.
- VI. HOW USED: User identification data, photography, signature, fingerprint, etc., placed on a unique presensitized type of material which would effect a permanent, non-alterable record of identification. Any information that may be photographically reproduced may be emplaced on the permanent I.D. "plate". Any attempt to alter this flexible metal-card which could only be accomplished with a metal-working tool, would render it useless.
- VII. COST: Initial: Transfer of technique development into production requires initial set-up of pre-production prototype test, quality-assurance and low-volume facility, est: \$300,000.00

Operational: Current estimates indicate production unit costs per card (credit card size only) would approximate .28¢ to .34¢ each. Indicators point to regionally "secure" and franchised service centers, or "turn-key" I.D. production centers for Government.
- VIII. PROBABILITY OF DEFEAT: Sensor team associate indicates need to establish test and preproduction prototype facility to postulate an entire system.
Alteration
Counterfeit
Imposture
Provides proof of identification, unalterable characteristics. Sample I.D. cards could not be altered and attempts to do so rendered the produce useless. Neither an individuals photo, signature, other data or color-coding proved alterable.
- IX. IMPACT ON PUBLIC: Privacy: Permanent imaging provides proof-positive of bearer and bearer's signature or embossed I.D. No.

Convenience: Lightweight (no heavier than current plastic cards). Fireproof. Heat, flame and all non-corrosive solutions cannot impart damage to the product or structurally change it's characteristics. Can be used as effective safeguard for permanent record.

- X. PRINCIPLE OF OPERATION: Utilizes a photographic "type" of presensitized lightweight metal whose characteristics allow simple photo contact and overprinting, and upon completion a special treatment "seals" the record within the top metal layer thereby affording permanence. Quality assurance and production techniques for variety of documents need development funding.
- XI. UNIQUE FEATURES: The process technique yielded an unalterable, positive identification that was near-indestructible. Product may be color coded for use; proof-positive photo's, signatures, fingerprints, typed information etc., may be recorded and are not subject to alteration and retard any fraudulent use. Product lends itself to inclusion of magnetic striping and indicators point to direct reading by optical characters readers.

PRODUCT INFORMATION BRIEF

- I. FIRM: Optronics International, Inc.
7 Stuart Road
Chelmsford, MA 01824
(617)272-9104 or (617)256-4511
(George Cagliuso)
(John Ward)
- II. PROFILE: Small corporation--\$3 million annual sales
- III. TECHNIQUE OFFERED: Holographic Identification System
- IV. STATUS: Patents have been issued. Currently negotiating licensing agreement with larger company presently selling to the banking industry.
- V. APPLICATION: Credit cards, identification cards, bank passbooks, passports, library cards, classified documents for retail stores, banks, access control, document verification, welfare, etc.
- VI. HOW USED: A coded holographic film chip is optically (photographically) obtained of the identification data relative to the identification document. The film chip is embedded in a plastic card, badge or document. Upon needed identification, the coded hologram is illuminated by a special device and is rendered readable for use in available visual or semi-automatic verification systems. Can be machine or computer readable.
- VII. COST: Initial: \$300.00 per terminal.
Operational: \$100.00 per terminal.
- VIII. PROBABILITY OF DEFEAT: Statistically random code on information base makes alterations and counterfeiting extremely difficult.
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: Increased privacy on identification data.
Convenience: Same as conventional ID cards.
- X. PRINCIPLE OF OPERATION: Information is holographically photographed, utilizing laser techniques, and further distorted by means of a random code. Information is made coherent for visual or automatic reading by utilizing a small, helium-neon c-w laser and optical code to match that used in generating the coded hologram.
- XI. UNIQUE FEATURES: Cannot be seen with the naked eye, even if magnified.

PRODUCT INFORMATION BRIEF

- I. FIRM: Ralph C. Wicker
4199 West Henrietta Rd.
Rochester, N.Y. 14623
- II. PROFILE: Ralph Wicker, inventor in photo-optical, security fields.
Originator of 9 products with over 30 issued patents.
Background in printing, color, private research, specializing
in use of moire printing systems and methods of control.
- III. TECHNIQUE OFFERED: Hidden half-tone image printing and viewing.
- IV. STATUS: System is technically developed but not prepared for mass
production. Original system covered by two issued patents
and sold to American Banknote Co. of NYC. Present system
is an improvement over method sold to American in that
photographs can be hidden now as well as signatures and type.
New patents are being applied for. This photographic system
is now being offered for sale or license to qualified
credit card manufacturers.
- V. APPLICATION: Drivers licenses, social security card, credit cards, car
registration, passports security passes, checks for use by
banks, stores, police and other law enforcement agencies,
customs officials, etc.
- VI. HOW USED: A photograph of the identified individual and all pertinent
information including signature is placed on the card during
fabrication, using a special hidden method of printing.
The card then is totally transparent to the eye. All cards
are individual and specific to the card holder. The devices
for viewing are mass produced from one master. In principle
the card is placed on a projection or TV device and the
hidden images on the card can now be seen to identify the
card holder.
- VII. COST: Initial: Cost per unit document set up approx. 9 to 15¢
addition, assuming normal printed document. Viewing
apparatus cost approx. \$33.00 per unit for volumes of 1,000
units, for a direct viewing system only; however, this does
not include TV or projection systems.
Operational: Dependent on wide range of operational system
configurations.
- VIII. PROBABILITY OF DEFEAT: Need to postulate an entire system. American Bank Note
purchased the invention only after satisfaction that, with
the use of a black overprint, no counterfeit was possible.
Alteration No possible method of forgery or of changing photos or
Counterfeit descriptions was possible. Master screens in bank cameras
Imposture will self destruct if tampered with.

- IX. IMPACT ON PUBLIC: Privacy: Since imaging on the card is transparent or invisible, privacy can be guaranteed to the user either from theft or duplication or alteration. Since only viewing systems sold to banks and retail outlets can be used to view the hidden photo and signature, any theft or forgery attempt can be stopped at point of source. Card holders private information such as age, wt., social security number can now be kept totally private until needed for identification.
- Convenience: Since the hidden photo card is a basic I.D. system, it can incorporate all or a number of credit card systems such as Master Charge, Bank America Card, and magnetic bank cards. The basic symbols and I.D. numbers for these cards could be hidden or visual for credit usage along with the photo, signature, and other pertinent information. This would eliminate carrying a number of different credit or ID cards. The fact that this system is completely tamper proof will build a high level of confidence for both the user and the creditor, eliminating long waiting lines and embarrassing questions in banks and retail stores.
- X. PRINCIPLE OF OPERATION: To supply to the public, creditor, and law enforcement officials, a positive ID system that can be incorporated into present credit or identification systems.
- XI. UNIQUE FEATURES: Hidden photographs, signatures, and all pertinent information can be reduced to minute size approx. $\frac{1}{2}$ " by $\frac{1}{4}$ ". This would allow imaging on other credit systems. The image can then be projected to full size on viewers. Method of producing card prevents forgery or counterfeiting by photography, alteration or duplication. Real image cannot be seen by any method including high magnification.

III. PERSONAL IDENTIFICATION TECHNIQUES

The products described in this section are intended to assist in verification of identity through comparison of such personal characteristics as appearance, voice, or handwriting. In each case, the characteristics of an individual seeking verification are compared with the characteristics on file for that person; a decision must be made as to whether the characteristics match. Some of the products described require a human operator to make the comparison and decision; other products can perform these functions automatically.

NOTE: Product descriptions and claims made herein are the sole responsibility of the offerors. The FACFI, its staff, and the Department of Justice have not endorsed these products or verified the claims made for them.

PRODUCT INFORMATION BRIEF

- I. FIRM: Alden Electronic & Impulse Recording Equipment Co., Inc.
Alden Research Center
Westborough, MA 01581
(617)366-8851
(George F. Stafford)
- II. PROFILE: Designer, developer and manufacturer of electronic impulse and recording equipment. Offers implementation and operational services using off-the-shelf equipment or built-to-order.
- III. TECHNIQUE OFFERED: Signature, fingerprint, or photo or document transmission and reception system.
- IV. STATUS: Operational--several hundred Alden 400 FM fax systems in use for signature verification.
- Built-to-order--Alden 8080 digitizer interfacing the Alden 400 FM Fax systems to ASCII signal source or CPU files.
- Larger document 6", 8", 11" and 18" systems available.
- V. APPLICATION: Wherever the fax transmission of a signature, fingerprint, photo or document may be used. Allows central or remote verification of signature only, signature and a fingerprint, or signature and a photo. Possible utilizations include banks, retail stores, public officials, plant security, customs immigration, border check points, in short any IV (Identification Verification) needs.
- VI. HOW USED: Remote locations initiating documents (sales slips, bank withdrawals, etc.) or needing I.V. can verbally request identity data from the Central and make the I.V. decision or can fax the data on the identity document (signature only, and/or a print, and/or photo) to Central and they make the I.V. and notify the Remote location.
- A signature can be faxed in 10 seconds, one print or a 2" x 2" photo can be faxed in one minute.
- VII. COST: List prices are Scanner \$3500, Recorder \$2500. Volume prices can reduce to \$1700 and \$900. Remote decision making uses one or few Scanners at Central and a Recorder for each remote location. Central decision making uses few Recorders at Central and a Scanner at each remote location.
- To marry the FM Fax distribution to a digital source of data involves use of an Alden 8080 Digitizer custom adapted--approx. price \$5000 to \$6000.

- VIII. PROBABILITY OF DEFEAT: Alteration Counterfeit Imposter Decreases considerably as a fingerprint is used in addition to a signature and is further decreased with addition of a photo. It is a function of relative abilities of the decision maker and the forger. A combination of signature and a fingerprint would be difficult to beat.
- IX. IMPACT ON PUBLIC: Privacy: Not contained in CBD response.
Convenience: "... no one refuses to sign a sales slip, withdrawal form, etc...", the taking of a fingerprint can be made just as simple..."
- X. PRINCIPLE OF OPERATION: Facsimile system allows for transmission and reception of identification document containing items such as a signature, fingerprint or photograph. Verification system is not a part of the technique offered. However, the technique offered allows for the employment of a centralized, standardized and sophisticated verification system. Technique offered also allows for individual at checkpoint to do comparisons of signatures, photographs, etc. of individuals desiring identification by comparing with that contained in a central data file.
- XI. UNIQUE FEATURES: Enhances verification options available in a given checkpoint. Possibly reduces skills required at checkpoint in that verification responsibility may be accomplished at a centralized facility utilizing dedicated and skilled personnel.

PRODUCT INFORMATION BRIEF

- I. FIRM: International Business Machines Corporation
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, N.Y. 10598
(914)945-2064
(Noel M. Herbst)
- II. PROFILE: Large corporation possessing research, design, development, implementation, operational and field support capabilities in many diverse areas embracing computer technology and application.
- III. TECHNIQUE OFFERED: Automatic Signature Verification
- IV. STATUS: Operational in a research laboratory
- V. APPLICATION: Personnel identification for security, in applications such as financial transactions and access control.
- VI. HOW USED: Users enters tentative identification by keyboard or magnetic card, and signs with an instrumented pen of conventional size and shape. Up to three signatures may be required for verification.
- VII. COST: Initial: Not contained in CBD response
Operational: Not contained in CBD response. (Need to complete development and formulate an entire system.)
- VIII. PROBABILITY OF DEFEAT: On 70 test subjects, the laboratory system indicated a forger acceptance rate of 2% and a valid rejection rate of 2.87%. Forgers were knowledgeable about the verification technique and did their best to break the system. Field experience is not available.
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: "... it is free from the unfavorable connotations attached to other methods of personal identification."
Convenience: Would appear to be acceptably convenient. An average of 1.17 signatures were required for verification.
- X. PRINCIPLE OF OPERATION: The fine structure of the muscle forces exerted during a signature is very precise for most people and is not subject to conscious control. Based on this observation, a system comprising an instrumented pen coupled to a computer has been developed and is operational in the laboratory. The verification algorithm is based upon the acceleration-time function.
- XI. UNIQUE FEATURES: Not contained in CBD response

PRODUCT INFORMATION BRIEF

- I. FIRM: Wen C. Lin
Professor of Computer Engineering
Dept. of Computing and Information Sciences
Case Western Reserve University
Cleveland, Ohio 44106
- II. PROFILE: Professor at Case Western Reserve University
- III. TECHNIQUE OFFERED: Speech and signature computer-aided recognition and verification.
- IV. STATUS: R&D - 90% operational on speech
- 50% operational on signature
- V. APPLICATION: Wherever identification document may contain a signature or where identification can be wholly or partially based upon speech identification.
- VI. HOW USED: It is an on-line and adaptive minicomputer-based system.
- VII. COST: Initial: Not contained in CBD response
Operational: Not contained in CBD response
- VIII. PROBABILITY OF DEFEAT: Not contained in CBD response
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: Dependent upon results of R&D and upon wide range of operational system configurations.
Convenience: Dependent upon results of R&D and upon wide range of operational system configurations.
- X. PRINCIPLE OF OPERATION: Computer analysis and pattern recognition of speech or signature characteristics. Detailed principle dependent upon result of R&D.
- XI. UNIQUE FEATURES: Not contained in CBD response.

PRODUCT INFORMATION BRIEF

- I. FIRM: Peerless Printing Company, Inc.
2745 Lafitte Street
New Orleans, Louisiana 70119
(504)486-6222
(George L. Mayer)
- II. PROFILE: Established check printing company
- III. TECHNIQUE OFFERED: Signature comparison display
- IV. STATUS: Being considered for development--patented.
- V. APPLICATION: Check cashing, credit card purchases, identification, etc.
- VI. HOW USED: Reference signature contained on check, card, etc. in a scrambled manner, unidentifiable to the holder. Reference signature and user signature, obtained at time of desired identification, is compared by placing both in a small display like device and visually comparing. Both signatures are displayed and may be positioned electronically as desired on the display screen.
- VII. COST: Initial: Plan to make it available in quantity for under \$500.00
Operational: Estimated at 1/4¢ per printed check.
- VIII. PROBABILITY OF DEFEAT:
Alteration - highly improbable
Counterfeit = highly improbable
Imposture - approximately one in five thousand by experienced forger working from signatures on previous checks.
- IX. IMPACT ON PUBLIC: Privacy: Near zero, since signature is now in common use.
Convenience: It is easy to operate. It requires nothing extra or new on the part of the customer.
- X. PRINCIPLE OF OPERATION: Valid reference signature is taken from signature card and optically scrambled into hundreds of unidentifiable "squiggles". This pattern is printed on check at the time the name, address and Magnetic Ink Character Recognition (MICR) is printed. An opto-electronic device is then used to unscramble this image so it can be compared with the signature on the bottom of the check.
- XI. UNIQUE FEATURES: Provides on-the spot reference signature without giving the forger a signature to copy.

PRODUCT INFORMATION BRIEF

- I. FIRM: George H. Warfel
Technical Consultant
P.O. Box 627
Menlo Park, Calif. 94025
(415)322-0488
(George H. Warfel)
- II. PROFILE: Consultant/inventor
- III. TECHNIQUE OFFERED: Dynamic Digital Signature Data in Magnetic Stripe, in central file, or partially in each.
- IV. STATUS: Working model and issued patent
- V. APPLICATION: Personal identification of customer in financial transactions and other areas of ID.
- VI. HOW USED: As part of credit, cash, or automatic teller terminal systems, or with access control systems.
- VII. COST: Initial: \$100 per unit
Operational: Line charges when central data base is accessed.
- VIII. PROBABILITY OF DEFEAT: Probability of defeat by impostor estimated as 1 in 10,000. Other techniques do not appear to be a problem.
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: Minimal, since signature is now commonly used to verify transactions.
Convenience: Portable signature tablet similar to that used in gasoline credit card purchases makes method convenient for customer and merchant. Present formsets and customer's own pen may be used.
- X. PRINCIPLE OF OPERATION: Profile of rhythm and speed of customer's pen motion during normal signature is obtained through pressure-sensitive pad and stored in digital form both in central data base and on magnetic stripe of card carried by customer. This enrollment procedure can be accomplished during first five transactions. File information is compared with signature profile at each successive transaction attempt. Profile can be updated after customer verification by changing data on stripe, central data base, or both, thus enhancing the accuracy of the system with usage.

XI. UNIQUE FEATURES: Customer may use his own or any pen for signature; no need to involve central data base for verification in small transactions (terminal compares signature profile with card data). Customer validated at each transaction; low cost system. Tablet will extract signature data through existing printed form or formset up to light card stock.

PRODUCT INFORMATION BRIEF

- I. FIRM: Westinghouse Electric Corporation
Defense & Electronic Systems Center
Baltimore-Washington International Airport
Box 1693
Baltimore, Maryland 21203
(301)765-2207
(J. P. Hirl)
- II. PROFILE: Large defense and electronic corporation possessing research, design, development, implementation and operational capabilities in many diverse areas.
- III. TECHNIQUE OFFERED: Speaker identification
- IV. STATUS: Presently in research and development phase with some prototype testing and evaluation. Two prototypes built to date.
- V. APPLICATION: Law enforcement, identification of phone caller, credit card and key card user, access control and banking.
- VI. HOW USED: Real-time speech analysis and accompanying verification techniques.
- VII. COST: Initial: Estimated that a system providing a 5 to 10 percent error rate will cost less than \$1,000 per unit in volume. Costs increase for decreased error rate.
Operational: Operational cost data not yet available.
- VII. PROBABILITY OF DEFEAT: Dependent upon postulated entire system and specific application.
Alteration
Counterfeit
Imposture
- IX. IMPACT ON PUBLIC: Privacy: System responds to voice characteristics which are uniquely related to each individual.
Convenience: Does not require elaborate recordkeeping. System inputs are natural spoken words for both initial setup and recognition. Automatic recognition capability.
- X. PRINCIPLE OF OPERATION: The system operates on the principle of real-time formant analysis utilizing Westinghouse proprietary techniques.
- XI. UNIQUE FEATURES: Not contained in CBD response

APPENDIX C4

**A SURVEY OF FOREIGN NATIONAL SYSTEMS
FOR PERSONAL IDENTIFICATION**

C.E. Harrison

**The MITRE Corporation
Bedford, Massachusetts**

June 1976

C-131

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
LIST OF TABLES	C-133
I INTRODUCTION	C-135
II FALSE ID PROBLEMS IN OTHER LANDS	C-137
III METHODS OF PERSONAL IDENTIFICATION	C-145
IV IDENTITY SYSTEMS OF REPRESENTATIVE COUNTRIES	C-151
V SUMMARY AND CONCLUSIONS	C-157
ATTACHMENT A - INTERPOL QUESTIONNAIRE	C-160
ATTACHMENT B - STATE DEPARTMENT QUESTIONNAIRE	C-165
ATTACHMENT C - EXTRACT FROM FRENCH CRIMINAL CODE	C-167
REFERENCES	C-169

LIST OF TABLES

<u>Table Number</u>	<u>Page</u>
I DOCUMENTS AND PROCEDURES USED TO OBTAIN IDENTITY DOCUMENTS	C-138
II SUMMARY OF LAWS ON MISUSE OF IDENTITY DOCUMENTS	C-141

SECTION I
INTRODUCTION

Purpose

The Federal Advisory Committee on False Identification (FACFI) is investigating the problem of false identification in commission of criminal acts. As a part of this investigation this report documents the results of a survey of the related experience of various foreign countries. The interest of the U.S. Government in this matter is in the following two general areas:

1. Many foreign countries have used advanced techniques of personal identification for many years and the U.S. can, therefore, profit by their experience.
2. Some U.S. problems, such as illegal immigration and drug smuggling, involve falsification of foreign documents. The U.S., therefore, has need to know about foreign personal identification procedures to effectively combat the use of such false documents.

This report is intended to provide a general appreciation of the false identification problems in foreign countries; however, since it is based on limited data, it should not be considered a reference document.

Sources of Data

The principal sources of information used in this report are surveys made by the U.S. State Department through embassy channels and by the International Criminal Police Organization (INTERPOL).* The INTERPOL survey covered twenty-five countries of which sixteen replied. The State Department survey^[1] covered fourteen countries of which twelve replied. A total of thirty countries were included in these surveys. Countries providing useful information to the INTERPOL survey^[2] included: Australia, Austria, Bermuda, Denmark, Egypt, France, West Germany, Jamaica, Japan, the Netherlands, Peru, Spain, and the United Kingdom. Useful inputs to the State Department

*The questions asked in these surveys are shown in Attachments A and B.

survey were provided by Argentina, Brazil, Colombia, France, West Germany, Greece, Italy, Japan, Romania, Sweden and the United Kingdom.

The general response to these surveys was excellent considering that this was an initial effort. Specific questions on identification procedures, laws, identity documents used, etc. were responded to in a useful manner by a large portion of the addressees. More general questions involving such considerations as social cost of false identification were not consistently answered. There were some indications of a lack of appreciation for or understanding of the problem of false identification by some of the countries responding.

The results of these surveys were supplemented to the extent possible from other sources. The most useful of these other sources was the report of the International Symposium on Automation of Population Register Systems held in Jerusalem, Israel, 25-28 September 1967, and sponsored by the International Federation for Information Processing.^[3] This report contained useful information on actual or planned population register systems in Denmark, Finland, West Germany, India, Israel, Italy, the Netherlands, Norway, Sweden and Switzerland.

From all sources, significant information was received pertinent to twenty-five countries.

SECTION II

FALSE ID PROBLEMS IN OTHER LANDS

Common Personal Identification Documents

The most common identification document used in the countries surveyed is a national identity card (commonly referred to as a national identification document or national ID). Fifteen out of the twenty-one countries about which we have positive information use such a document. One (Greece) has a police identity document which is approximately equivalent. Peru is planning to establish a national ID. All countries have passports; however, these are not normally used for identification purposes within the country of issue. All countries issue drivers licenses. In addition, police and military identification cards, health insurance cards, company identification cards, social security cards, selective service cards, voter and tax registration cards are used in varying degrees as a means of identification in the countries surveyed.

In countries which have national IDs, this is the normal means of identification. Where no such document exists, there is a tendency for documents issued for other purposes to be used as a substitute for it. In the United Kingdom, the National Health Insurance card, and in Switzerland the national social insurance card performs this function to a limited extent.

The cards used for personal identification are supported by personal or family records and by application procedures which are part of the identification process. Application procedures include use of photographs and/or fingerprints, personal questionnaires, certificates from officials and citizens, employers or use of other supportive documentation. The most common supportive documents used are birth and marriage certificates. The value of an identification document as a means of providing assurance that the bearer is correctly identified is derived from the total process involved in issuing such documents and not solely on any inherent characteristics associated with the document per se. Table I lists the supporting documentation and procedures involved in the issuance of a representative cross section of identity documents from various countries.

The existence of considerable numbers of resident aliens among the population poses a special problem of personal identification. For very short-term visits (less than 2 months) the passport or visa

issued by their country of citizenship is normally sufficient identification. National identity documents issued by the countries of the European Economic Community are also commonly recognized by all members of that community. For longer periods of residence some other form of temporary or permanent identification is commonly required. Brazil and Argentina issue identity cards to resident aliens which are similar to those used by citizens. Germany and Greece use residence permits. Japan requires a certificate of alien registration. In the United Kingdom national passports are used by resident, long-term aliens who are citizens of the British Commonwealth. Those who are citizens of the European Economic Community are issued a resident's permit. Other aliens in permanent residence must have a police registration certificate. Other countries probably use similar documents for identification of aliens, but did not indicate these in the survey.

Nature and Scope of False Identification

The information received from survey respondents on the nature and scope of the false identification problem was in most cases very limited. The United Kingdom, however, provided a detailed listing of uses of documents for false identity. Birth certificates, passports, social security cards, drivers licenses, immigration, nationality and registration certificates, credit cards and examination certificates were frequently used to establish a false identity. False documents were used in illegal immigration (including that of fugitive offenders), to obtain goods fraudulently, to drive illegally, to obtain employment for which the applicant was not qualified and for general identification purposes. Argentina cited the use of illegal certificates to establish U. S. citizenship, and use of lost passports for drug trafficking, smuggling, etc. Australia and Japan cited the fraudulent obtaining of passports. Several countries cited problems related to foreigners using false foreign drivers licenses and other problems involving aliens as a source of false identification problems.

The extent of the problem of false identity perceived by countries responding to our surveys can be categorized as follows:

I. Significant Problems Exist

Australia, Colombia, United Kingdom

II. Some Problems Exist

Argentina, Egypt, France, West Germany, Peru, Sweden

III. No Significant Problems Exist

Denmark, Japan, the Netherlands, Romania, Spain

For the other countries included in the data base, there was insufficient information on which to make a judgment.

An attempt was made to correlate the reported extent of the problem of misuse of identity documents with the International Crime Statistics by INTERPOL for the years 1969-1970 and 1971-1972. This attempt was unsuccessful in that statistics in these documents cover very broad categories of crimes only and none of these could be directly associated with misuse of identity documents.

False ID and the Law

Ten countries (Argentina, Australia, Brazil, Colombia, France, Germany, Greece, Japan, Spain and Sweden) supplied responses to our queries as to legal penalties for use of documents for false identification.

The applicable provisions of the laws provided by the above ten countries have been summarized in Table II. This table provides a comparative picture of the legal constraints within these countries and, to the extent that these countries are typical, of the worldwide variation in legal penalties for use of documents to establish false identity.

The French laws are among the most complete; they cover all significant documents and the most significant ways in which crimes involving false identification could be committed. An extract of these laws has, therefore, been included as Attachment C to this report. The laws of Brazil and Germany are very similar to those of France. Japanese laws are also very thorough; however, the use of false identification documents (as contrasted to their production) does not appear to be included. Argentina, Colombia, Greece, Spain and Sweden provide substantial penalties; however, the coverage is not as comprehensive as for the French laws. All of these countries have laws which could be real deterrents to false identification. In contrast, the Australian laws cover only limited aspects of the problem and do not appear to be a significant deterrent.

Other countries in the data base may have similar laws, but did not describe them. Crimes involving misuse of identity documents may also be covered by more general laws covering the specific crimes committed. For example, an individual who uses illegally obtained

TABLE II
SUMMARY OF LAWS ON MISUSE OF IDENTITY DOCUMENTS

COUNTRY	AUSTRALIA	FRANCE	GREECE	JAPAN	SPAIN
IDENTITY DOCUMENTS COVERED	Passports	Permits, Certificates, Memorandum books, Cards, Reports, Receipts, Passports, Laissez-passer, etc.	Documents, Police ID	(a) Official Documents, (b) Private Documents, (c) Official Seals/Signatures, (d) Private Seals/Signatures	Documents, certificates
(a) Counterfeits, forges falsifies, alters document		6 mo.-1 yr. imprisonment 1500-15,000 Frs. fine 5-10 yrs. loss of civil rights	At least 3 mo. imprisonment *Up to 10 yr. incarceration	* (a) 1-10 yr (b) 3mo.-5 yr. ** (a) Up to 3 yr or 300 yen fine ** (b) Up to 1 yr or 100 yen fine (c) 3 mo-5 yr (d) Up to 3 yr	Major detention
(b) Issues/utters false document (official or public servant)		1-4 yr imprisonment 1500-15,000 Frs. Fine 5-10 yr. loss of civil rights			
(c) Uses false or obsolete document		Same as (a) above	Same as (a) above		
(d) Obtains document using false information	50 pounds or 3 mo. imprisonment	3 mo.-2 yr. imprisonment 500-5000 Frs. fine		* (a) Up to 5 yr or 1000 yen fine ** (a) Up to 1 yr or 300 yen fine	Major detention 5,000-10,000 pesetas fine
(e) Uses document obtained using false information		Same as above			
(f) Drafts false document				(a) and (b) Same as (a) above	
(g) Fails to return invalid document or one obtained using false information	50 pounds or 3 mo. imprisonment	Same as for act attempted			
(h) Attempts to commit above acts					

ACTS PUNISHABLE BY LAWS

TABLE II (Concluded)

COUNTRY	ARGENTINA	BRAZIL	GERMANY	SWEDEN	COLOMBIA
IDENTITY DOCUMENTS COVERED	National ID Card All documents (forgery)	All identity documents	Birth Certificates, Drivers Licenses, Other Identity Documents	All official records or documents submitted as a means of establishing identity	Documents, Passports, National ID
(a) Counterfeits, forges, falsifies, alters document	6 mo.-2 yr. imprisonment	2-6 yr. imprisonment Fine up to \$1.00 U.S.	Up to 5 yr. imprisonment	Up to 2 yr. imprisonment	6 mo.-3 yr. imprisonment. Fine, Job suspension
(b) Issues/Utters false document (Official or public servant)		1-5 yr. imprisonment	Up to 5 yr. imprisonment or fine		3-10 yr. imprisonment Up to \$1800 fine
(c) Uses false or obsolete document	2 yr. up imprisonment	2-6 yr. imprisonment	Up to 1 yr. imprisonment or fine	Up to 2 yr. imprisonment	3-10 yr. imprisonment Up to \$1800 fine
(d) Obtains document using false information		1-5 yr. imprisonment Fine up to \$1.00 U.S.	Up to 1 yr. imprisonment 3 mo.-5 yr. (aggravated)	Up to 2 yr. imprisonment	
(e) Uses document obtained using false information	2 yr. up imprisonment	1-5 yr. imprisonment Fine up to \$1.00 U.S.	Up to 1 yr. imprisonment 3 mo.-5 yr. (aggravated)		
(f) Drafts false documents					
(g) Fails to return invalid document or obtained using false information					
(h) Attempts to commit above acts					
(i) Use of false name by alien		1-3 yr. imprisonment. Fine up to \$1.00 U.S.			(Penalties are not normally enforced)

ACTS PUNISHABLE BY LAWS

documents in the process of committing embezzlement or fraud may be prosecuted for embezzlement or fraud rather than the associated act of false identification. The existence of specific laws against the creation and use of false identity documents such as those listed in Table II provides a significant deterrent even in cases in which no other serious crime was involved.

SECTION III

METHODS OF PERSONAL IDENTIFICATION

Personal identification systems used in foreign countries consist of a collection of components with various degrees of national control. The effectiveness of these systems depends both upon the design of these components and how well the components are coordinated within the complete system. The most complete systems contain the following major components:

- a. National identity document or equivalent.
- b. Family or personal records.
- c. Population register.

We will discuss each of these components in turn below. In Section IV the personal identification systems of selected countries are described on an integrated basis.

a. National Identity Document

In most of the countries surveyed, the national ID is the primary means of identification. It is normally a pocket-sized, folding card which contains essential information required for personal identification. This information consists as a minimum of name, date of birth (birth number may be included in some countries), address, and identification document number. In some countries additional information such as personal characteristics (height, weight, color of eyes and hair, blood group, occupation, religion, name of father, mother and spouse) may be added. Specific detailed information was obtained on six National ID's. All of these required signatures and photographs and four of these six documents contained fingerprints. Spain employs a unique technique of placing the fingerprints half on and half off the photograph, thereby making it difficult to substitute photographs without detection. Various techniques of fabrication are known to be used to make alteration or forgery more difficult; however, very little specific information on this subject has been made available.

In most countries the national identity document must be carried at all times; however, this is not universal and in at least one country (West Germany) the national identity document is not normally carried on a day-to-day basis.

The most important item on this document is the identifying number. This number is unique and carefully controlled. Through the use of this number, the personal records kept on the population can be accessed. For this reason, it is possible in many countries through the use of this number alone to provide reasonable verification that an individual is the person he claims to be, and it may also be relatively easy to detect a false document by its incorrect number.

b. Family or Personal Records

Three of the countries surveyed (France, Japan and Spain) maintain a system of family records in which changes in the personal status of all members of the family (births, deaths, marriages, divorce, adoption, etc.) are recorded. These records are historically well established and are the basic reference in establishing a person's identity. They are, for example, used as a required supporting document for issuance of national identity documents or passports in these countries. The existence of these carefully maintained family records provides a good assurance that the country's population is accurately and correctly identified and a positive basis for a personal identification program.

c. Population Register

Many countries have well established population registration systems. The use of such systems is widespread in Western Europe and especially in Scandinavia and the Netherlands. The Swedish population register system is 300 years old. The Netherlands' population register system originated with a Royal Decree in 1849. Other systems have been in use for several decades.

These population registration systems have historically been developed in response to fundamental long-standing needs of governments for information on inhabitants in much the same way as, for example, William the Conqueror felt required to make the population survey of England which resulted in the famous Domesday Books in the eleventh century. The principal application for population register systems is for statistical purposes (including census data). For an established system the creation of new sub-registers for specialized purposes is relatively easy and inexpensive (especially in highly automated systems) and the number of applications tend to multiply. A

review of eight population register systems identified the following uses: statistics, census, voting rolls, tax records, police records, criminal records, military records, health insurance, national insurance, public health programs, educational programs, national pensions, social security, church records, welfare, civil servant registers, federal payrolls, and public utilities.

The ability to identify individuals is a necessary pre-requisite and by-product of the existence of personal register systems. Those countries which have a well organized population registration system consistently claim that they have minimal problems of misuse of identity documents and in many cases give primary credit to these systems for that condition.

In a sophisticated system, population registers operate as portions of an overall personal register system consisting of the following general components:

1. A personal and/or family record (see Section IIIb).
2. A personal identity card or as a minimum a personal number uniquely identifying every registered person in the country (see Section IIIa).
3. Local population registers containing general information on inhabitants of a town, parish, or other administrative sub-unit.
4. A central population register containing minimal information on each registered individual in the country.
5. Sub-registers or associated registers dedicated to specific applications (taxation, motor vehicles, etc.).
6. Procedures for making inputs into and obtaining outputs from the system.

All of these components are tied together by the personal number (generally the same number used in the national identity document).

Although the manner of operation of population registers can vary extensively, the most common procedure is to establish a population register at the local government level which contains a reasonably detailed amount of information on each individual and a consolidated but somewhat abbreviated record covering all residents at a central office in each country. Generally, the local registers are under the control of local administrative officials, who may be clergy acting in a civil capacity, tax officials, or police.

The operation of the central registers is a responsibility of a central bureau of statistics or some similar agency. The amount of

information in the local population registers varies. In an automated system one data card per individual is normally required. At the central register either a duplicate of this card or a simplified card containing only identifying information may be used. The data card used with the Danish population register system contains all the information listed for the national identity document described in Section IIIa plus information on pensions, health insurance, conscription status, occupation, tax and election numbers, declaration of incapacity and several data fields allocated to changes in status, local use, etc.

Both the local and central registers are interconnected with a series of other registers in which detailed information within a specialized area of interest is stored. Sensitive information which should not be available for general use is normally confined to these specialized registers. The maximum number of specialized registers identified as being associated with a population register system for the countries surveyed was ten (in Finland). There is regular feedback between these registers and the population registers in order to keep all of them up-to-date. Regular inputs are also obtained from the offices of records for birth, marriage and death certificates, immigration and emigration, census, taxes, voting, etc. Population registers are routinely updated on a weekly or monthly basis to reflect any change in status or address of covered personnel. This systematic updating and routine interaction with all the official actions affecting a person's status makes it very difficult for an error in personal identification to remain undetected for any length of time.

There are a number of problems that a population register system must solve to be effective. The most common problems are:

- a. Obtaining and maintaining a single list of person numbers corresponding to all covered individuals,
- b. Maintaining good address locations,
- c. Security of information.

The problem of maintaining a complete, accurate person list is especially important in initiating a personal registration system. It is inherently interrelated to the maintaining of addresses. People may have multiple residences or move without notification. For a personal register system to work, each individual must be associated with a single precise location. He must not change that location without appropriate action with respect to the personal register system. For this reason Finland and Sweden tie their population register system into a land (real estate) register. To assure a single listing for all registrants, it is necessary to keep track of persons who are transients in the system. Separate sub-registers are often maintained for persons who have died, emigrated, are listed as missing, etc.

A census is a good means of correcting a population list. Israel, by correlating its population registers with the 1961 census, reduced incorrect listings from approximately 25% to around 0.5%.

Countries with population registration systems have a keen awareness of the necessity to preserve personal security and privacy. The most common actions taken are to limit the amount of information in the central registers and to maintain the most sensitive information (criminal records, etc.) in related files which are not for public use. Fairly strong controls are generally maintained to insure that only limited information (name, address) is made available to private parties. Potential abuse of registration systems by government officials and employees is controlled by careful supervision and imposing substantial legal penalties for violations of trust. The fact that these measures for assuring security of information can be successful is evidenced by the rapid growth of personal registration systems right after World War II in three countries which had recently suffered through occupation by a foreign power (Finland, Norway, the Netherlands). Under the circumstances one would expect the population to be suspicious of any personal identification system that displayed a vulnerability to government abuse.

It is worthy of note that the three problems associated with population registers must also be solved by any personal identification system.

d. Other Methods of Identification

Countries which have either a national identification document, a family record or a population registration system tend to place primary reliance on them for personal identification. The majority of the countries included in the data base are in this category. For those countries which do not have an official legal personal identification system a variety of documents may be used to establish identity. The most frequently used documents are drivers licenses, passports, bank cards, health insurance or social security cards. These same documents may be used as supplemental means of identification in countries having formal identification systems. The design and credibility of these documents varies widely. A drivers license, for example, can be a reliable means of identification in countries such as Japan or Spain, which rigidly control its issuance and manufacture. In others, it is no more reliable than in the U.S.

Documents used for registration of aliens tend to be similar in design and utilization to comparable ones used by citizens. The alien residence permit used in Greece and the temporary resident's identity card in Brazil resemble very closely the police or national identification card used for citizens.

The procedures which govern application, investigation and issuance of identity documents are an essential element in the personal identification process. These procedures are closely associated with the concept of a legal domicile. In countries with formal personal registration systems every individual has a single legal residence and a location where his personal records are kept. These may or may not be the same; however, in all cases these locations are a part of the personal records, are unambiguous and are not changed without formal procedures. All applications for identity documents are accompanied by some statement of personal history. Matching this personal history and the physical characteristics of the individual with the information in personal or family registers provides a relatively strong assurance that the applicant has identified himself correctly. Statements or certificates from knowledgeable citizens or local officials are also used to support the application. In the Netherlands and Japan (and possibly other countries) a notification to pick up his completed identity document is mailed to the applicant at his established legal residence as shown in the personal records. This makes it difficult for someone who does not live at that residence to falsely obtain such documents.

The degree of confidence in the authenticity of personal identification documents is derived from the combination of supporting documentation, investigative procedures and personal records. Table I (on page 4) gives an overview of the documentation and procedures used to obtain selected identity documents.

SECTION IV

IDENTITY SYSTEMS OF REPRESENTATIVE COUNTRIES

In this section we discuss identity systems used in selected countries in relation to the problem of false identification. These countries have been selected to provide a representative cross-section of the types of identification systems used. The systems surveyed fall in the following categories:

- (a) Highly centralized systems using national identity documents and sophisticated population register systems. Denmark, the Netherlands, Norway, Sweden, and Finland are considered to be in this category.
- (b) Systems in which much authority is delegated to the lower government levels and there is no legally recognized identity document or integrated population system. (Australia and the United Kingdom are in this category.)
- (c) Systems which are at various levels of centralization in between the two extremes described above. All of the other countries in the data base are in this category.

Sweden has been selected as representative of the highly centralized systems. The United Kingdom is representative of the less highly organized systems. West Germany represents an intermediate level of centralization. Japan has a unique system which is of interest. Brazil has been selected as one of the more highly developed Latin American countries.

Sweden

Sweden, a country of 8 million people, is divided into 25 provinces (or counties), communes and parishes. It has a system of population registers which is 300 years old and is apparently well accepted because it was considered essential for providing fair income taxation, maintaining accurate election rolls, etc. Another contributing factor may be that Sweden, like other Scandinavian countries has a limited number of surnames and Swedish names do not by themselves provide adequate identification. The heart of this system is the Civic Registration Office, maintained in each parish by the parish vicar in his civil capacity as a census official. This

dual role for church officials is not unusual in countries which, like Sweden, have national churches. At the Civic Registration Office a basic record is kept for each person in the parish (including immigrants and aliens) from birth until death.

Each person's basic record is kept on a separate document containing name, data and place of birth, nationality, parent's name, civil status, name of husband or wife and children, and other pertinent information on his status which has administrative or legal significance. This information is filed by a ten-digit civic registration number containing in its internal design information on date of birth, province of birth, sex and sequence number. This number is unique and will stay with the person it identifies throughout his life.

Consolidated population registers are maintained by counties and a Central Population Register is maintained by the National Board of Civic Registration and Tax Collection. The system is largely automated. It is interconnected with other registers devoted to motor vehicles, drivers licenses, military personnel, and land (real estate).

All births, marriages, deaths, divorces and name changes are registered with the Civic Registration Office. Changes of residence must be sent to the parish office within two weeks. In addition, landlords, the post office, hospitals (births and deaths), courts and social security agencies routinely submit changes of status within their jurisdiction to the Civic Registration Office. The entire system is updated on a weekly basis. There is an annual registration as of 1 November each year, at which time the entire population register is updated and the legal residence of individuals is established for the following year.

In Sweden two types of documents are commonly used for identification purposes. An ID card, commonly referred to as the national ID card, is issued by banks and post offices. The possession of this card is not required; however, its use is widespread. The other card is the drivers license issued by the county board. The issue, manufacture and use of these documents is carefully controlled by the Swedish government. Both require inputs from the Civic Registration Office at the parish of domicile. Drivers licenses require doctors and police board certificates. These documents are issued by the "AB-ID-Kort," a quasi-governmental company. Company ID cards produced for internal use are also accepted for check transactions.

Sweden claims to have minimal problems with fraud (including that related to false identity). The Swedish police in 1975 recorded

a total of 23,807 cases of fraud of which 1,198 involved the use of identity cards.[4] In comparison to other countries supplying similar statistics, this incidence rate of approximately 15 per 100,000 persons is considerate moderate. Sweden has moderately strong laws (up to two years imprisonment) governing most manners of misuse of identity documents.

United Kingdom

The United Kingdom has no form of population register, family register or any other systematic method of maintaining a controlled information file on personal identities. There is no national identity document. The document that most closely approximates a national ID is the national insurance health card, which is issued to all employed persons (citizen or alien) and has an assigned card number which is maintained for life. Drivers licenses or other similar commonly used documents have some credibility for establishing identity. In reviewing passport applications, the British rely more on investigative techniques and on countersignatures by private or government officials of some stature (Ministers, Bank Officers, Police Officers, etc.) attesting to applicants' identity than on documents.

The United Kingdom has an exceptionally severe problem of false identity due to the presence of many non-citizens. By longstanding tradition, citizens of British Commonwealth countries have the privileges of relatively free access. Residents of the European Economic Community are also permitted relatively easy entrance. The United Kingdom has different identification rules for each category of aliens. Commonwealth citizens need only national passports; citizens of Common Market countries use national passports, national identity documents or residents permits. Other aliens are required to obtain police registration certificates.

British laws pertinent to false identity vary in severity. Forgery of birth certificates with intent to defraud or deceive can be punished with up to fourteen years imprisonment, whereas forgery of a license is punishable by a maximum of four months imprisonment or 100 pounds fine. The more severe penalties are seldom imposed.

Although the United Kingdom Passport Office states that there is no widespread practice of misuse of United Kingdom documents of identity, Scotland Yard (through INTERPOL) describes numerous documents (birth certificates, social security cards, passports, credit cards, etc.) which are frequently used as a means of establishing a false identity.

West Germany

West Germany occupies a position midway between countries like Sweden which have highly integrated, sophisticated personal identification systems and those like the United Kingdom or the United States in which there is no organized system for personal identification.

West Germany is a federation of more or less independent states; however, certain functions, which in the United States are in the exclusive jurisdiction of the states, are subject in West Germany to a considerable degree of centralized control. West Germany has a national identity document; however, it is not required to be carried at all times and other identity cards (student ID cards, drivers licenses) are satisfactory for many routine identifications within the country. All legal personal records are kept at the place of birth in the office of personal records, an office of the local police. Passports, identity cards and birth certificates are issued by that office, and death certificates are forwarded to that office from anywhere in Germany (East or West) and most other countries in Europe. Although drivers licenses are issued by local authorities, there are plans to produce them using a standardized "forgery proof" synthetic paper to be issued and numbered consecutively by the Federal Printing Establishment. Their issuance will be coordinated with car registration by the "Federal Vehicle Office."

West Germany has a comprehensive set of laws with rather severe penalties covering misuse of identity documents. West Germany maintains no statistics on falsification of identity documents; however, 22,749 cases of forgery of documents were recorded in 1974. In comparison to other countries for which similar statistics are available, this incidence of approximately 36 per 100,000 persons is considered moderate.

Japan

The Japanese system of personal identification has some unique features. Two of these are the use of family registers or "Koseki" and the use of official or private seals or "Jitsuin." The system of "Koseki" is highly developed in Japan and all Japanese nationals are registered at a city, town or village office. The "Koseki" is a unique system of family records which is thirteen centuries old. The Family Registration Law of December 22, 1947 requires the mayor of a city, town or village where the family makes its permanent domicile to keep an accurate record of all changes in the personal status of a specific individual, and any changes in the personal status not entered into the "Koseki" are not recognized as legal in

Japan. This "Koseki" is customarily and widely used for identification purposes in Japan.

Government offices in Japan require individualized personal seals on all documents presented to them. Seals are used for cashing checks at banks, postal money orders at post offices, etc. For local purposes a specific seal, called "Jitsuin," which is registered with the mayor of the city, town or village in which the residence of the individual is located, must be presented. This "Jitsuin" is customarily and widely accepted as a means of identification.

Japanese government offices tend to require a combination of three or more items for the purpose of identification; some offices require, as an additional precaution, submission of a postcard which has been mailed to the legal address of the individual concerned and which must be presented at the time the service is requested. This trend is accepted and followed by private concerns such as insurance companies, banks, etc. as well. Items usually required for identification are:

- a. "Koseki" (Family Register)
- b. "Jitsuin" (Seal)
- c. Automobile Drivers License
- d. Inhabitants' Certificate
- e. Rice Ration Book
- f. Health Insurance Certificate
- g. Private Identification Cards.

The inhabitants' certificate is issued by the mayor of the city, town or village to each inhabitant in his jurisdiction. The Rice Ration Book is a historically important document no longer extensively used as a basis of identification.

The Japanese believe that the "Koseki" system makes it virtually impossible to mistakenly issue an identification document to an individual who is either dead, missing, or for any other reason, is not the individual he claims to be. The sole exception is a case in which an individual falsely uses someone else's identity with that person actively cooperating.

Japan has a comprehensive set of laws which imposes penalties which should be real deterrents for crimes involving false identity. Of special interest are those crimes involving misuse of seals that are more severely punished than corresponding ones in which seals are not involved. Japan in 1974 recorded 500 cases of obtaining drivers licenses using false identity documents, and 854 cases of illegal use or altering of credit cards. A total of 4,607 cases of

falsification of documents were known to police. This incidence of 4.3 cases per 100,000 persons is considered low in comparison to other countries which provided similar statistics.

Brazil

Brazil uses a national identification document and is known to be in the process of establishing a centralized population register system.[4] The national identity document (Cedula) is a wallet-sized, laminated card containing a photograph and thumbprint as well as normal personal identification information and the assigned personal identification number. It is issued to all citizens 18 years of age or older except those possessing identification cards issued to civilian employees and military personnel of the Armed Forces by local identification offices operated by the Department of Public Security in each state. These offices are subject to the policy guidance of the National Institute of Identification, a division of the Federal Police. Aliens are issued permanent or temporary Alien Identity Cards very similar to the Cedula.

Births and deaths are registered by offices of Civil Registry which are established by Federal license on the basis of local need and population. Drivers licenses are issued by local offices of State Department of Transportation. There is no procedure at present for matching deaths and births. The establishment of the population register system should alleviate this problem somewhat.

Brazil operates under a uniform penal code which provides moderate penalties (with the exceptions of fines which have become ridiculously low due to inflation) for most potential misuses of identity documents. Brazil is in the process of changing these fines to a system in which the judge, within limits set by law, determines the value of fines in terms of multiples of the minimum daily wage in accordance with the financial condition of the guilty party. False identification is considered to be a normal concomitant to other primary types of criminal activity, and there are no statistics available on the extent of this problem.

SECTION V

SUMMARY AND CONCLUSIONS

This report provides a general overview of the problem of false identification in commission of criminal acts in selected foreign countries. It is based primarily on surveys made by the State Department through U.S. embassies abroad and by the International Criminal Police Organization (INTERPOL). Through these surveys and use of other sources of information, it has been possible to provide a reasonably comprehensive description of the false identification problem in twelve of the twenty-five countries on which significant information has been obtained. These twelve countries are mostly Western European or other highly developed countries with which the U.S. has extensive political, social and economic relations. This description is not necessarily representative of a worldwide situation, nor does it cover certain other countries such as Canada and Mexico with which significant common problems of false identity could be anticipated. The extent of the false ID problem in these nations, and the effectiveness of the countermeasures used, is based primarily on the perceptions of the respondents to the survey.

The practices and procedures for personal identification vary greatly from country to country. The countries surveyed tend to fall into one of the following three categories:

1. Countries with strong systems of population registration and personal identification. (Denmark, the Netherlands, Norway, Sweden and Finland).
2. Countries with no highly centralized systems for personal identification characterized by a considerable amount of independence at lower levels of government and little coordination between governmental activities. (Australia and the United Kingdom).
3. Countries which are intermediate between the above two extremes. (Argentina, Brazil, Columbia, France, West Germany, Greece, Japan, Spain).

Those countries which appear to have the least problems with false identification tend to use a combination of techniques designed to counteract each common method of misuse of identity documents. Some form of population registration system and thorough investigative procedures are used to minimize the possibility of a person obtaining

an identity document by use of false information or fraudulently obtained supporting documentation. The content of identity documents and techniques used for their fabrication are selected to make forgery or alteration difficult. Penalties against all common methods of misuse of identity documents, sufficiently severe to provide a real deterrent, are established by law.

The greatest emphasis is normally placed on the systematic use of population registration systems. These can vary from highly automated systems with central population registers to manual systems maintained at the local level. The essential ingredients of an effective system are:

- a. A single file containing significant information affecting the status of each registered individual.
- b. A positive determination of legal residence or domicile for each individual.
- c. Consistent use supported by law and practice of the personal file as a required reference for legal actions affecting status.
- d. A procedure for regularly updating and verifying the personal file both on an individual and a collective basis.

The prime motivating force behind establishment of population registration systems is administrative efficiency and assurance of equity in establishing tax and voting rolls, etc.; their value as a means of minimizing the problem of false identification is an essential by-product of their establishment.

A unique personal number is normally assigned to each registered individual. This number by itself is a powerful means of identification.

In most countries with population registration systems (and some without) a national identity document of some form is used. In these countries this document is normally the primary means of identification. Where a national identity document does not exist, there is a tendency for some other form of commonly used document (social security, national health insurance cards, etc.) to be used as a partial substitute. Drivers licenses, commercial identity cards, etc. are also used in varying degrees for general identification.

Three countries are known to use family registers, a document maintained by local officials in which all births, deaths, marriages, and other important status information are entered, as a fundamental basis for issuing identity documents.

The most common supporting documents used as a basis for obtaining identity documents are birth and marriage certificates.

Many countries tend to emphasize procedures for investigating and processing applications as a fundamental method for assuring the authenticity of identity documents. Procedures commonly used include requirements for applications to be reviewed at the local level where officials may have personal knowledge of the applicant's identity, careful comparison of statements on applications with data in the applicant's personal/family register, and mailing notifications to receive approved documents to applicant at his legal residence as indicated in his personal record files.

Personal identification practices, to be effective, must be suitable for the country involved. They can become effective only if accepted by the population and integrated into the administrative machinery of the country concerned. Generally, a relatively long time is required to institute and perfect the operation of new procedures.

Some consideration should be given to future expansion of the effort described in this report to create a more authoritative reference document. This effort could take the direction of:

- a. Expansion of the coverage to include more countries, particularly all those with which problems involving false identification could be anticipated (i.e., Canada, Mexico, etc.).
- b. Developing a detailed, country-by-country descriptive list of all identity documents commonly used together with suggested methods for assuring their validity.
- c. In-depth study of population register systems and their relation to the identification process.
- d. Determination of specific suggestions for international coordination to minimize the possibility of international crimes involving false identity.

ATTACHMENT A
INTERPOL QUESTIONNAIRE

I. INTRODUCTION

A. Methods used to gather data.

1. List surveys conducted, numbers and types of organizations.
2. List and describe other data sources.
3. List areas in which adequate data could not be obtained and why.

B. List areas which require further investigation or data gathering.

II. DESCRIPTION OF THE FALSE IDENTIFICATION PROBLEM

A. Kinds of transactions of interest to the Task Forces.

1. "Application" phase.

- a. List the types of documents applied for and give a general description of the application processes for each.
- b. List documents which are applied for and give an estimate of number of applications per year and the number falsely applied for.

<u>Document</u>	<u>No. of applications per year</u>	<u>No. of false applications</u>
-----------------	---	--------------------------------------

- _____
- c. For each type of document applied for, what types of identity documents is the applicant asked to produce? (If none are required, why are they not required?) Which of these are most frequently involved in false applications?

Document applied for _____.

<u>Identity Document</u>	<u>Check if requested of applicant</u>	<u>Check if frequently used in false I.D.</u>
1. Birth certificate	_____	_____
2. Social security card	_____	_____
3. Drivers License	_____	_____
4. Credit cards Retail-Travel Bank-	_____	_____
5. Employer I.D. card	_____	_____
6. Selective Service card	_____	_____
7. Military I.D. card	_____	_____
8. Military discharge papers	_____	_____
9. Immigration & Naturalization papers	_____	_____
10. Passport	_____	_____
11. References	_____	_____
12. None	_____	_____
13. Other-Specify	_____	_____

d. Is the authenticity of these documents verified with these sources as a part of the application approval process?

2. "Use" Phase

- a. Describe, in general, the ways applicants use documents issued to them.
- b. List the uses. For each use estimate the total scope of such use and the scope of fraudulent use.

<u>Use (List)</u>	<u>Total scope of use (Dollar volume, number of uses, or both, etc.)</u>	<u>Scope of fraudulent use (Same units)</u>	<u>Percentage of fraudulent use</u>
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

- c. For each document and type of use, indicate what supporting identification documents, if any, are simultaneously requested of user:

Type of document _____.

Use _____.

<u>Identity Document</u>	<u>Check if requested</u>
1. Birth certificate	_____
2. Social Security Card	_____
3. Drivers License	_____
4. Credit Card	_____
Retail-Travel-Bank	_____
5. Employer identification card	_____
6. Selective Service Card	_____
7. Military Identification card	_____
8. Military Discharge Papers	_____
9. Immigration & Naturalization Papers	_____
10. Passport	_____
11. References	_____
12. None	_____
13. Other - Specify	_____

- d. In all of the fraudulent uses of each type of document what fraction can be classified as:
1. Altered _____
 2. Counterfeit _____
 3. Imposter _____
- e. Describe which false identification techniques are most common and least common, and which are the most and least successful and why?
- B. Give profiles of users of false identity documents.
1. Age
 2. sex
 3. race
 4. education level
 5. prior criminal record (including types of crimes)
 6. employed or unemployed
 7. residence (rural, suburban, urban)
- C. Give other false identity "use" data.
1. Principal geographical areas
 2. Season of year
 3. State of national or regional economy
 4. Other patterns of use.
- D. Give profiles of victims of criminal use of false identification as in B above. Which victims is it used most and least successfully against and why?
- E. What is the social, psychological, political or other cost of the obtaining and use of false identification?
- F. What is the impact of the use of no identification where it might be used as a tool to deter crime?

- G. How many false identification investigations, prosecutions, and declinations were there? Include data for prosecutions.
- H. Total estimated administrative costs, including, but not limited to salaries, benefits, transportation, overhead, etc., for the purpose of investigation, prosecution and recovery activities: break out costs for cases for the years 1970-1974 if data is available.
- I. Please attach copies of the forms used for the referral of the fraud cases and reporting of fraud investigative activities.

III. COUNTERMEASURES TO CRIMINAL USE OF FALSE IDENTIFICATION

- A. For each document which you issue, list the countermeasures which are presently employed or about to be employed, together with specific estimates of cost and effectiveness of each countermeasure.
 - 1. For the "application" phase.
 - 2. For the "use" phase.
- B. Preliminary Recommendations - List your preliminary recommendations for combating the obtaining and use of false identification.

For each document which you issue, list additional countermeasures which could be taken and evaluate each as cost, effectiveness, and other relevant criteria such as acceptability to the public.

IV. OTHER COMMENTS

V. ATTACHMENTS

Please attach all relevant supporting data, including:

- a. Synopses of selected criminal false identification cases.
- b. Copies of statutes, if any, that set forth penalties for individuals who provide others with false identification documents. What efforts are made to enforce the provisions of such statutes?
- c. Copies of statutes, if any, that prevent or limit verification and reporting of false identification to law enforcement officials (e.g., confidentiality statutes prohibiting disclosure of information by employees to law enforcement officials).

ATTACHMENT B

STATE DEPARTMENT QUESTIONNAIRE

1. Is there a standard identification document in use in your country?
2. If the answer to #1 is affirmative, describe briefly the procedure used to issue the document including the method of establishing identity, the type of documents issued, and the agency responsible for the task.

NOTE: If possible, furnish copies of laws and regulations, application forms, and the document or documents issued.
3. If the answer to question #1 is negative, state how a person's identity is generally established in your country.
4. Does the identification system differ with regard to citizens, resident aliens and temporary aliens? If so, describe the system used for each category.
5. What is the primary issuing agency for:
 - a. Birth Certificates
 - b. Death Certificates
 - c. Drivers' Licenses
6. Is there any system at this time for matching death certificates with birth certificates? If so, please describe in detail, and estimate its effectiveness in preventing fraudulent use of birth certificates.
7. What are the present legal penalties for fraudulent obtention or use of birth certificates, drivers' licenses, and other identity documents.
8. What is the present legislative trend or attitude regarding penalties for fraudulent use of personal identity documents?
9. Is there any mutual cooperation between this nation and other nations regarding enforcement of legal penalties, and investigation of fraudulent obtention or use of identity documents?

10. Is there any legislation presently in force similar to our Privacy Act which would protect the privacy of personal information given to obtain personal identity documents? If so, please describe.
11. While statistics would be extremely useful to our Committee, it is realized that these may be impossible to obtain. It would be helpful however, if you could relate the circumstances of any widespread practice or any important cases which had wide publicity.

COMMENT: If it would be helpful in obtaining this information, you may inform the local government that the Committee will be pleased to furnish it with its final report which will include the scope of the problem as well as recommended solutions.

Please translate any information which is given other than pamphlets, laws and regulations.

ATTACHMENT C

EXTRACT FROM FRENCH CRIMINAL CODE

Article 153 (Ord. nr 58-1298 of 23 Dec. 1958). "Whosoever counterfeits, falsifies or alters permits, certificates memorandum books, cards, official reports, receipts, passports, laissez-passer or other documents issued by public administrations in order to verify an identity or a position, or to grant an authorization, will be punished by imprisonment of from six months to one year and fined from 1500 to 15000 francs."

The guilty party will also be denied the rights mentioned in Article 42 of this Code for at least five years and with a maximum of ten years counting from the day of his conviction.

The attempt will be punished in the same way as the completed action.

The same punishment will be applicable to:

1. He who made use of counterfeit, falsified or altered documents.
2. He who uses one of the documents described in the first paragraph when the data provided by the subject have become incomplete or incorrect.

Article 154 (Ord. nr 58-1298 of 23 Dec. 1958) "Whosoever unduly has issued to himself, or attempts to have issued any of the documents described in the preceding article, either by making false statements, by taking a false name or position, or by furnishing false information, certificates or affidavits will be punished by imprisonment of from three months to two years and fined from 500 to 5000 francs."

The same sentences will be applied to he who has used such a document, either obtained through the aforementioned conditions or made out in a name other than his own.

The official who issues or causes to have issued one of the documents covered by the preceding article to a person that he knows does not have rights to it, will be punished by imprisonment of from one to four years and fined from 1500 to 15000 francs, without prejudice to more severe sentence he might be given through application of articles 177 and those following. The guilty party might also be denied the rights mentioned in article 42 of this Code for at least five years and with a maximum of ten years from the date of his conviction.

LIST OF REFERENCES

1. Record file of replies from U.S. embassies in twelve countries to the Department of State's Operations Memoranda of January 22 and March 26, 1976, subject: "Information for Federal Advisory Commission," maintained by the office of William E. Duggan, Deputy Director for Legal and Security Affairs Passport Office (PTT/U). Duplicate working file at The MITRE Corporation, Bedford, Massachusetts.
2. Record file of replies from INTERPOL offices in sixteen foreign countries to letter dated, 15 July 1975, Number 100, Survey 55, maintained in the office of Louis B. Sims, Chief, International Criminal Police Organization, USA, National Central Bureau, Department of the Treasury. Duplicate working file at The MITRE Corporation, Bedford, Massachusetts.
3. "International Symposium on Automation of Population Register Systems," Information Processing Association of Israel, Volume I, "Proceedings," Jerusalem, Israel, 25-28 September 1967.
4. 1971 Fall Joint Computer Conference, November 16-18, 1971, American Federation of Information Processing Societies, Conference Proceedings, Volume 39.

APPENDIX D
SPECIAL STUDIES

Personal identification in the United States is based primarily on documents organized and issued at the state and local level. Birth certificates and driver's licenses are the most common of these documents. The FACFI has made major recommendations to the states for the improvement of their birth certification and driver licensing systems; however, detailed implementation plans for these recommendations – providing worked-out examples and cost estimates for the states – were felt to be highly desirable. As part of its mission to provide assistance to state governments, the Law Enforcement Assistance Administration (LEAA) funded the MITRE Corporation to develop programs for putting FACFI's recommendations into action. These programs are described in Appendices D1 through D3, which deal, respectively, with birth certification, correlation of birth and death records, and driver licensing. Additional detailed recommendations for increased security of driver's licenses (and state-issued ID cards) are contained in Appendix D4, which was written by Ronald O'Connor of the Polaroid Corporation.

APPENDIX D1

**A PLAN FOR REDUCING THE ABUSE
OF BIRTH CERTIFICATION**

**L.B. Collins
T.P. Kabaservice
C.F. Lowell**

**The MITRE Corporation
Bedford, Massachusetts**

June 1976

This project was supported by Contract Number J-LEAA-014-76 awarded by the Law Enforcement Assistance Administration, U.S. Department of Justice, under the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Points of view or opinions stated in this document are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice.

TABLE OF CONTENTS

<u>Section</u>		<u>Page</u>
	LIST OF ILLUSTRATIONS	D-5
I	INTRODUCTION	D-7
II	CONCLUSIONS AND RECOMMENDATIONS	D-9
	Protection Against Imposture	D-10
	Protection Against Counterfeiting and Alteration	D-19
	Protection Against Misuse	D-25
III	DISCUSSION OF PROBLEMS IN INSTITUTING CHANGE	D-29
	Access to Vital Statistics Data	D-29
	Application	D-30
	Forms	D-31
	Use and Misuse	D-32
ATTACHMENT I.	MODEL STATE VITAL STATISTICS ACT	D-35
ATTACHMENT II.	PROPOSED AMENDMENTS TO MODEL ACT	D-55
ATTACHMENT III.	MODEL STATE VITAL STATISTICS REGULATIONS	D-61

LIST OF ILLUSTRATIONS

<u>Figure Number</u>		<u>Page</u>
1	Model Vital Statistics Office	D-14
2	A Model Application Form for Birth Certification	D-18
3	Sample Form and Format for Certified Copy of Birth Certificate	D-20

SECTION I

INTRODUCTION

The Federal Advisory Committee on False Identification (FACFI) was created to study, characterize, and propose solutions to the false identification problem. The FACFI has identified the birth certificate as a prime source from which to establish a false identity and secure further false IDs. This problem has been characterized by FACFI and a number of solutions proposed.

The Law Enforcement Assistance Administration (LEAA), a member of FACFI, sponsored a study by The MITRE Corporation to investigate further those FACFI proposals directed to the filing and issuance of birth certificates and to help states improve their systems for the issuance and protection of birth certifications. Detailed plans for implementing the FACFI recommendations with respect to birth certifications are contained in this report. The elements of the plan are feasible and do not require either massive expenditures or severe dislocation of state operations. The proposed program should serve the legitimate interests of both state government and the private citizen.

The birth certificate is frequently used to establish a false identity. Since it can be used to obtain a variety of genuine identification documents in a false name, it is considered a "breeder" document. As outlined by Task Force 5 of the FACFI Committee (See Appendix A5 of the FACFI Final Report), the false ID problem associated with birth certificates can be described as the result of two fraudulent acts:

- Application fraud, in which a birth certificate is requested by an imposter claiming to be the person described on the certificate, and
- Use fraud, in which the imposter then uses the certificate as "proof" of identity.

Birth certificates can be applied for by mail or obtained in person at state, city, or county offices. Procedures, issuing authority, amount of information, and type of information required to obtain a certified copy of a birth certificate vary greatly from state to state. Statutes and procedures limiting access to the vital records themselves are not consistent. In many instances, no identification is required for access or to obtain a certificate. As a minimum, the information needed in the application is that

necessary to locate the document. At the other extreme, procedures and information are required which will allow for the determination that the requesting individual has a right under state law to obtain the certificate and that the individual is indeed properly identified. The application process further varies from state to state in that some states issue certificates only at a single state level while others have many points of issuance throughout the state.

A birth certificate is commonly and legally used to establish age, citizenship, and parentage of the individual to whom the certificate pertains. This is used to claim Social Security benefits, to obtain passports, and is sometimes necessary for school entrance, to secure employment, and for commercial or business purposes when one or all of these facts are required. Task Force 5 of the FACFI has reported that the total utilization of the birth certificate as an identification document is impossible to estimate. In the majority of cases, a birth certificate is considered a primary identification document in that no additional documentation is required. Since the certificate contains no information that would link the person it describes to the bearer of the document, it can easily be used by an imposter. This fact alone makes the birth certificate a document of major concern.

MITRE has found that at least three versions of certification (certified copies) of the birth certificate are issued by states. They are:

- A full photographic or typewritten version of the complete birth certificate.
- A "short form" version of the birth certificate.
- A "birth card" version of the birth certificate.

Intended use of these forms varies from state to state. Federal guidelines for form utilization do not exist. In some states, for example, the "birth card" is not considered a certified abstract of the birth certificate. The "short form" version is frequently viewed as a less personalized version of the full copy and may be used interchangeably. All states do not utilize all forms.

It appears clear that the fraudulent use of birth certificates can be effectively reduced only by simultaneously addressing:

- The application process for birth certification.
- The form itself.
- The use of the birth certificate as an identification document.

SECTION II

CONCLUSIONS AND RECOMMENDATIONS

The need exists for a systematic and consistent approach to limiting the false use of birth certificates. Three primary areas of birth certificate utilization must be addressed:

- Obtaining the birth certificate of another person through false pretense.
- Counterfeiting or altering a birth certificate.
- Using a birth certificate fraudulently.

If steps are not taken in each of these three areas to decrease such false use of the birth certificate, fraudulent users will simply choose the method not addressed. In addition, an overall legal context for penalizing the false use of birth certificates must be instituted, which should diminish false use by increasing the legal risk of such activities. To effectively counter and penalize this activity, it is recommended that:

1. Legislation be enacted to restrict access to vital records.
2. The physical security of vital records be assured.
3. Control over issuance of birth certification be improved.
4. Application forms for birth certification be standardized.
5. Certificate forms utilize unique, controlled safety paper with special printed identifiers.
6. Full certified copies contain standard information and format.
7. Blank forms be controlled and pre-numbered.
8. The legal status and level of security for short forms and birth cards be standardized.

9. States adopt federally recommended, issued and regulated standard certificate forms.
10. Direct agency to agency interchange of data (to verify facts of birth) be encouraged, i.e., vital statistics office to passport office, vital statistics office to Social Security, etc.

Each of these recommendations is discussed in detail in this report and proposals are given for their implementation. Problems that may arise from their implementation are also outlined.

PROTECTION AGAINST IMPOSTURE

In this section recommendations are made pertaining to imposture, i.e., the presentation of a birth certificate by an individual falsely purporting to be the documented individual. This section is concerned specifically with the misuse of a genuine document obtained by false pretense. Specific problems related to "false" documents - counterfeited or altered - that either create a false identity or allow assumption of someone else's identity are discussed in subsequent sections.

Vital records are a peculiar form of record; they are neither completely public nor completely private. In a sense, they are a public record of a private event. They do not share the inherent personal privacy of, for example, a medical record; at the same time they are not a record of "public business" to which the public is entitled, nor a record of information collected and recorded by a public agency. They have been held by the courts to be "public documents of a privileged nature." The statistics derived from such record are, however, public information. Birth certificates also contain a confidential section containing medical information and personal family background data. Access to this record could disclose illegitimacy of registrant, birth of older illegitimate children to same mother, birth defects, or maternal venereal disease. It should be made clear that in all discussion of vital records, the confidential section of the record is privileged and is not included in normal disclosure and copying procedures. It appears that the value of total and uncontrolled public access to vital records is outweighed by the negative impact on society and the individual resulting from misuse of such records.

The potential for misuse lies not only in the use of birth certificates for establishing identity, but also in the obtaining of data from other records to use in false application for birth certificates. For example, infant death records can be used to find birth dates and other facts needed to apply for birth certifi-

cates of dead individuals, while marriage records can be used to buttress false claims for insurance, Social Security benefits, and others. For this reason, access to all vital records must be controlled if misuse is to be minimized.

Freedom of Information (FOI) laws have been passed by the Federal government and many states granting public access to public records. In most cases, these laws permit any person to obtain a copy of any record, except as excluded by other statute. Vital records may or may not, according to local variation in the law and local adjudication, be included as open public records. If misuse of vital records is to be curbed, it is clear that statutory action is necessary where not already applied. Current statutes must be modified to apply restrictions to all vital records, or state legislatures must pass comprehensive vital statistics statutes.

Protection against imposture will rely on implementation of recommendations regarding:

- Statutory basis for access control
- Physical access to records
- Centralized state issuance of birth certificates
- Information requirements for application

Statutory Basis for Access Control

Recommendation

Legislate action to restrict access to vital records (FACFI Proposed Solution No. 1).

Proposal

State legislatures should pass new legislation or amend existing statutes to restrict access to vital statistics records. Such restrictions should include the following:

1. Provision of privileged status for birth records less than 100 years old and for death, marriage and divorce records less than 50 years old.
2. Issuance of certified copies of records only to individuals having a "direct and tangible interest" in the specific records.
3. Limiting access to privileged records to employees of the recording agency.

4. Regulation by the state registrar of use of vital statistics for research purposes.
5. Provision of appropriate penalties for misuse of privileged records.

These provisions are contained in the most recent version of the Model State Vital Statistics Act. This Model Act which was developed by a panel of state vital registration officials under the sponsorship of the Department of Health, Education and Welfare, is included in its entirety on Attachment I of this report. Model state regulations to implement the provisions of the Act are included in Attachment III.

Impact

1. Most states presently employ some form of restriction of physical access to vital records. The suggested Model Act and regulations, if enacted by all states, would provide a uniformly privileged status for records that are likely to be abused for false identification. The recommended restrictions will normally be acceptable to the general public.
2. Of special importance in the control of access to birth records is the fact that the original records contain confidential sections which can be disclosed only under very restricted circumstances. This information must certainly be protected from access by "casual browsers" or by investigators who do not have rights to the confidential data in the record.
3. Genealogists and other researchers may be given access to records of a specified age, i.e., birth records older than 100 years or death and marriage records older than 50 years.
4. State legislatures considering changes to existing statutes or a new comprehensive statute would be aided by a concise statement of the problem of false identification, the cost to society and the state, and the relationship to access to vital statistics. The need for vital records protection should be clearly stated and model legislation suggested. The FACFI report(s) can be used to aid this process by providing information for an "information kit" which could be communicated to state legislatures by appropriate in-state agencies seeking new legislation.

Physical Access to Records

Recommendation

Assure physical security of vital records (FACFI Proposed Solution No. 2).

Proposal

States or other registries that do not currently have adequately secure facilities and procedures should adopt appropriate measures to meet or approach a common standard. It is recognized that:

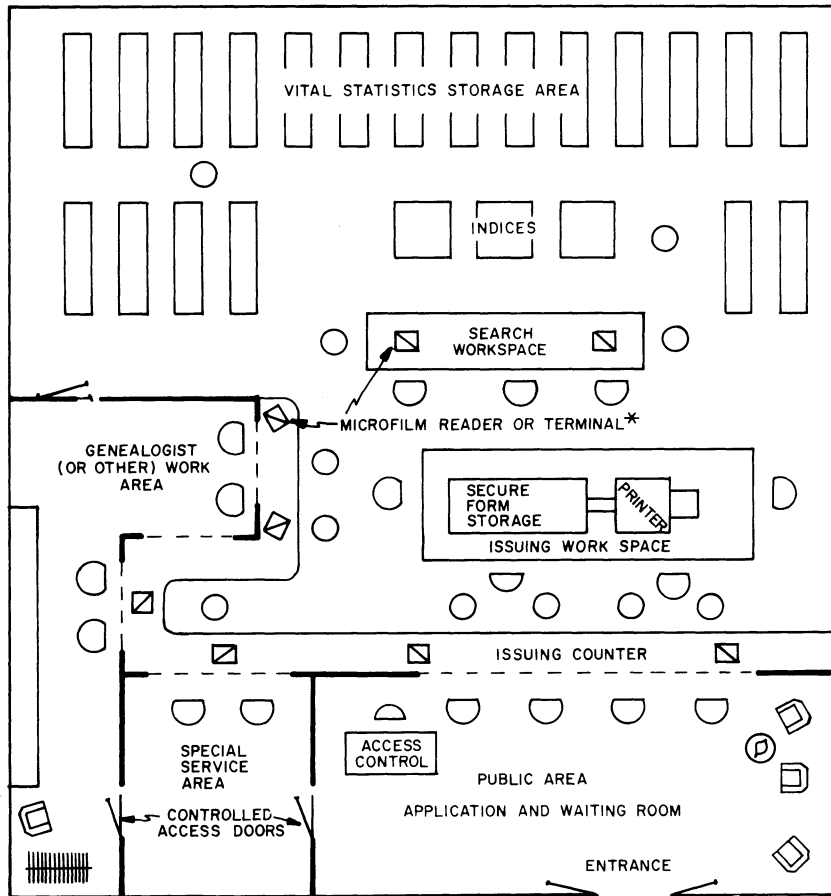
1. Many registries have already implemented appropriate procedures and facilities,
2. Each registry's facilities must be designed to meet local conditions and existing local structures.

Within these limits, it is proposed that registries adopt a physical layout functionally similar to that shown in Figure 1. Within this facility, it is proposed that:

1. The general public be limited to the area outside the counter and their requests be served completely by the record clerks.
2. A special room service cases in which a clerk may wish to discuss special problems with an applicant.
3. A special room be made available to genealogists and other researchers. Preferably, they would request records from the clerk and work on them in this room. This area can be used for access to records which have become public by virtue of age.
4. Secure storage facilities be maintained for off-hours storage of certificate forms and any other sensitive material.

Impact

1. Alteration of facilities may require some additional expense; however, the total cost should be reasonable.



* FOR MICROFILM OR COMPUTER RECORDS OR INDICES

IA-48,611

Figure 1. Model Vital Statistics Office

2. Since users may be irritated at changes in their access to records, every attempt should be made to educate them as to the reasons for changes and the importance of assuring the legitimacy of record use. The public should be assured that no barriers are being placed in the way of obtaining legitimate record copies, and research or other interests should be aided in obtaining legitimate access.

Centralized State Issuance of Birth Certificates

Recommendation

Improve the control over issuance of birth certificates by centralizing issuance at the state registrar or by strict state regulation of issuance at local offices (FACFI Proposed Solution No. 47).

Proposal

Vital records are traditionally kept at both state and local (county, township, city) registries; in many states, certified copies are issued from both locations. In order to provide protection against issuance of birth certificates to improper parties, it is proposed that all issuance of certified copies be made by the state registrar's office either in person, or by mail.

Alternatively, the local offices would continue to issue certificates but under strict regulation and control by the state registrar, who would supply forms, issue regulations, and audit procedures. At present, many states have strict regulations for the issuance of birth certificates that apply to all issuing offices. However, it is difficult to properly control such issuance and assure that regulations are being met when as many as 1,500 local agencies are involved, each with a great variety of size, volume of applications, and professionalism of personnel. In many states, the local agencies do not use the same forms as the state, or each other, and may not follow the same rules for application. The most effective solution appears to be centralized issuance.

Impact

1. In many states there is a tradition of issuance by local county or town officials. In addition to the convenience afforded to the applicant by local application and issuance, there may be a perception that both prestige and income are attached to the right of local issuance (in fact, the real cost may be higher than the income in small

offices). To some extent, this local function can be retained by having application forms available at local registrars as well as health departments and clerk's offices. These offices could assist the applicant in proper preparation of the application.

2. Centralized issuance will probably be slower than local issuance; if quick service is of sufficient value in a given area, local issuance with state control may be more suitable.
3. Centralized issuance may require legislation in many states, which could be proposed simultaneously with a request for statutory authority to restrict access to vital statistics records. In this way a consistent "case" can be presented to the legislature.
4. It must be emphasized that no procedures for protecting the integrity of birth certificate are going to work if they can be circumvented simply by dealing with local agencies that are not bound by regulations and procedures employed at the state level.

Information Requirements for Application

Recommendation

Institute national standard application forms for birth certification (FACFI Proposed Solution No. 58).

Proposal

Most agencies presently issuing birth certificates honor applications containing only minimal data (for example, name of person on certificate, place of birth and data of birth). Imposters are able to locate such limited information easily. In particular, the fraudulent applicant need only obtain data from a death notice, newspaper article, or other easily available source, to fill out an application or mail an unsigned letter request for a certified copy. We propose that a standardized application form for birth certification be adopted that includes:

1. Full name at birth
2. Date of birth
3. Sex
4. Place of birth (town, hospital)
5. Information on father (full name, place of birth)

6. Information on mother (maiden name, place of birth, street address at time of birth).
7. Information on person making request (name, address, signature).
8. Purpose for which copy is requested.
9. Applicant's relationship to person named on certificate.

It is proposed that parents' full names, parents' places of birth, and mother's maiden name, be included on any application for a certified copy of birth record. Such data is difficult to get and the total package of data is unlikely to be known to another person not related to the individual in question. States should honor only those requests containing a sufficient subset of information, i.e. more than that which could be readily obtained by any individual from a source such as the obituary columns. The request should, however, always clearly identify the requestor and his relationship to the person whose certificate is being requested.

The request can be returned to the applicant if there are mistakes or completely insufficient information. If the applicant cannot supply all the required data, he can be handled as a special case at the registrar's office or possibly at local offices. If he can satisfy the clerk of such office, in person, as to his identity, the clerk would process the application with a special identity voucher section allowing reduced information. Mail applications would be restricted to the required data. It is envisioned that standard forms could be made available at local health departments, county clerks, city halls, etc. The proposed format is given in Figure 2. A list of addresses of issuance offices in all states should be supplied at each such location.

Impact

1. Many applicants may not be able to supply all the required information. This may result in an increased volume at rejected applications; on the other hand, many applications are presently rejected because of insufficient information. The standardized application may reduce such errors.
2. The use of a national standard form will ease the problems of a resident of one state applying for a certificate from his natal state. Local offices in the home state will have the proper form, be familiar with application requirements, and will know the proper address for application (from the list of state issuance offices).

REQUEST FOR COPY OF BIRTH CERTIFICATE

Mail request with fee or bring to:
 _____ STATE DEPT. OF HEALTH
 (name) _____
 Public Health Statistics Section, Room _____
 _____ (address)

PLEASE PRINT

I. BIRTH CERTIFICATE OF:

FULL NAME AT BIRTH		FATHER'S FULL NAME		FATHER'S BIRTHPLACE (Town)
DATE OF BIRTH	SEX	MOTHER'S MAIDEN NAME		MOTHER'S BIRTHPLACE (Town)
PLACE OF BIRTH (City, County, State, Hospital)				


II. PARENTS OF PERSON NAMED IN BIRTH CERTIFICATE

RESIDENCE OF PARENTS AT TIME OF THIS BIRTH		NUMBER OF COPIES WANTED
Your Name _____ (No. and Street)		FEE ENCLOSED
Your Address _____ (Town, State) (Zip Code)		(See Fee Schedule) \$

For the protection of the individual, certificates of vital events are not open to public inspection.

The following must be completed in order to permit this office to comply with the request.

RELATIONSHIP TO PERSON NAMED IN CERTIFICATE (e.g., parents, attorney)	FOR WHAT PURPOSE DO YOU NEED THIS COPY?
---	---

Your Signature 

Warning: False application for a birth certificate is punishable by up to five years in prison and/or \$10,000 fine.

Figure 2. A Model Application Form For Birth Certification

3. This proposal is closely tied to more restrictive legislation since, if no restriction is placed on issuance of certified copies, or access to original records, then an application form cannot insure that the applicant is properly identified.

PROTECTION AGAINST COUNTERFEITING AND ALTERATION

This section contains recommendations pertaining to the problem of false documents that are either falsely created (counterfeited) or altered. When the procedures to obtain genuine certificates are tightened, it is likely that counterfeiting and alteration will increase. Methods are proposed that will protect against counterfeiting and alteration of a "certified copy" of a birth certificate. Figure 3, which is a prototype certified copy derived from a form developed and manufactured by the American Bank Note Company for the Commonwealth of Virginia is included here for reference. Information content was derived from certificate data utilized by the Commonwealth of Virginia and from the U.S. Standard Certificate of Live Birth (Public Health Service form PHS-796). It must be noted that Figure 3 is for illustrative purposes only; many of the safeguards proposed are, by design, not possible to duplicate.

Counterfeiting and alteration of certified copies of birth certificates can be reduced by implementing the recommendations discussed below, which are offered here as a package. They are in many respects integral to and dependent upon one another; therefore, an overall design is necessary. Any implementation of a subset of these recommendations should be closely examined to assure that the integrity of the entire document still stands.

Proposals in this section relate to both the full certified copy of a birth certificate and to abbreviated forms, which are to be considered as certified copies.

Creating "Secure" Certified Certificate Forms

Recommendation

Prepare certificate forms utilizing unique, controlled safety paper with special, printed identifiers (part of FACFI Proposed Solution No. 2).

Proposal

In order for security features to be applied to all certified certificate forms, it is proposed that:

COMMONWEALTH OF VIRGINIA

— CERTIFICATE OF LIVE BIRTH —
DEPARTMENT OF HEALTH — BUREAU OF VITAL RECORDS AND HEALTH STATISTICS

(Name of State) _____ (Address) _____

ABNCO TEST

1. AREA NUMBER		2. SEX OF CHILD	
3. NAME OF CHILD		4. DATE OF BIRTH	
5. NAME OF HOSPITAL OR INSTITUTION OF BIRTH		6. COUNTY OF BIRTH	
7. CITY OR TOWN OF BIRTH		8. STREET ADDRESS OR NO. OF PLACE OF BIRTH	
9. STATE (OR FOREIGN COUNTRY) OF BIRTH		10. COUNTY OF RESIDENCE	
11. CITY OR TOWN OF RESIDENCE		12. STREET ADDRESS OR NO. OF RESIDENCE	
13. FULL MAIDEN NAME OF MOTHER		14. FULL NAME OF FATHER	
15. AGE OF MOTHER		16. AGE OF FATHER	

SPECIMEN

17. CERTIFY THAT THIS CHILD WAS BORN ALIVE ON THE DATE AND HOUR STATED ABOVE

18. SIGNATURE OF ATTENDANT

19. ADDRESS OF ATTENDANT

20. DATE RECORD SIGNED

21. REGISTRAR'S SIGNATURE

22. DATE RECORD FILED


*On Abbreviated Certified Copy, Not Applicable. Must Be Typed In

This is to certify that this is a true and correct reproduction of the original record filed with the Bureau of Vital Statistics, Virginia Department of Health, Richmond, Virginia.

Deane L. Huxtable
DEANE HUXTABLE, State Registrar

ANY REPRODUCTION OF THIS DOCUMENT IS PROHIBITED BY STATUTE. DO NOT ACCEPT UNLESS ON SECURITY PAPER WITH SEAL OF THE BUREAU OF VITAL STATISTICS CLEARLY AFFIXED. Section 32-353.27, Code of Virginia, as Amended.

DATE ISSUED



DEPARTMENT OF HEALTH — BUREAU OF VITAL RECORDS AND HEALTH STATISTICS

Figure 3. Sample Form And Format For Certified Copy of Birth Certificate (derived from form used by Commonwealth of Virginia).

1. Forms be prepared on special "safety" paper.
2. Unique "safety" features be utilized and utilization limited.
3. Certified forms with special identifiers, hidden monograms, and identifying raised borders be preprinted.

All certified copies of birth certificates should be prepared on paper that contains "safety" marks that are difficult to alter or reproduce. These marks are in the background area of the sample form in Figure 3. Alteration is made difficult by the fact that any attempted alteration will mask or alter the "safety" features. Counterfeiting would require complete duplication of the "safety" features as it is recommended that the paper utilized not be made available except for the purposes of certified birth certificates. Cost of this paper is only a few cents more per sheet than that of ordinary paper. Some states presently use only ordinary paper for these forms, which allows the name of a person to be "whited out", the blanked form reproduced, or a false name appended. While "safety" features are an aid in preventing counterfeiting, utilization of this paper might increase attempted counterfeits because alteration would be so easily detectable.

Because safety paper is presently available from many sources, a unique safety paper should be used for the production of certified copies of birth certificates and its production should be controlled. Uniqueness aids in verification at the point of inspection and could be made extremely cost-competitive by the implementation of a national standard. Limited utilization and availability makes counterfeiting difficult.

Certified copies of birth certificates should be prepared on preprinted forms that incorporate unique printed features. Preprinted forms should utilize special identifiers, hidden monograms, and raised borders produced by sophisticated reproduction techniques, and hidden image printing techniques should be used in selected areas. Selected legends and margins should be comprised of closely spaced lines, differing color intensities, and identifying monograms. Intaglio printing that will produce selected images in relief should also be utilized. Raised seals or multi-colored dry stamp seals may be added at the time of certification. Salient and important features can readily be incorporated to aid in the inspection or verification process.

Referring to Figure 3, special identifiers are visible in the form of the seals at the top and in the center, etc. Hidden monograms, which cannot be reproduced here, appear in the top left and right circles; on the original they may be viewed only at oblique angles.

Raised printing is used for the closely spaced lines comprising the design in the border area. Differing color intensities are used on the printed form.

There is little uniformity from state to state in present birth certificate forms insofar as safety features and identifiers are concerned. Forms vary from those that are extremely simple to those that approximate the recommended form shown in Figure 3. While costs of a few thousand dollars would be incurred in the initial set-up for these certificates, they could be spread over a large number of applicants. For those states presently using preprinted forms, this recommendation does not appear to appreciably increase the per-unit or per-volume costs. For states presently using simply prepared forms, per-unit costs may be approximately 25¢.

Impact

1. The introduction of safety features and unique identifying characteristics into the certified birth certificate forms will increase the probability of attempted form theft. This concern is discussed under the section on controlling forms.
2. When a person requests a birth certificate, he receives a certified copy which is derived from the original official copy. The copy which he receives may be prepared by manual script or printing on a form, a Xerox copy of the original, a microfilm reader output of the original, or by computer printout. The proposal contained herein appears compatible with these methods of certified certificate issuance with the possible exception of methods presently used to obtain certificates from a microfilm reader output. Where a certificate so obtained is photographic in nature, the safety features proposed cannot be used. Photographic copies are easily altered by photographic methods. Compatibility with our proposal is possible by introducing a Xerox-type copying procedure of an illuminated microfilm copy. Xerox machines exist which are compatible with our recommended form and capable of accepting microfilm source input. Roll-fed or card inputs may be used at a cost of from 4¢ to 6¢ per hard copy output.

Creating Uniformity in Certificate Data

Recommendation

Prepare certified certificates using standard information content and format (part of FACFI Proposed Solution No. 2).

Proposal

Use format and information such as that shown in Figure 3 for all certified copies of birth certificates. The following 11 items should appear on any form issued as a certified copy of a birth certificate:

1. Certificate number (Birth Number)
2. Full name of Child
3. Sex of child
4. Date of birth
5. Name of hospital
6. County and state of birth
7. City or town of birth
8. Street address of place of birth (if not hospital)
9. Date filed
10. Registrar's signature
11. Date of certification

The following additional information could be contained in the full copy:

1. State or foreign country of mother's residence
2. County of residence
3. City or town of residence
4. Street address of residence
5. Full maiden name of mother
6. Age of mother
7. Mother's place of birth
8. Full name of father
9. Age of father
10. Father's place of birth
11. Informants signature
12. Attendants certification

Confidential information such as race, education, birth order, medical data, etc., is not proposed for any certificate copy. The abbreviated copy would be identical to the full certified certificate except that personal information on parents would be omitted. This proposal is compatible with the U.S. Standard Certificate of Live Birth, Public Health Service Form 796.

Because many different formats and information contents are presently used, it is extremely difficult to readily identify a fraudulent birth certificate. Standardizing to a minimum content will simplify the inspection procedure. The utilization of

a standard data format and information content is also mandatory to make optimum utilization of recommended preprinted form features.

Impact

1. The use of a standard data content and format reduces the variables from state to state. This allows for an easier inspection of certificates. However, widespread use of a single format might encourage counterfeiting attempts, so secure forms must be provided.
2. It should be recognized that general use of a standard format will probably occur gradually over many years. Copies will continue to be made from old original certificates that do not follow the standard format. However, even these copies can be made on secure forms.

Controlling Certificate Forms

Recommendations

Pre-number and control blank certificate forms (part of FACFI Proposed Solution No. 2).

Proposal

The introduction of security and uniqueness into the certified birth certificate form will increase the probability of attempted form theft. Pre-numbered and tightly controlled blank forms will help prevent theft and facilitate audit and control procedures.

At the present time not all states utilize a pre-numbered form; many of those that do report that pre-numbering and control have not significantly increased costs. Pre-numbered blanks are, however only as useful as the control and storage features implemented in conjunction with this feature. Numbered blanks must be controlled from the point of origin to state offices, and within these offices, up to the time of issuance to individuals. Relatively straightforward security procedures must be used to guard all blanks and appropriate auditing techniques must be used to detect and deter improper availability of forms.

Impact

1. Control of waste matter will require procedures and training of personnel; for example, copies created in error and discarded will have to be accounted for.

PROTECTION AGAINST MISUSE

Through improvements in application, issuance, and security of forms, the possibility is minimized of an individual's obtaining the genuine birth certificate of another person or attempting to counterfeit or alter documents. The likelihood of an agency accepting such documents must now be decreased. The following recommendations are concerned with protection against misuse of birth certificates. A concomitant effort must be made to legislate against fraudulent use; to clarify and define the status of birth certificate documentation in relation to other documents and to proper usage; and to educate personnel in the "using" agencies to understand and apply procedures related to the other recommendations made in this study.

It is recommended that Federal and state legislation be adopted to penalize misuse of birth certificate documents as discussed in the FACFI Final Report and as recommended in Attachments I and II of this report. Statutes should include statements such as:

"Any request in the form of an application, and/or such certified copy that is issued upon request in any form shall contain explicit warnings, conspicuously displayed, that willful and knowing falsification of information on an application, and/or will-full and knowing possession or use of a copy with knowledge that it contains such false information, shall be cause for criminal liability, etc., etc..."

Limitation of Certificate Forms

Recommendation

Standardize legal status of short forms and birth card use.
(Not discussed by FACFI.)

Proposal

Many states presently issue "short forms" of birth certificates, or "birth cards," or both. These forms generally contain less information than a full certified copy and sometimes are not certified. Their legal and practical status varies from state to state.* It is

*Based on a survey of "birth cards" conducted by Mr. Irvin G. Franzen, Department of Health and Environment, Kansas. He is also president of American Association for Vital Records & Public Health Statistics.

proposed that the short forms and birth cards, if issued, be standardized to be legally and functionally equivalent to a full birth certificate. The short form, an abbreviated version of the full certified copy, can be made using the same form used for the full copy (see Figure 3) but using the insertion "Not Applicable" in areas where parental information would appear.

It is extremely difficult to regulate or educate all "users" of birth certificates. In a situation where many forms of birth certificates are issued, the user tends to accept any form, even if that form is not a certified copy. State procedures vary regarding the degree of certification of the short form/card and the difficulty of obtaining one. The intent of this proposal is that any form issued by a state registrar that appears to be a certified copy is, in fact, certified and is issued only to persons meeting the requirements for receipt of a certified copy.

Impact

1. From the point of view of minimizing misuse of birth certificates, it would be desirable to eliminate both short forms and birth cards - i.e., to have only one, secure, well-known, controlled form of certificate. However, both abbreviated forms appear to be useful in various ways and have gained broad acceptance. Short forms may satisfy the information requirements for most uses of birth certificates without displaying data, such as parents names, place of birth, etc., which the holder may not want known to other parties. Short forms might reduce preparation time and cost, although significant net gain over a standard long form is doubtful if both forms are used. In view of the utility of the short form, and the argument that suppression of parental data is sometimes in the interest of the registrant, it is recommended that such forms continue to be used. However, the requirements for short-form certification should in all cases be the same as those for a full certified copy.
2. The very convenience of birth cards has led to their frequent use as personal identification. This is unfortunate, because like other forms of birth certification, the birth card contains no physical description of the person whose birth it verifies. Because of their size, and the tendency to carry them on the person, they are easily lost, stolen or loaned; when so obtained by another person the card can easily be misused. Birth cards are usually more expensive to issue than other types of cer-

tification. Because of those factors, it is recommended that their use be superseded by state-issued photo ID's such as the driver's license or "age-of-majority" card. These documents can be made more secure against use by imposters. Security and identification requirements for state-issued ID's are discussed in Appendix D3 of the FACFI Final Report. Recommended identification of applicants for these documents would include a certified copy of the birth certificate, plus independent corroborating evidence of identity.

Adoption of Federally-Supported Standard Forms

Recommendation

States adopt standard forms developed, regulated, and possibly issued by the Federal government (not discussed by the FACFI).

Proposal

Currently each state uses one form for a certified copy of a birth record and another for a birth card, if issued. In addition, within some states, local agencies issue different forms. It is proposed that the Federal government develop a standard, high-security form that would incorporate the needs of the various state registrars. This form could be produced under Federal funding and control and be made available to the states at nominal or no cost. A serial numbering system would provide both Federal and state control and auditing capability, although states could also apply a local numbering or control procedure. Paper stocks and printing of such forms should be under tight Federal security.

Impact

1. This proposal would obviously require modification of procedures in every state; however, it is felt that the extent and cost of these modifications would be minimal. In a questionnaire involving standardization of birth card forms, the bulk of responses by state registrars implied that the states would not object to such a standard form if it did not involve a Federal identification system.
2. States use a wide variety of methods for producing copies of birth records. It is assumed, however, that a form can be designed that is adaptable to all state requirements. One state is presently using a high-security form

which is intended for use both with electrostatic copy and computer output. If a state wished to hand print or type information onto such a form, it could overprint a format onto the standard form or have the form printed originally with such information.

3. It should be noted that the Federal government, as one of the principal "users" of state birth certificates (i.e., for passport issuance, immigration, military enlistment, employment, etc.) has an interest in supporting the states using standard forms.
4. As an alternative to this proposal, the Federal government could provide guidelines, standards, and technical support for nationwide standard forms, which would then be produced and controlled by each state.

SECTION III

DISCUSSION OF PROBLEMS IN INSTITUTING CHANGES

ACCESS TO VITAL RECORDS DATA

The basic problem in limiting the use of vital statistics information to prevent false identification is one of balance between three conflicting interests:

1. The private and public interest in maintaining "open" public records which might be subject to misuse by the state.
2. The public interest in preventing the misuse of public records by individuals attempting to establish a false identity.
3. The private and public interest in assuring that obtaining or issuing a certificate or copy is not too expensive in time or money for the issuer or issuee.

The spectrum of current practice regarding access is illustrated by two adjoining states - Massachusetts and Connecticut. In Massachusetts, the records are considered basically open and subject to public scrutiny and copy; in Connecticut they have been considered closed and issuance of a certified copy of birth records is controlled by statute. (Many states have adopted stricter statutes based on the Model Vital Statistics Act.) Connecticut procedures also illustrate another factor in the issue of public access; marriage and death records, previously considered closed, have been opened by the Freedom of Information Commission following Connecticut's new FOI statute. This case is being adjudicated, and the final outcome is unknown; however, specific legislation may be required if marriage and death records are to be protected, as birth records are, by statute.

A clear distinction must be established between verifying the existence and content of a birth record and obtaining a birth certificate, which can be used to obtain privileges and other official documents. If adequate vital records legislation has not been passed and it is necessary, under existing vital record and Freedom of Information (or other public access) laws, to provide record information to the public, it should be done using a special form for record verification, containing data necessary only to locate and identify the record and labeled, for example, VOID AS IDENTIFICATION

OF BEARER: FOR INFORMATION PURPOSES ONLY. It should be impossible to interpret this form as a birth certificate.

Misuse of birth certificates can also be reduced simply by decreasing the number of birth certificates in circulation, thereby decreasing the potential for stolen or altered certificates and allowing registries to apply more resources to processing each application. A move in this direction would be to institute procedures designed to reduce the need to obtain and show a birth certificate in order to become eligible for government services such as welfare, schools, pensions, employment, etc. If the need for birth record information in such cases could be filled by inter-agency transfer of information (from registrar to using agency) rather than requiring the applicant to produce a birth certificate, the number of certificates issued would be reduced. The potential for fraud, through use of false certificates in application for services, might also be diminished by taking the applicant out of the information transfer process. To protect rights of individual privacy, such transfer should require the written consent of the applicant to release the data. The form sent to the requesting agency should also be labelled to preclude its use as a false ID. In many states this form of data transfer may require institution of new procedures for reimbursing the registrar's office for time spent in search and data preparation; otherwise, income-producing applications may receive priority, delaying inter-agency transfers.

APPLICATION

Recommendations of improved methods of applying for birth certificates (to insure that the applicant is eligible) are clearly related to the legal basis for application. If the birth record is considered completely public and available to anyone, then the application need contain only enough information to identify the desired records; this is essentially the current practice in some states. If the statutory basis requires that certificates be issued only to the recorded individual (or some other specified person such as a guardian or attorney) then clearly the application must, in some way, provide assurance that the applicant is legally eligible.

The most practical way of assuring identity is to include on the application required data that can be known to the proper applicant but which would be difficult for an improper applicant to obtain. Such data can include: parents' place of birth, mother's maiden name, birth order, etc. The disadvantage of requiring such data is that a higher percentage of applications, particularly those submitted by mail, must be returned for additional data. Some legitimate applicants may not know or remember all the required data, and these cases

will require special handling. It has been suggested that minor errors or omissions in application be tolerated as long as correct information is supplied beyond that probably available to an imposter using newspaper accounts or similar records. An opportunity should be provided for individuals whose applications have been rejected to establish their eligibility for certification through a supplemental application or personal appearance at a local registry. Final recourse through a court order would still be available after a second denial.

FORMS

The basic thrust of recommendations concerning forms themselves is:

- To simplify the type and style of forms to a minimum number,
- To make the forms as secure as possible against alteration and counterfeiting, and
- To ensure that all users (agencies requiring vital record information) understand the appropriate uses and inappropriate uses (i.e., for identification) of birth certificates.

Secure, national standard forms will aid all of these purposes. Ideally, one certificate form could serve most users. If short forms and/or birth cards are acceptable to user agencies, and their convenience is considered worth the maintenance of multiple form types, then an approach that might be considered is to standardize the short form or card as the normal certificate form, with the addition of a standardized, secure supplemental or trailer form. The second form would be issued on request by the applicant only in conjunction with the normal form and would serve the applicant in special circumstances where additional information is required.

No technical problems are foreseen in applying a secure form to certificates produced by xerography, typewriter, computer printer, or other conventional reproduction methods. There is a special problem, however in copying microfilm data, where at present photographic processes are used. It is considered technically feasible, within the current state-of-the-art, to develop special output devices to convert a selected microfilm record into a printed or xero-graphic image on a secure form. A federally-sponsored development effort in this area might be appropriate.

USE AND MISUSE

It is not only fraudulent use of the birth certificate itself which is costly to society, but also its use in obtaining other documents which are of value to the perpetrator. The use of birth certificates in establishing identity is both confusing and controversial. Many state registrars protest, "the birth certificate is not an identity document" and will describe other agencies as "naive" in the way they use certificates. These statements have a large measure of truth; however, the reality is that birth certificates are used to establish identity, just as driver's licenses, over the protests of motor vehicle administrators, are used as identification cards.

Considering the processes of birth certificate application and issuance alone, all that can be done is to minimize the chance of an individual having a certificate which is false or improperly obtained. From the overall point of view of minimizing false identification, a program of clarification and education is necessary to prevent the misuse of birth certificates. User agencies at every level must be clear about exactly what the certificate means. Basically, until a superior overall identification system is developed (and that may not be feasible), the birth certificate simply certifies that the data on the document is true and relates to the named individual; it does not in any way indicate that the individual presenting the certificate is the named individual. It does not appear feasible, however, to include data that can be used to positively identify the individual. Fingerprinting at birth has been proposed but would certainly be cumbersome and is of doubtful reliability. Otherwise there is little to relate the presenting person with the baby whose birth is recorded on the birth certificate.

The capability of a using agency to properly evaluate the authenticity of a presented document can be considerably enhanced by the use of standardized forms, particularly if the standards are applied nationwide and combined with education in anti-counterfeit and anti-alteration measures. Certainly the present profusion of forms carrying varying degrees of certification aids the person establishing false identification.

ATTACHMENTS

MODEL ACTS AND REGULATIONS

In the attachments are several proposed model acts and associated regulations which illustrate the statutory base required for adequate protection of vital records against misuse. Many of these measures are currently in force in state statutes; however, a comprehensive set is in effect in only a few states. The attachments include:

I. Model State Vital Statistics Act, Proposed Revision, November 24, 1975. PHS Document No. 46817 (DRAFT)

This model has been prepared by a Technical Consultant Panel, composed of state vital registration executives and sponsored by the Department of Health, Education and Welfare. Intended to supersede Model State Vital Statistics Act of 1959, PHS Publication No. 794, 1960.

II. Proposed Amendments to Model Act

Prepared by the Department of Justice in 1974, these amendments to the above Model Act are intended to protect vital records against misuse. An analysis of the amendments is included. Some have been included in the Model Act.

III. Model State Vital Statistics Regulations, Provision Final Draft, 8-7-73, PHS Document No. 616.6

Those sections pertinent to control of birth certificates are excerpted from a provisional final draft of model regulations prepared by the Department of Health, Education and Welfare. These regulations accompany the Model Act given above.

ATTACHMENT I

MODEL STATE VITAL STATISTICS ACT

Model State Vital Statistics Act. Proposed revision by the Technical Consultant Panel MODEL STATE VITAL STATISTICS ACT and REGULATIONS, Document No. 648.7, November 24, 1975, DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE.

TECHNICAL CONSULTANT PANEL

on

MODEL STATE VITAL STATISTICS ACT AND REGULATIONS

Charge

To undertake a comprehensive review of the Model Vital Statistics Act: 1959 Revision, and develop revised languages as need to meet current requirements of the U. S. Vital Statistics System.

Structure

Consists of five members, including the Chairman, selected in terms of their detailed working knowledge of both law and vital registration practice in State and local jurisdictions.

MEMBERS

Mr. Donald J. Davids, Chairman, and Chief, Records and Statistics Section, Colorado State Department of Health, 4210 East 11th Avenue, Denver, Colorado 80220

Mrs. Hazel V. Aune, Valley View Road, Route 1, Verona, Wisconsin 53593
(formerly Chief, Registration Methods Branch, Division of Vital Statistics, NCHS:DHEW)

Mr. Irvin G. Franzen, Director, Registration and Health Statistics, Kansas State Department of Health, Topeka, Kansas 66603

Miss Martha H. Pattillo, Assistant Director, Vital Records Unit, Department of Human Resources, 47 Trinity Avenue, S.W., Atlanta, Georgia 30334

Mr. Ronald V. Saf, Attorney and Executive Director, Iowa State Board of Medical Examiners, 910 Insurance Exchange Building, Des Moines, Iowa 50309

Staff Resource

Mr. Loren E. Chancellor, Chief, Registration Methods Branch, Division of Vital Statistics, NCHS.

Mr. George A. Gay, Public Health Analyst, Registration Methods Branch, Division of Vital Statistics, NCHS.

CONTENTS

	Title	Page
Section 1	Definitions	D-37
Section 2	Office of Vital Statistics and Statewide System	D-38
Section 3	Rules and Regulations	D-38
Section 4	Appointment of State Registrar of Vital Statistics	D-38
Section 5	Duties of State Registrar	D-38
Section 6	Content of Certificates and Reports	D-39
Section 7	Birth Registration	D-40
Section 8	Infants of Unknown Parentage; Foundling Registration	D-41
Section 9	Delayed Registration of Birth	D-41
Section 10	Judicial Procedure to Establish Facts of Birth	D-42
Section 11	Court Reports of Adoption	D-43
Section 12	New Certificates of Birth Following Adoption, Legitimation, and Paternity Determination	D-43
Section 13	Death Registration	D-44
Section 14	Delayed Registration of Death	D-46
Section 15	Reports of Fetal Death	D-46
Section 16	Reports of Induced Termination of Pregnancy	D-46
Section 17	Authorization for Final Disposition	D-47
Section 18	Marriage Registration	D-48
Section 19	(Divorce, Dissolution of Marriage, or Annulment) Registration	D-48
Section 20	Amendment of Vital Records	D-48

Section 21	Reproduction of Vital Records	D-49
Section 22	Disclosure of Information from Vital Records	D-50
Section 23	Copies or Data from the System of Vital Statistics	D-50
Section 24	Fees for Copies and Searches	D-51
Section 25	Persons Required to Keep Records	D-51
Section 26	Duties to Furnish Information Relative to Vital Events	D-52
Section 27	Penalties	D-52
Section 28	Applicability	D-53
Section 29	Severability	D-53
Section 30	Uniformity of Interpretation	D-53
Section 31	Short Title	D-53
Section 32	Repeal	D-53
Section 33	Time of Taking Effect	D-53

Section 1. Definitions

As used in this Act:

(a) "Vital statistics" means the data derived from certificates and reports of birth, death, fetal death, induced termination of pregnancy, marriage and (divorce, dissolution of marriage, or annulment) and related reports;

(b) "System of vital statistics" includes the registration, collection, preservation, amendment and certification of vital records; the collection of other reports required by this Act; and activities related thereto including the tabulation, analysis and publication of vital statistics.

(c) "Vital records" means certificates or reports of birth, death, marriage, (divorce, dissolution of marriage, or annulment) and data related thereto.

(d) "File" means to present a vital record provided for in this Act for registration by the (Office of Vital Statistics).

(e) "Registration" means the acceptance by the (Office of Vital Statistics) and the incorporation of vital records provided for in this Act into its official records.

(f) "Live Birth" means the complete expulsion or extraction from its mother of a product of human conception, irrespective of the duration of pregnancy, which, after such expulsion or extraction, breathes or shows any other evidence of life such as beating of the heart, pulsation of the umbilical cord or definite movement of

voluntary muscles, whether or not the umbilical cord has been cut or the placenta is attached.

(g) "Fetal Death" means death prior to the complete expulsion or extraction from its mother of a product of human conception, irrespective of the duration of pregnancy; the death is indicated by the fact that after such expulsion or extraction the fetus does not breathe or show any other evidence of life such as beating of the heart, pulsation of the umbilical cord or definite movement of voluntary muscles.

(h) "Induced termination of pregnancy" means the intentional termination of pregnancy with the intention other than to produce a live-born infant or to remove a dead fetus.

(i) "Dead body" means a human body or such parts of such human body from the condition of which it reasonably may be concluded that death recently occurred.

(j) "Final disposition" means the burial, interment, cremation, removal from the State or other authorized disposition of a dead body or fetus.

(k) "Physician" means a person authorized or licensed to practice medicine or osteopathy pursuant to the laws of this State.

(l) "Institution" means any establishment, public or private, which provides in-patient medical, surgical or diagnostic care or treatment or nursing, custodial or domiciliary care, or to which persons are committed by law.

Section 2. Office of Vital Statistics and Statewide System

There is hereby established in the (State public health administrative agency) an (Office of Vital Statistics) which shall install, maintain and operate the only system of vital statistics throughout this State. The (Office of Vital Statistics) shall be provided with sufficient staff, suitable offices, and other resources for the proper administration of the statewide system of vital statistics and for the preservation of its official records.

Section 3. Rules and Regulations

The (State agency empowered to adopt public health regulations), hereinafter referred to as "State agency," is authorized, after notice and public hearing, to adopt, amend and repeal rules and regulations for the purpose of carrying out the provisions of this Act.

Section 4. Appointment of State Registrar of Vital Statistics

The (State Health Officer) shall appoint the State Registrar of Vital Statistics, hereinafter referred to as "State Registrar," in accordance with civil service laws and regulations.

Section 5. Duties of State Registrar

(a) The State registrar shall:

(1) Administer and enforce the provisions of this Act and the rules and regulations issued hereunder, and issue instructions for the efficient administration of the statewide system of vital statistics.

(2) Direct and supervise the statewide system of vital statistics and the (Office of Vital Statistics) and be custodian of its records.

(3) Direct, supervise and control the activities of all persons engaged in the operation of the statewide system of vital statistics as their activities relate to the statewide system

(4) Conduct training programs to promote uniformity of policy and procedures throughout the State in matters pertaining to the system of vital statistics.

(5) Prescribe, with the approval of the (State agency), furnish and distribute such forms as are required by this Act and the rules and regulations issued hereunder or prescribe such other means for transmission of data as will accomplish the purpose of complete and accurate registration.

(6) Prepare and publish reports of vital statistics of this State and such other reports as may be required by the (State agency).

(b) The State registrar may establish or designate additional offices in the State to aid in the administration of the statewide system of vital statistics.

(c) The State registrar may delegate such functions and duties vested in him to employees of the (Office of Vital Statistics) and to employees of an office established or designated under Section 5(b).

(d) The State registrar shall provide copies of certificates or reports required under this Act or data derived from such certificates or reports as he shall determine are necessary to local health agencies for local health planning and program activities. The State registrar shall establish a schedule for such transmittal with each local health agency. The records or data shall remain the property of the (Office of Vital Statistics) and the uses which may be made of such records or data shall be governed by the State registrar. A schedule for the disposition of the certificates, reports or data provided under this section shall be established by the State registrar.

Section 6. Content of Certificates and Reports

(a) In order to promote and maintain nationwide uniformity in the system of vital statistics, the forms of certificates, reports, and other returns required by this Act, or by regulations adopted hereunder, shall include as a minimum the items recommended by the Federal agency responsible for national vital statistics.

(b) Each certificate, report and form required to be filed and registered under this Act shall be on a form or in a format prescribed by the State registrar and shall contain the date received for registration.

(c) Information required by certificates or reports authorized by this Act may be filed and registered by photographic, electronic or other means as prescribed by the State registrar.

Section 7. Birth Registration

(a) A certificate of birth for each live birth which occurs in this State shall be filed with the (Office of Vital Statistics) or as otherwise directed by the State registrar within five days after such birth and shall be registered if it has been completed and filed in accordance with this section.

(b) When a birth occurs in an institution or enroute thereto, the person in charge of the institution or his designated representative shall obtain the personal data, prepare the certificate, secure the signatures required by the certificate and file it with the (Office of Vital Statistics) or as otherwise directed by the State registrar within the required five days. The physician in attendance shall provide the medical information required by the certificate and certify to the facts of birth within 72 hours after the birth. If the physician does not certify to the facts of birth within the required 72 hours, the person in charge of the institution shall complete and sign the certification.

(c) When a birth occurs outside an institution, the certificate shall be prepared and filed by one of the following in the indicated order of priority:

(1) The physician in attendance at or immediately after the birth, or in the absence of such a person,

(2) Any other person in attendance at or immediately after the birth, or in the absence of such a person,

(3) The father, the mother, or, in the absence of the father and the inability of the mother, the person in charge of the premises where the birth occurred.

(d) When a birth occurs on a moving conveyance within the United States and the child is first removed from the conveyance in this State, the birth shall be registered in this State and the place where it is first removed shall be considered the place of birth. When a birth occurs on a moving conveyance while in international waters or air space or in a foreign country and the child is first removed from the conveyance in this State, the birth shall be registered in this State but the certificate shall show the actual place of birth insofar as can be determined.

(e) (1) If the mother was married at the time of either conception or birth, or anytime between conception and birth, the name of the husband shall be entered on the certificate as the father of the child and the surname of the child shall be entered on the certificate as that of the husband, unless paternity has been determined otherwise by a court of competent jurisdiction.

(2) If the mother was not married at the time of either conception or birth or between conception and birth, the name of the father shall not be entered on the certificate of birth without the written consent of the mother and the person to be named as the father, in which case, upon the request of both parents in writing, the surname of the child shall be that of the father.

(3) In any case in which paternity of a child is determined by a court of competent jurisdiction, the name of the father and surname of the child shall be entered on the certificate of birth in accordance with the finding and order of the court.

(4) In all other cases, the surname of the child shall be the legal surname of the mother.

(5) If the father is not named on the certificate of birth, no other information about the father shall be entered on the certificate.

(f) A child born to a married woman as a result of artificial insemination, with consent of her husband, shall be deemed to be the legitimate child of the husband and wife.

(g) Either of the parents of the child or other informant shall attest to the accuracy of the personal data provided in time to permit the filing of the certificate within the five days prescribed above.

Section 8. Infants of Unknown Parentage; Foundling Registration

(a) Whoever assumes the custody of a live born infant of unknown parentage shall report on a form and in a manner prescribed by the State registrar within five days to the (Office of Vital Statistics) the following information:

- (1) The date and place of finding;
- (2) Sex, color or race, and approximate birth date of child;
- (3) Name and address of the person or institution with whom the child has been placed for care;
- (4) Name given to the child by the custodian of the child;
- (5) Other data required by the State registrar.

(b) The place where the child was found shall be entered as the place of birth.

(c) A report registered under this section shall constitute the certificate of birth for the child.

(d) If the child is identified and a certificate of birth is found or obtained, the report registered under this section shall not be subject to inspection except upon order of a (court of competent jurisdiction) or as provided by regulation.

Section 9. Delayed Registration of Birth

(a) When the birth of a person born in this State has not been filed within the time period provided in Section 7, a certificate of birth may be filed in accordance with regulations of the (State agency). The certificate shall be registered subject to such evidentiary requirements as the (State agency) shall by regulation prescribe to substantiate the alleged facts of birth.

(b) Certificates of birth registered one year or more after the date of birth shall be marked "Delayed" and show on their face the date of the delayed registration.

(c) A summary statement of the evidence submitted in support of the delayed registration shall be endorsed on the certificate.

(d) (1) When an applicant does not submit the minimum documentation required in the regulations for delayed registration or when the State registrar has reasonable cause to question the validity or adequacy of the applicant's sworn statement or the documentary evidence, and if the deficiencies are not corrected, the State registrar shall not register the delayed certificate of birth and shall advise the applicant of the reasons for this action. The State registrar shall advise the applicant of his right of appeal to (a court of competent jurisdiction).

(2) The (State agency) may by regulation provide for the dismissal of an application which is not actively prosecuted.

Section 10. Judicial Procedure to Establish Facts of Birth

(a) If a delayed certificate of birth is rejected under the provisions of Section 9, a petition signed and sworn to by the petitioner may be filed with (a court of competent jurisdiction) for an order establishing a record of the date and place of the birth and the parentage of the person whose birth is to be registered.

(b) Such petition shall be made on a form prescribed and furnished by the State registrar and shall allege:

(1) That the person for whom a delayed certificate of birth is sought was born in this State;

(2) That no certificate of birth of such person can be found in the (Office of Vital Statistics) or (the office of any local custodian of birth certificates);

(3) That diligent efforts by the petitioner have failed to obtain the evidence required in accordance with Section 9 of this Act and regulations adopted pursuant thereto;

(4) That the State registrar has refused to register a delayed certificate of birth; and

(5) Such other allegations as may be required.

(c) The petition shall be accompanied by a statement of the State registrar made in accordance with Section 9 and all documentary evidence which was submitted to the State registrar in support of such registration.

(d) The court shall fix a time and place for hearing the petition and shall give the State registrar () days notice of said hearing. The State registrar or his authorized representative may appear and testify in the proceeding.

(e) If the court finds, from the evidence presented, that the person for whom a delayed certificate of birth is sought was born in this State, it shall make findings as to the place and date of birth, parentage, and such other findings as the case may require and shall issue an order on a form prescribed and furnished by the State registrar to establish a certificate of birth. This order shall include the birth data to be registered, a description of the evidence presented, and the date of the court's action.

(f) The clerk of court shall forward each such order to the State registrar not later than the tenth day of the calendar month following the month in which it was entered. Such order shall be registered by the State registrar and shall constitute the certificate of birth.

Section 11. Court Reports of Adoption

(a) For each adoption decreed by (a court of competent jurisdiction) in this State, the court shall require the preparation of a report of adoption on a form prescribed and furnished by the State registrar. The report shall include such facts as are necessary to locate and identify the certificate of birth of the person adopted; provide information necessary to establish a new certificate of birth of the person adopted; and identify the order of adoption and be certified by the clerk of court.

(b) Information in the possession of the petitioner necessary to prepare the report of adoption shall be furnished by each petitioner for adoption or his attorney. The (social, welfare agency) or a person having knowledge of the facts shall supply the court with such information as may be necessary to complete the report. The provision of such information shall be a prerequisite to the issuance of a final decree in the matter by the court.

(c) Whenever an adoption decree is amended or annulled, the clerk of the court shall prepare a report thereof, which shall include such facts as are necessary to identify the original report of adoption and the facts amended in the adoption decree.

(d) Not later than the () day of each calendar month or more frequently as directed by the State registrar, the clerk of such court shall forward to the State registrar reports of decrees of adoption, annulment, or amendments thereof entered in the preceding month, together with such related reports as the State registrar shall require.

(e) When the State registrar shall receive a report of adoption or annulment of adoption or amendment of a decree of adoption from a court for a person born outside this State, such report shall be forwarded to the State registrar in the State of birth. If the birth occurred in a foreign country, the report of adoption shall be returned to the attorney or agency handling the adoption for submission to the appropriate federal agency.

Section 12. New Certificates of Birth Following Adoption, Legitimation, and Paternity Determination

(a) The State registrar shall establish a new certificate of birth for a person born in this State when he receives the following:

(1) A report of adoption as provided in Section 11 or a report of adoption prepared and filed in accordance with the laws of another State or foreign country, or a certified copy of the decree of adoption, together with the information necessary to identify the original certificate of birth and to establish a new certificate of birth; except that a new certificate of birth shall not be established if so requested by the court decreeing the adoption, the adoptive parents, or the adopted person.

(2) A request that a new certificate be established and such evidence as required by regulation proving that such person has been legitimated, or that a (court of competent jurisdiction) has determined the paternity of such a person.

(b) When a new certificate of birth is established, the actual place and date of birth shall be shown. It shall be substituted for the original certificate of birth.

(1) Thereafter, the original certificate and the evidence of adoption, paternity determination or legitimation shall not be subject to inspection except upon order of (a court of competent jurisdiction) or as provided by regulation.

(2) Upon receipt of a report of an amended decree of adoption, the certificate of birth shall be amended as provided by regulation.

(3) Upon receipt of a decree of annulment of adoption, the original certificate of birth shall be restored to its place in the files and the new certificate and evidence shall not be subject to inspection except upon order of (a court of competent jurisdiction) or as provided by regulation.

(c) If no certificate of birth is on file for the person for whom a new birth certificate is to be established under this section, a delayed certificate of birth shall be filed with the State registrar as provided in Section 9 or Section 10 of this Act before a new certificate of birth is established. The new birth certificate shall be prepared on the delayed birth certificate form in use at the time of adoption, legitimation or paternity determination. When the date and place of birth and parentage have been established in the adoption proceedings, a delayed certificate in the name and parentage at birth shall not be required.

(d) When a new certificate of birth is established by the State registrar, all copies of the original certificate of birth in the custody of any custodian of permanent local records in this State shall be sealed from inspection or forwarded to the State registrar, as he shall direct.

Section 13. Death Registration

(a) A death certificate for each death which occurs in this State shall be filed with the (Office of Vital Statistics) or as otherwise directed by the State registrar within five days after death and prior to final disposition, or as prescribed by regulations of the (State agency). It shall be registered if it has been completed and filed in accordance with this section.

(1) If the place of death is unknown but the body is found in this State, the death certificate shall be completed and filed in accordance with this section. The place where the body is found shall be shown as the place of death. If the date of death is unknown, it shall be determined by approximation.

(2) When death occurs in a moving conveyance in the United States and the body is first removed from the conveyance in this State, the death shall be registered in this State and the place where it is first removed shall be considered the place of death. When a death occurs on a moving conveyance while in international waters or air space or in a foreign country and the body is first removed from the conveyance in this State, the death shall be registered in this State but the certificate shall show the actual place of death insofar as can be determined.

(b) The funeral director or person acting as such who first assumes custody of the dead body shall file the death certificate. He shall obtain the personal data from the next of kin or the best qualified person or source available and shall obtain the medical certification from the person responsible therefore, as set forth below.

(c) The medical certification shall be completed, signed, and returned to the funeral director within 48 hours after death by the physician in charge of the patient's care for the illness or condition which resulted in death, except when inquiry is required by the (Post-Mortem Examinations Act). In the absence of said physician or with his approval the certificate may be completed and signed by his associate physician, the chief medical officer of the institution in which death occurred or by the pathologist who performed an autopsy upon the decedent.

(d) When death occurs more than ten days after the decedent was last treated by a physician, or if the cause of death appears to be other than the illness or condition for which the deceased was being treated or if inquiry is required by the (Post-Mortem Examinations Act), the case shall be referred to the (medical) examiner, coroner) for investigation to determine and certify the cause of death. If the (medical examiner, coroner) determines that the case does not fall within his jurisdiction, he shall within 24 hours refer the case back to the physician for completion of the medical certification.

(e) When inquiry is required by the (Post-Mortem Examinations Act), the (medical examiner, coroner) shall determine the cause of death and shall complete and sign the medical certification within 48 hours after taking charge of the case.

(f) If the cause of death cannot be determined within 48 hours after death, the medical certification shall be completed as provided by regulation. The attending physician or (medical examiner, coroner) shall give the funeral director or person acting as such notice of the reason for the delay, and final disposition of the body shall not be made until authorized by the attending physician or (medical examiner, coroner).

(g) When a death is presumed to have occurred within this State but the body cannot be located, a death certificate may be prepared by the State registrar upon receipt of an order of (a court of competent jurisdiction), which shall include the finding of facts required to

complete the death certificate. Such a death certificate shall be marked "Presumptive" and shall show on its face the date of registration and shall identify the court and the date of the decree.

(h) The (State agency) may by regulation provide for the extension of time periods prescribed for the filing of death certificates in cases where compliance therewith would result in undue hardship.

Section 14. Delayed Registration of Death

(a) When a death occurring in this State has not been registered within the time period prescribed by Section 13, a certificate shall be registered subject to such evidentiary requirements as the (State agency) shall by regulation prescribe to substantiate the alleged facts of death.

(b) Certificates of death registered one year or more after the date of death shall be marked "Delayed" and shall show on their face the date of the delayed registration.

Section 15. Reports of Fetal Death

(a) Each fetal death of 20 completed weeks gestation or more, or a weight of 350 grams or more, which occurs in this State shall be reported within five days after delivery to the (Office of Vital Statistics) or as otherwise directed by the State registrar.

(1) When a dead fetus is delivered in an institution, the person in charge of the institution or his designated representative shall prepare and file the report.

(2) When a dead fetus is delivered outside an institution, the physician in attendance at or immediately after delivery shall prepare and file the report.

(b) The name of the father shall be entered on the fetal death report in accordance with the provisions of Section 7.

(c) When a fetal death required to be reported by this section occurs without medical attendance at or immediately after the delivery or when inquiry is required by the (Post-Mortem Examinations Act), the (medical examiner, coroner) shall investigate the cause and shall prepare and file the report.

(d) The reports required under this section are statistical reports to be used only for medical and health purposes and shall not be incorporated into the permanent official records of the system of vital statistics. A schedule for the disposition of these reports shall be provided for by regulation.

Section 16. Reports of Induced Termination of Pregnancy

(a) Each induced termination of pregnancy which occurs in this State shall be reported to the (Office of Vital Statistics) within five days by the person in charge of the institution in which the induced termination of pregnancy was performed. If the induced termination of pregnancy was performed outside an institution, the attending physician shall prepare and file the report.

(b) The reports required under this section are statistical reports to be used only for medical and health purposes and shall not be incorporated into the permanent official records of the system of vital statistics. A schedule for the disposition of these reports shall be provided for by regulation.

Section 17. Authorization for Final Disposition

(a) The funeral director or person acting as such who first assumes custody of a dead body shall, within 72 hours and prior to final disposition of the body, obtain authorization for final disposition of the body. The physician or (medical examiner, coroner) when certifying the cause of death shall also authorize final disposition of the body on a form prescribed and furnished by the State registrar. If the body is to be cremated, authorization for cremation must be obtained from the (medical examiner, coroner) on a form prescribed and furnished by the State registrar.

(b) Prior to final disposition of a dead fetus, irrespective of the duration of pregnancy, the funeral director, the person in charge of the institution or other person assuming responsibility for final disposition of the fetus shall obtain from the parents authorization for final disposition on a form prescribed and furnished or approved by the State registrar. After final disposition the authorization shall be retained for a period of _____ years by the funeral director, the person in charge of the institution or other person making the final disposition.

(c) With the consent of the physician or (medical examiner, coroner) who is to certify the cause of death, a body may be moved from the place of death for the purpose of being prepared for final disposition.

(d) An authorization for disposition issued under the law of another State which accompanies a dead body or fetus brought into this State shall be authority for final disposition of the body or fetus in this State.

(e) Authorization for disinterment and reinterment shall be required prior to disinterment of a dead body or fetus. Such authorization shall be issued by the State registrar to a licensed funeral director or person acting as such, upon proper application.

(f) No sexton or other person in charge of any premises in which interments or other disposition of dead bodies is made shall inter or allow interment or other disposition of a dead body or fetus unless it is accompanied by authorization for final disposition. Each person in charge of any place for final disposition shall keep a record of all final dispositions made in the premises under his charge, stating the name of the deceased person, date and place of death, date of final disposition, and the name and address of the funeral director or person acting as such.

(g) Each person in charge of any place for final disposition shall endorse upon the authorization the date of disposition over his

signature and shall return all authorizations to the (Office of Vital Statistics) in the State where death occurred within 10 days after the date of disposition. When there is no person in charge of the place for final disposition, the funeral director or person acting as such shall endorse and return the authorization.

Section 18. Marriage Registration

(a) A record of each marriage performed in this State shall be filed with the (Office of Vital Statistics) and shall be registered if it has been completed and filed in accordance with this section.

(b) The official who issues the marriage license shall prepare the record on the form prescribed and furnished by the State registrar upon the basis of information obtained from (one of) the parties to be married.

(c) Every person who performs a marriage shall certify the fact of marriage and return the record to the official who issued the license within () days after the ceremony. (This record shall be signed by the witnesses to the ceremony.) (A signed copy shall be given to the parties.)

(d) Every official issuing marriage licenses shall complete and forward to the (Office of Vital Statistics) on or before the () day of each calendar month the records of marriages filed with him during the preceding calendar month.

(e) A marriage record not filed within the time prescribed by statute may be registered in accordance with regulations of the (State agency).

(f) Provision for a recording fee may be added here if desired.

Section 19. (Divorce, Dissolution of Marriage, or Annulment)

Registration

(a) For each (divorce, dissolution of marriage, or annulment) granted by any court in this State, a record shall be filed by the (clerk of court) with the (Office of Vital Statistics) and shall be registered if it has been completed and filed in accordance with this section. The record shall be prepared on a form prescribed and furnished by the State registrar by the petitioner or his legal representative and shall be presented to the (clerk of court) with the petition. In all cases the completed record shall be a prerequisite to the granting of the final decree.

(b) The (clerk of court) shall complete and forward to the (Office of Vital Statistics) on or before the () day of each calendar month the records of each (divorce, dissolution of marriage or annulment) filed with him during the preceding calendar month.

(c) Provision for a recording fee may be added here if desired.

Section 20. Amendment of Vital Records

(a) A certificate or record registered under this Act may be amended only in accordance with this Act and regulations adopted by the (State agency) to protect the integrity and accuracy of vital records.

(b) A certificate or record that is amended under this section shall be marked "Amended" (Except as provided in paragraph (c) of this section). The date of amendment and a summary description of the evidence submitted in support of the amendment shall be endorsed on or made a part of the record. The (State agency) shall prescribe by regulation the conditions under which additions or minor corrections may be made to certificates or records within one year after the date of the event without the certificate or record being considered as amended.

(c) Upon written request of both parents and receipt of a sworn acknowledgment of paternity of a child born out of wedlock signed by both parents, the State registrar shall amend a certificate of birth to show such paternity if paternity is not shown on the birth certificate. Upon written request of both parents, the surname of the child shall be changed on the certificate to that of the father. Such certificate shall not be marked "Amended."

(d) Upon receipt of a certified copy of a court order changing the name of a person born in this State and upon request of such person or his parents, guardian or legal representative, the State registrar shall amend the certificate of birth to show the new name.

(e) Upon receipt of a sworn statement from the physician performing the surgery certifying the sex of an individual born in this State has been changed by surgical procedure, and upon written request of such individual, the birth certificate shall be amended to reflect such change. The name of the individual may also be changed in accordance with the provisions of Section 20(d) of this Act.

(f) When an applicant does not submit the minimum documentation required in the regulations for amending a vital record or when the State registrar has reasonable cause to question the validity or adequacy of the applicant's sworn statements or the documentary evidence, and if the deficiencies are not corrected, the State registrar shall not amend the vital record and shall advise the applicant of the reason for this section. The State registrar shall advise the applicant of his right of appeal to a (court of competent jurisdiction).

(g) When a certificate is amended under this section, the State Registrar shall report the amendment to the (custodian of any permanent local records) and such record shall be amended accordingly.

Section 21. Reproduction of Vital Records

To preserve vital records, the State registrar is authorized to prepare typewritten, photographic, electronic or other reproductions of original records and files in the (Office of Vital Statistics). Such reproductions when certified by the State registrar shall be accepted as the original records. The documents from which permanent reproductions have been made and verified may be disposed of as provided by regulations.

Section 22. Disclosure of Information from Vital Records

(a) To protect the integrity of vital records, to insure their proper use, and to insure the efficient and proper administration of the system of vital statistics, it shall be unlawful for any person to permit inspection of, or to disclose information contained in vital records or to copy or issue a copy of all or part of any such record except as authorized by this Act and by regulation or by order of a (court of competent jurisdiction). Such regulations shall provide for adequate standards of security and confidentiality of vital records.

(b) The (State agency) may authorize by regulation the disclosure of information contained in vital records for research purposes.

(c) Appeals from decisions of the custodians of permanent local records refusing to disclose information, or to permit inspection of or copying of records under the authority of this section and regulation issued hereunder shall be made to the State registrar, whose decisions shall be binding upon the (local custodians of permanent local records).

(d) When 100 years have elapsed after the date of birth, or 50 years have elapsed after the date of death, marriage, or (divorce, dissolution of marriage or annulment), the records of these events in the custody of the State registrar shall become public records and shall be made available to any interested person in accordance with regulations which shall provide for the continued safe keeping of the records.

Section 23. Copies or Data from the System of Vital Statistics

In accordance with Section 22 of this Act and the regulations adopted pursuant thereto:

(a) The State registrar and other custodian(s) authorized by the State registrar to issue certified copies shall upon receipt of written application issue a certified copy of a vital record in his custody or a part thereof to any applicant having a direct and tangible interest in the vital record. Each copy issued shall show the date of registration and copies issued from records marked "Delayed" or "Amended" shall be similarly marked and show the effective date. All forms and procedures used in the issuance of certified copies of vital records in this State shall be approved or provided by the State registrar.

(b) A certified copy of a vital record or any part thereof, issued in accordance with subsection (a), shall be considered for all purposes the same as the original and shall be prima facie evidence of the facts stated therein.

(c) The Federal agency responsible for national vital statistics may be furnished such copies or data from the system of vital statistics as it may require for national statistics, provided such Federal agency share in the cost of collecting, processing and transmitting such data, and provided further that such data shall not be used for other than statistical purposes by the Federal agency unless so authorized by the State registrar.

(d) Federal, State, local and other public or private agencies may, upon request, be furnished copies or data for statistical or administrative purposes upon such terms or conditions as may be prescribed by regulation, and provided that such copies or data shall not be used for other than the purpose for which it was requested unless so authorized by the State registrar.

(e) The State registrar may, by agreement, transmit transcripts of records and other reports required by this Act to offices of vital statistics outside this State when such records or other reports relate to residents of those jurisdictions or persons born in those jurisdictions. The agreement shall require that the transcripts be used for statistical and administrative purposes only as specified in the agreement. Such transcripts shall not be retained by the other jurisdiction for more than two years from the date of the event or after the statistical tabulation have been accomplished, whichever time period is shorter.

Transcripts received from other jurisdictions by the (Office of Vital Statistics) in this State shall be handled in the same manner as prescribed in the preceding paragraph.

(f) No person shall prepare or issue any certificate which purports to be an original, certified copy or copy of a vital record as authorized in this Act or regulations adopted hereunder.

Section 24. Fees for Copies and Searches

(a) The (State agency) shall prescribe the fees to be paid for certified copies or certificates or records, or for a search of the files or records when no copy is made, or for copies or information provided for research, statistical or administrative purposes.

(b) Fees collected under this section by the State registrar shall be deposited in the (general fund, special vital statistics fund) of this State, according to the procedures established by (the laws governing collection, the State Treasurer).

Section 25. Persons Required to Keep Records

(a) Every person in charge of an institution as defined in this Act shall keep a record of personal particulars and data concerning each person admitted or confined to such institution. This record shall include such information as required by the certificates of birth and death and the reports of fetal death and induced termination of pregnancy forms required by this Act. The record shall be made at the time of admission from information provided by the person being admitted or confined, but when it cannot be so obtained, the same shall be obtained from relatives or other persons acquainted with the facts. The name and address of the person providing the information shall be a part of the record.

(b) When a dead body is released or disposed of by an institution, the person in charge of the institution shall keep a record showing the name of the deceased, date of death, name and address of the person to whom the body is released, date of removal from the institution, or if finally disposed of by the institution, the date, place, and manner of disposition shall be recorded.

(c) A funeral director, embalmer, or other person who removes from the place of death or transports or finally disposes of a dead body or fetus, in addition to filing any certificate or other report required by this Act or regulations promulgated hereunder, shall keep a record which shall identify the body, and such information pertaining to his receipt, removal, and delivery of such body as may be provided in regulations adopted by the (State agency).

(d) Records maintained under this section (shall be retained for a period of not less than () years and shall be made available for inspection by the State registrar or his representative upon demand.

Section 26. Duties to Furnish Information Relative to Vital Events

Any person having knowledge of the facts shall furnish such information as he may possess regarding any birth, death, fetal death, marriage, or (divorce, dissolution of marriage or annulment), upon demand of the State registrar.

Section 27. Penalties

(a)(1) Any person who willfully and knowingly makes any false statement in a certificate, record, or report required to be filed under this Act, or in an application for an amendment thereof or in an application for a certified copy of a vital record, or who willfully and knowingly supplies false information intending that such information be used in the preparation of any such report, record, or certificate, or amendment thereof; or

(2) Any person who without lawful authority and with the intent to deceive, makes, counterfeits, alters, amends, or mutilates any certificate, record, or report required to be filed under this Act or a certified copy of such certificate, record or report; or

(3) Any person who willfully and knowingly obtains, possesses, uses, sells, furnishes, or attempts to obtain, possess, use, sell, or furnish to another, for any purpose of deception, any certificate, record, report, or certified copy thereof so made, counterfeited, altered, amended, or mutilated; or

(4) Any person who with the intention to deceive willfully and knowingly obtains, possesses, uses, sells, furnishes, or attempts to obtain, possess, use, sell, or furnish to another any certificate of birth or certified copy of a certificate of birth knowing that such certificate or certified copy was issued upon a certificate which is false in whole or in part or which relates to the birth of another person, whether living or deceased; or

(5) Any person who willfully and knowingly furnishes or processes a certificate of birth or certified copy of a certificate of birth with the knowledge or intention that it be used for the purposes of deception by a person other than the person to whom the certificate of birth relates; or

(6) Any person who without lawful authority possesses any certificate, record, or report, required by this Act or a copy or certified copy of such certificate, record or report knowing same to have been stolen or otherwise unlawfully obtained; shall be punished by a fine of not more than \$10,000 or imprisoned not more than five years, or both.

(b)(1) Any person who willfully and knowingly refuses to provide information required by this Act or regulations adopted hereunder; or

(2) Any person who willfully and knowingly transports or accepts for transportation, interment, or other disposition of a dead body without an accompanying permit as provided in this Act; or

(3) Any person who willfully and knowingly neglects or violates any of the provisions of this Act or refuses to perform any of the duties imposed upon him by this Act shall be punished, unless otherwise stated, by a fine of not more than \$1,000 or be imprisoned for not more than one year, or both.

Section 28. Applicability

The provisions of this Act also apply to all certificates of birth, death, marriage, and (divorce, dissolution of marriage or annulment) and reports of fetal death and induced termination of pregnancy previously received by the (Office of Vital Statistics) or by any (custodian of permanent local records).

Section 29. Severability

If any provision of this Act (or the application thereof to any person or circumstances) is held invalid, such invalidity shall not affect other provisions or applications of the Act which can be given effect without the invalid provision or application, and to this end the provisions of this Act are declared to be severable.

Section 30. Uniformity of Interpretation

This Act shall be so construed as to effectuate its general purpose to make uniform the laws of those States which enact it.

Section 31. Short Title

This Act may be cited as the "Vital Statistics Act."

Section 32. Repeal

(Section ___ and Section __, __ Laws of ___ are hereby repealed; and) all other laws or parts of laws which are inconsistent with the provisions of this Act are hereby repealed.

Section 33. Time of Taking Effect

This Act shall take effect _____ .

ATTACHMENT II

PROPOSED AMENDMENTS AND ANALYSIS
(Suggested by the Department of Justice)

Proposed Amendments to the Model State Vital Statistics Act

*Section 12: Birth Registration

(a) A certification of birth for each live birth which occurs in this State shall be filed with the (local registrar) of the district in which the birth occurs and with the (State registrar) within seven days after such birth and shall be registered by such registrars if it has been completed and filed in accordance with this section: Provided, that when a birth occurs on a moving conveyance a birth certificate shall be filed in the district in which the child was first removed from the conveyance.

**Section 18: add new subsection (e):

Alternative 1

(e) Where it is known that the deceased was born in this State, the (local registrar) of the district in which the death occurred shall cause notice of such death to be filed at the office of the (local registrar) having custody of the deceased's certificate of birth. It shall be the duty of such (local registrar) having custody to conspicuously indicate on the face of such certificate the fact of death of the person whose birth is recorded therein.

Alternative 2

(e) Where it is known that the deceased was born in another State, the (local registrar) of the district in which death occurred shall cause notice of such death to be filed in such other State at the office of the (local registrar) having custody of the deceased's certificate of birth. It shall be the duty of such (local registrar) in the State of birth to conspicuously indicate on the face of such certificate the fact of death of the person whose birth is recorded therein.

*Section 26(a): Add after the words "except as authorized by regulation..." in paragraph (a);

*These sections have been included in the Model Act (Attachment I)
**These sections have not been included in the Model Act (Attachment I)

Such regulation shall provide for minimum standards of security and confidentiality for the retention and disclosure of vital statistics records.

****Section 27(a):** Add after the first sentence in paragraph (a):

Any request in the form of an application, and/or such certified copy that is issued upon request in any form shall contain explicit warnings, conspicuously displayed, that willfull and knowing falsification of information on an application, and/or willfull and knowing possession or use of a copy with knowledge that it contains such false information, shall be cause for criminal liability under Sections 31(a)(1)(3)(4) of this Act.

***Section 31: Penalties**

(a)(1) Any person who willfully and knowingly makes any false statement in a report, record, or certificate required to be filed under this Act, or in an application for an amendment or copy thereof, or who willfully and knowingly supplies false information intending that such information be used in the preparation of any such report, record, or certificate, or amendment thereof; or

(2) Any person who without lawful authority and with the intent to deceive, makes, counterfeits, alters, amends, or mutilates any report, record, or certificate required to be filed under this Act or a certified copy of such report, record, or certificate; or

(3) Any person who willfully and knowingly obtains, possesses, uses, furnishes, or attempts to obtain, possess, use, or furnish to another for use, for any purpose of deception, any certificate, record, report, or certified copy thereof so made, counterfeited, altered, amended, or mutilated; or

(4) Any person who with the intention to deceive willfully and knowingly obtains, possesses, uses, furnishes, or attempts to obtain, possess, use, or furnish to another any certificate of birth or certified copy of a record of birth knowing that such certificate or certified copy was issued upon a record which is false in whole or in part or which relates to the birth of another person, whether living or deceased; or

*These sections have been included in the Model Act (Attachment I)

**These sections have not been included in the Model Act (Attachment I)

(5) Any person, to include an employee of this State or political subdivision thereof, who willfully and knowingly furnishes or processes a certificate of birth or certified copy of a record of birth with the knowledge or intention that it be used by a person other than the person to whom the record of birth relates [shall be punished by a fine of not more than \$1,000 or imprisoned not more than one year, or both.]; or

(6) Any person who possesses any certificate, record, or report required to be filed under this Act or a certified copy of such certificate, record, or report, knowing same to have been stolen or otherwise unlawfully issued; shall be punished by a fine of not more than \$10,000 or imprisoned not more than five years, or both.

(b) Any person who willfully and knowingly refuses to provide information required to be filed under Sections 12, 13, 16, 17, 18, 19, 20, 22, or 23 of this Act or in completion of any application required to be filed thereunder, shall be punished by a fine not to exceed \$1,000 or imprisoned not more than one year, or both.

(c)(1) Any person who willfully and knowingly transports or accepts for transportation, interment, or other disposition a dead body without an accompanying permit as provided in this Act; or

[(2) Any person who refuses to provide information required by this Act; or]

(2) Any person who willfully and knowingly neglects or violates any of the provisions of this Act or refuses to perform any of the duties imposed upon him by this Act shall be punished, unless otherwise states, by a fine of not more than \$1,000 or be imprisoned for not more than six months, or both.

Section By Section Analysis of Proposed Amendments To The Model State Vital Statistics Act

The proposed amendments generally broaden the Act's present coverage to proscribe virtually every stage in the obtaining and use of false identification. The Department of Justice considers it imperative that the criminal technique of false identification be deterred at the state and local level. Of particular interest to the Department are the Model Act's penal provisions in Section

Brackets[] denote deletions.
Underlined words denote additions.

31. It is recommended that the illegal obtaining and use of identification records be upgraded from a misdemeanor to a felony under state law.

Section 12 would require the filing of a birth certificate both at the local and state level because the local registrar having custody of the certificate of birth (in the State of death under alternative 1 of Section 18, or in the state of birth under alternative 2, herein below) cannot always be determined unless birth records are centrally filed at the State level.

Section 18 goes hand in hand with Section 12. Centralized state filing of birth certificates in each state would enable officials in the state of death to pinpoint the precise location of birth, either within the state (alternative 1) or without the state (alternative 2), anywhere in the country. The objective is to match up death records with birth records by a notation on the birth certificate. Alternative 1 concerns only intra-state transmission of information: thus, each state would have the power to enact the proposed provision. But, alternative 2 necessarily involves interstate efforts at matching statistical records. Currently, the local registrar in the state of birth can match records, but it is considered likely that all states will have the same interest in protecting their birth and death records from would-be imposters. The state of death would notify the state of birth, in which event alternative 2 will require official notation on the birth certificate.

Section 26(a) and implementing regulations would allow inspection of vital statistics records only for proper purposes and under minimum standards of security. Each state should be allowed maximum flexibility in regulating public inspection of vital statistics records.

Section 27(a) would require a warning to deter fraudulent obtaining and use of false identification, primarily birth certificates. For those states that presently require an application to obtain a certified copy of a birth certificate, the suggested warning will help to deter fraud at the earliest possible stage - the application stage. Where a formal application is not required, a warning displayed on the issued copy will serve to deter further criminal use of the document.

Section 31(a)(1) broadens present coverage to prohibit false statements in an application for a copy of a record.

Section 31(a)(2) adds the offense of counterfeiting records.

Section 31(a)(3) prohibits other uses of bogus documents for deception.

Section 31(a)(4) specifies that willfull and knowing use is required for certain penalty provisions and proscribes the same uses of birth certificates as in the prior subsection relating to records in general. The subsection emphasizes the irrelevancy is proving a violation that the person whose birth certificate is illegally used is deceased.

Section 31(a)(5) deletes the present misdemeanor penalty provision; the penal provision as amended would make it a felony for a registrar or other state employee to fraudulently process a birth certificate.

Section 31(a)(6) adds the offense of possession with knowledge the record was illegally obtained. The second part makes all the above felonies at the state level, even though in the past fraudulent use of state documents was not a state crime. The objective is to cut off possession and use before passport fraud and other federally-relates offenses are committed.

Section 31(b) suggests a lighter penalty for the mere refusal to provide information to certain issuing authorities. However, a refusal to supply facts under Sections 14 (delayed registration of births) and 27 (copies of records) is remedied by denial of the petitioner's request.

Section 31(c)(2) has the effect of making violation of Section 31(c)(1) and other provisions of the Act a misdeamor.

ATTACHMENT III

MODEL STATE VITAL STATISTICS REGULATIONS (Selected Sections)
Department of Health, Education and Welfare

Regulation 13, Disclosure of Records

(Reference: Section 21 of the Model Act)

To protect the integrity of vital records

- (a) The (State registrar of vital statistics) or the custodian of permanent local records shall not permit inspection of, or disclose information contained in vital statistics records, or copy or issue a copy of all or part of any such record unless he is satisfied that the applicant has a direct and tangible interest in such record.
 - (1) The registrant, a member of his immediate family, his guardian, or their respective legal representatives shall be considered to have a direct and tangible interest. Others may demonstrate a direct and tangible interest when information is needed for determination or protection of a personal or property right.
 - (2) The term "legal representative" shall include an attorney, physician, funeral director, or other authorized agent acting in behalf of the registrant or his family.
 - (3) The natural parents of adopted children when neither has custody, and commercial firms or agencies requesting listings of names and addresses shall not be considered to have a direct and tangible interest.
- (b) The (State registrar of vital statistics) may permit the use of data from vital statistics records for statistical research purposes, subject to such conditions as the (State registrar of vital statistics) may impose. No data shall be furnished from records for research purposes until the (State registrar of vital statistics) has prepared, in writing, the conditions under which the records or data will be used

and received an agreement signed by a responsible agent of the research organization agreeing to meet with and conform to such conditions.

- (c) The (State registrar of vital statistics) or the local custodian may disclose data from vital statistics records to Federal, State, county, or municipal agencies of government which request such data in the conduct of their official duties.
- (d) Information from vital statistics records indicating a birth occurred out of wedlock may be disclosed only if it can be shown that the information is beneficial to the registrant.
- (e) Whenever it shall be deemed necessary to establish an applicant's right to information from vital statistics records, the (State registrar of vital statistics) or local custodian may require written application, identification of the applicant, or a sworn statement.
- (f) Nothing in this Regulation shall be construed to permit disclosure of information contained in the "Confidential Information for Medical and Health Use Only" Section unless specifically authorized by the (State registrar of vital statistics) for statistical research or if authorized by (a court of competent jurisdiction).

Regulation 14. Copies of Data from Vital Records

(Reference: Section 22 of the Model Act)

- (a) Full or short form certified copies of vital records may be made by mechanical, electronic, or other reproductive processes, except that the information contained in the "Confidential Information for Medical and Health Use Only" Section on birth and fetal death certificates shall not be included.
- (b) When a certified copy is issued, each certification shall be signed and certified as a true copy by the officer in whose custody the record is entrusted and shall include the data issued, the name or an authorized facsimile thereof, and the seal of the issuing office shall be affixed thereon.

- (c) Confidential verifications of the facts contained in vital statistics records may be furnished by the (State registrar of vital statistics) to any Federal, State, county, or municipal government agency or to any other agency representing the interest of the registrant, subject to the limitations as indicated in (a) above. Such confidential verifications shall be on forms prescribed and furnished by the (State registrar of vital statistics) or on forms furnished by the requesting agency and acceptable to the (State registrar of vital statistics); or, the (State registrar of vital statistics) may authorize the verification in other ways when it shall prove in the best interests of his office.
- (d) When the (State registrar of vital statistics) finds evidence that a certificate was registered through misrepresentation or fraud, he shall have authority to withhold the issuance of a certified copy of such certificate until a court determination of the facts has been made.

Regulation 15. Fees for Copies and Searches

(Reference: Section 23 of the Model Act)

No certified copies shall be issued until the fee for such copy is received unless specific approval has been obtained from the (State registrar of vital statistics) or otherwise provided for by statute or regulation.

For the issuance of a full certified copy or short form or birth card certification of a vital record, the fee shall be ___ per copy. For each search of the files when no record is found or no copy is made, the fee shall be _____. For statistical research purposes, the (State registrar of vital statistics) shall determine the fee for such services on the basis of the costs of providing such services and determine the manner in which such costs must be paid.

APPENDIX D2

MATCHING BIRTH AND DEATH RECORDS

M. Selvin

**The MITRE Corporation
Bedford, Massachusetts**

April 1976

This project was supported by Contract Number J-LEAA-014-76 awarded by the Law Enforcement Assistance Administration, U.S. Department of Justice, under the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Points of view or opinions stated in this document are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice.

TABLE OF CONTENTS

<u>Section</u>		<u>Page</u>
	LIST OF ILLUSTRATIONS	D-68
	LIST OF TABLES	D-68
I	INTRODUCTION	D-69
II	SUMMARY AND CONCLUSIONS	D-71
III	POPULATION STATISTICS	D-75
IV	TRANSMITTAL AND PROCESSING OF DEATH CERTIFICATES	D-85
	Documentation Interchange	D-85
	Modifications of the Present System to Include Birth/Death Matching	D-88
V	PROCEDURES AND COSTS FOR DEATH RECORD CODING	D-95
	Information Content of Birth and Death Certificates	D-95
	Coding of Matching Data	D-97
	Data Processing Costs	D-100
	REFERENCES	D-104

LIST OF ILLUSTRATIONS

<u>Figure Number</u>		<u>Page</u>
1	Birth and Death Rate vs. Time for U.S.	D-76
2	Population Distribution of U.S.	D-77
3	Death Rate per 1000 Population- 1965 Average of Males & Females	D-78
4	Probability of Dying within an Age Increment vs. Age in Years	D-80
5	Cumulative Probability of Dying at Less Than a Specified Age	D-81
6	Flow Diagram -- Transfer of Vital Statistics Data	D-86
7	Information Exchange of Vital Statistics	D-91
8	Simplified Information Diagram for Centralized Processing	D-93
9	Death Certificate Data Card	D-99

LIST OF TABLES

<u>Table Number</u>		<u>Page</u>
I	Maximum Matching Age Vs. Number of Annual Records	D-82
II	Birth/Death Matching Costs	D-101
III	Costs for Backdating Birth/Death Matches	D-103

SECTION I

INTRODUCTION

The Federal Advisory Committee on False Identification (FACFI) has endorsed the concept of birth/death matching as a deterrent to criminals seeking to obtain false IDs. The Law Enforcement Assistance Administration (LEAA) has recognized the need to analyze this recommendation in greater detail and has supported this MITRE study, which estimates the cost of birth/death matching and suggests procedures for implementing a partial solution to the false ID problem.

Birth/death matching implies that when a person dies, his birth certificate will be located from the information available on the death certificate and marked "deceased." At present, this is not done because there is no obvious relationship between where the person dies and where he was born; therefore, birth and death files are separately stored and rarely coordinated.

It is well known that false birth certificates are obtained (and subsequently false identities established) by applying for the birth certificate of deceased persons. If the issuer of the birth certificate has no death data and no reason to deny the request, a valid certified birth certificate is issued. The criminal recipient assumes the identity of the deceased person and uses the certificate to obtain a driver's license, passport and other documents, further reinforcing the apparent validity of his false identity.

When a person dies, a death certificate is filled out by the funeral director and attending physician. The death certificate contains a considerable amount of personal information about the deceased person that is supplied by a close relative.* Information such as Social Security number, veteran status, and marital status is necessary for legal and insurance purposes. In addition, the death certificate contains date of birth, place of birth, age, sex, full name, father's name, mother's maiden name, etc. This information is similar to the information required on a birth certificate request form. At present, a copy of the death certificate is forwarded from the state in which the person dies to the registrar of the state of the decedent's usual residence and is filed for census and statistical purposes.

*It is very rare for a deceased person to go unidentified, e.g., a derelict or unidentified suicide; these cases are statistically insignificant, and the false ID criminal would not know that the life/death match had not been made.

It has been determined from other FACFI studies that the false ID criminal is generally between the ages of 18 and 40, which led to the conclusion that an upper limit (greater than 40 years) for birth/death matching would be effective in thwarting false ID criminals and still be consonant with economy.

This report examines the cost of and procedures for effective birth/death matching. A step by step process is described and an appropriate cost analysis made which recognizes the realities of the present flow of data between states and the Federal government and the uses of this data for other than birth/death matching.

SECTION II

SUMMARY AND CONCLUSIONS

Low-cost procedures for matching birth and death certificates can be accomplished most effectively and efficiently if the procedure is limited to persons whose birth certificates would be of interest to false ID criminals (up to age 55). The most cost-effective and reliable method of implementing interstate birth/death matching is by coordinating it through the National Center for Health Statistics, rather than using present state-to-state cooperative procedures for transmitting "resident events." If the related activities of birth/death matching, resident events, a death index, and death statistics are centrally coordinated, the resulting overall cost will be minimized.

The search procedure needed to backdate birth/death matching is inherently labor intensive as 100 million records must be scanned by people without computer assistance. Matching recent deaths on a continuing basis will cost between 50¢ and \$1.25 per record and the speed is a function of how the centralized coordination is achieved and whether local office records are updated. A major saving can be achieved if the redundant files kept in about 7000 local offices were not used for issuing certified copies of birth certificates as these records would have to be updated monthly. The local offices could still provide the important roles of (1) helping applicants fill out the standardized application forms; (2) collect fees; and (3) forward birth certificate requests to the state office. The local offices could be compensated for their efforts on a population basis or by keeping a part of each fee collected. In-person applications for birth certificates are additionally a potential deterrent to false ID fraud.

In the long term, birth/death matching will be effective in denying the false ID criminal birth certificates of dead people; however, there is an interim period between the actual death and the monthly certificate update which a clever criminal may be able to exploit.

Birth/death matching will have no impact on the public's easy access to certified copies of birth certificates for lawful purposes but should increase personal privacy by preventing criminals from using names of deceased persons for fraudulent purposes.

There are 320,000 deaths annually of persons under 55 years of age. The annual cost of this birth/death matching averages .4 man-years/state, or \$320,000 at an average loaded salary of \$16,000. In the last 50 years,

100 million people have died but only 8 million birth/deaths must be matched. The total one-time cost of backdating is approximately 7 man-years/state or \$112,000/state. Although there is presently intrastate birth/death matching and interstate transmission of death data, the personalized procedure described in this report will require the explicit approval of every state, all of whom should consider the following conclusions.

- It is practical and not unduly expensive to institute an interstate process of birth/death matching. The death certificate contains six parameters that can be used for unique matching; in addition, there presently is an interstate exchange of death data for statistical purposes.
- The most economical and expedient method of matching can be done by transmitting the death certificates from the states to a central source, where sorting and mailing of data back to the appropriate states can be centrally performed.
- A saving can be realized by combining birth/death matching with the present interstate cooperative procedure of transmitting data on "resident events"; the National Center for Health Statistics (Division of HEW) could sort both sets of data. An additional saving will occur when the "death index" file and vital statistics function are coordinated using the same input data.
- A single birth/death match will cost between 50¢ and \$1.25, depending upon the requirement to update local offices and how the birth/death procedure is coordinated with the present transmittal of death data to HEW.
- Matching certificates of people who would be under 50 or 55 years of age if they were still alive appears to eliminate most false ID use and is much more economical than matching all previous deaths and births.
- The number of deaths that would have to be matched annually for false ID prevention is approximately 300,000.
- The number of deaths that must be updated from previous years is about seven million; of this number, about half are infant deaths for which the matching can be accomplished within a state. There is no available data on the number of adults who die in the same state in which they were born, but the number is probably significant, and intrastate matching of these people will further reduce the cost.

- The backdate search would have to be done manually, and the total cost of searching through 100 million records is estimated at 50 man-years.
- It is expensive to constantly update and maintain the duplicate birth files kept in local offices. There have been many arguments advanced for eliminating local offices issuance of birth certificates; birth/death matching provides an additional reason to eliminate this redundant issuance.
- There is a time delay loophole in the birth/death matching. It would not be practical to update birth certificate files more often than once a month; a clever criminal could take advantage of this time to acquire the birth certificate of a recently deceased person. This presents a loophole in the birth/death matching process as an effective deterrent to false ID proliferation.
- Birth/death matching has no impact on fraudulent applications for birth certificates of living persons.

SECTION III

POPULATION STATISTICS

This section computes the magnitude of the birth/death matching problem. The following demographic factors^{1,2,3} are useful in calculating the age distribution of the American population and the ages at which they die.

1975 U.S. Population	215 million*
1975 Birth Rate	3 million/year
1975 Death Rate	2 million/year
1975 Immigration Rate	400,000/year

The peak population of the U.S. is expected to occur in two generations. Assuming a constant death rate and that the birth rate continues to decrease linearly until the population reaches its steady state maximum, the U.S. population at the start of the 21st century will be:

U.S. Population** year 2000+ = 240 million

Figure 1 is a plot of birth rate and death rate for the United States from 1910 to 1974. The trend for the last 20 years shows a relatively constant death rate and sharply falling birth rate. The U.S. has already reached the "replacement fertility rate" of approximately 2.1 children per woman of childbearing age, but the population will continue to grow because of the relatively large number of young people who have yet to begin their families. Figure 2 shows the distribution of U.S. population in 1970 and the predicted distribution in the year 2000. The anticipated long-term steady state population distribution becomes almost uniform from birth to age 50, then decreases linearly to age 85+. Figure 3 is a plot of death rate per 1000 population of each age group. Each point, with the exception of under 1 year, is the average of 5-year groups. The infant mortality is high, followed by a minimum death rate in the 5 to 20 age bracket. The older age bracket has a sharply increasing death rate with increasing age.

*All figures have been rounded off.

**This figure is in agreement with the lowest estimate projection of Reference 4.

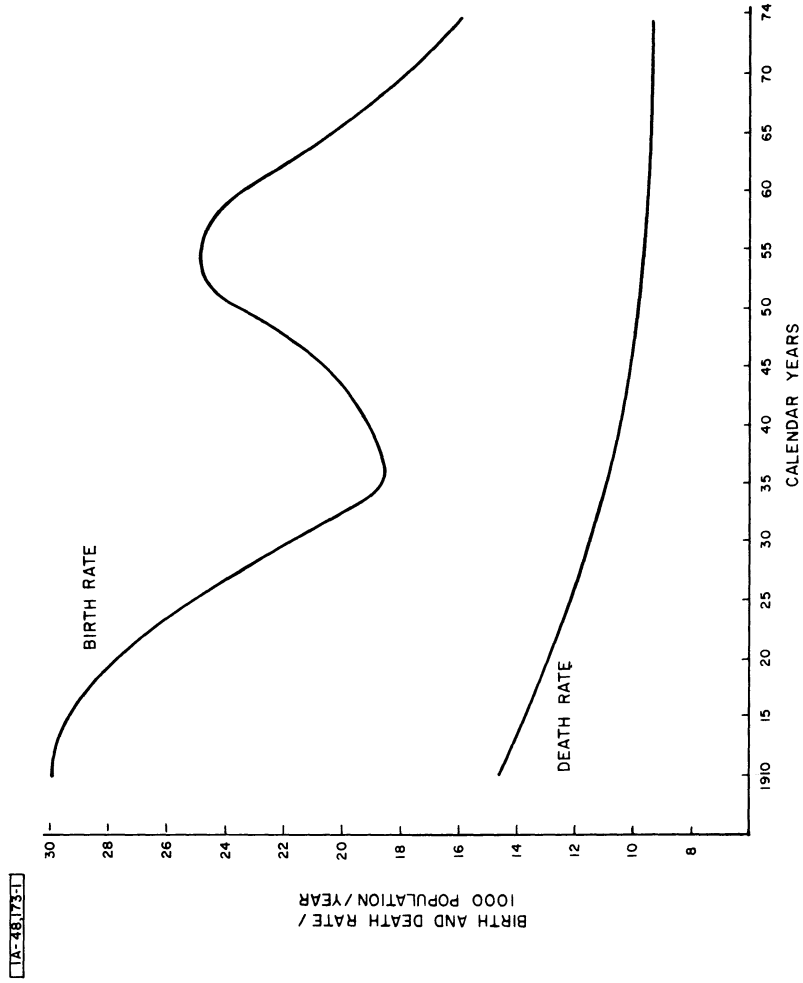


Figure 1. Birth and Death Rate Vs Time for U.S. (Source: Ref. 4)

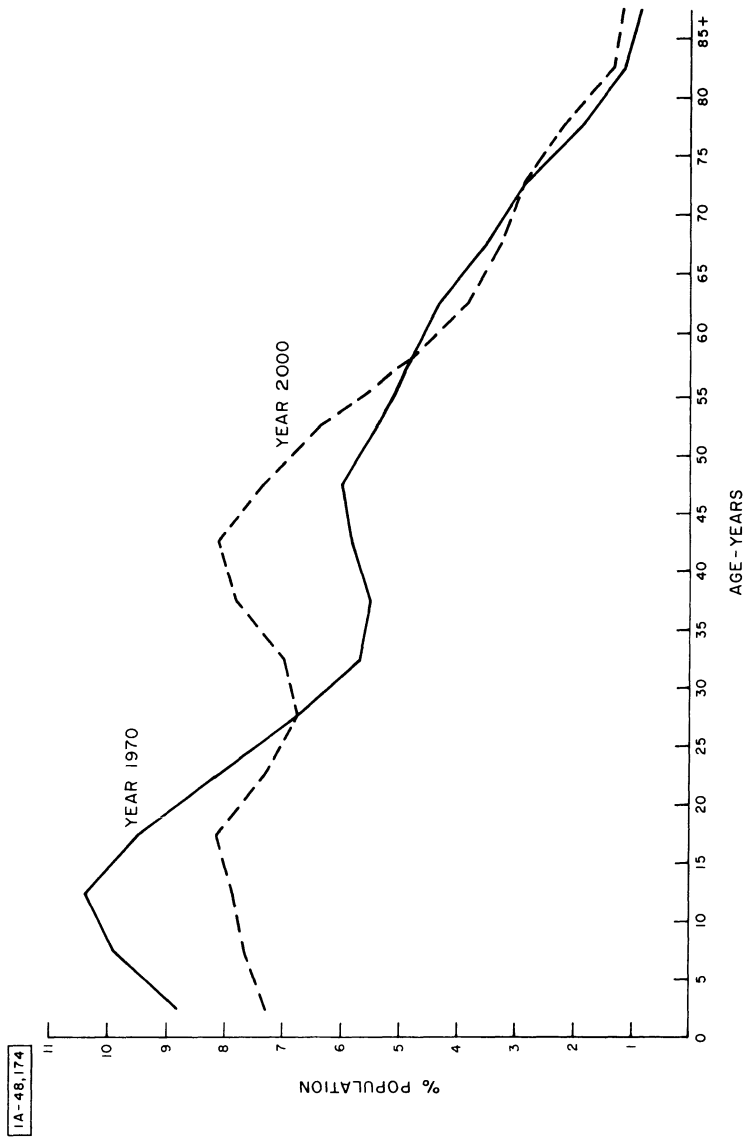
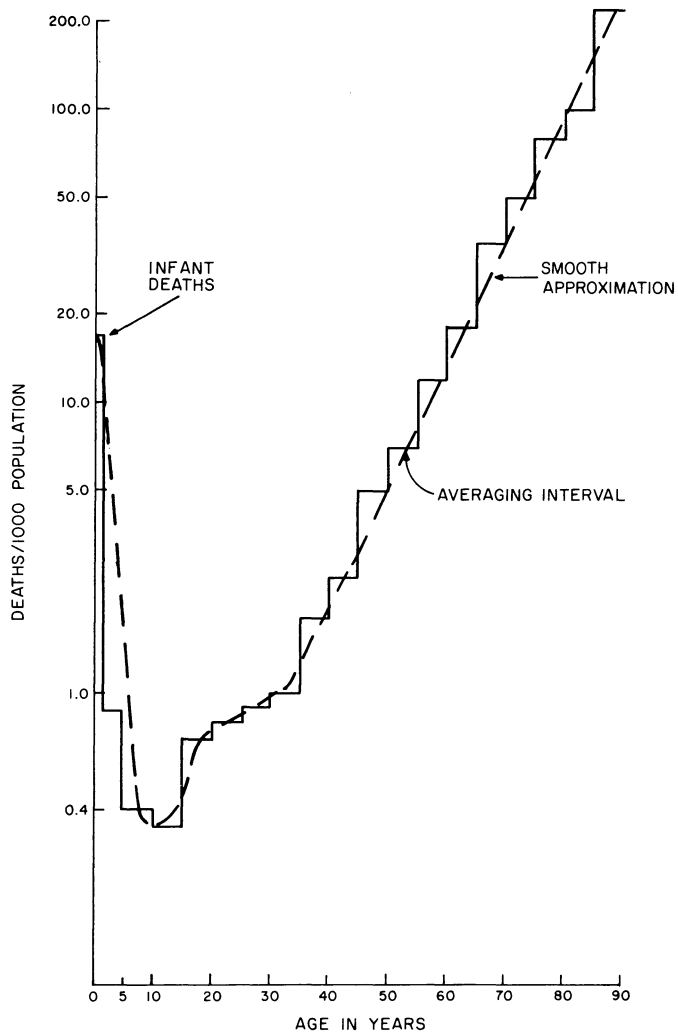


Figure 2. Population Distribution of U.S. (Source: Ref 2)



IA-48,175

Figure 3. Death Rate Per 1000 Population - 1965 Average of Males & Females (Source: Ref. 3)

Using the data in Figure 2 and Figure 3, it is possible to compute the probability of an American dying at any specific age, and the cumulative probability of dying before any age.

The assumptions made in the following calculations are:

1. The deaths/1000 population for each age group remains constant. This seems reasonable as medical science has already reduced the deaths due to infectious disease to a low level and little progress has been made with respect to health deterioration with advancing age.

2. The population distribution in the year 1985 is midway between the 1970 and year 2000 distribution.

This distribution is used in recognition of the inevitable delay between a recommendation and its implementation.

The curve of the probability of dying at a given age is obtained by determining the number of people that die at each age:

$$N_{DY} = P_T \cdot P_a \cdot P_D$$

where:

$$N_{DY} = \# \text{ of people dying per year at a specific age}$$

$$P_T = \text{Total Population}$$

$$P_a = \% \text{ population of age group}$$

$$P_D = \text{Probability of dying/1000}$$

which is the product of Figure 2 and Figure 3. These values must be normalized since the probability of dying at some age is 100%; and the computation is independent of the total population. The cumulative probability of dying before a given age is the sum of the probabilities of dying at each previous age.

These computations have been made and are shown graphically in Figure 4 and Figure 5.

It is clear that some limit must be established for which birth and death records will be correlated or:

1. The cost of transmitting and processing this data will be large.

2. Birth certificates which are of no interest to false ID criminals will be processed.

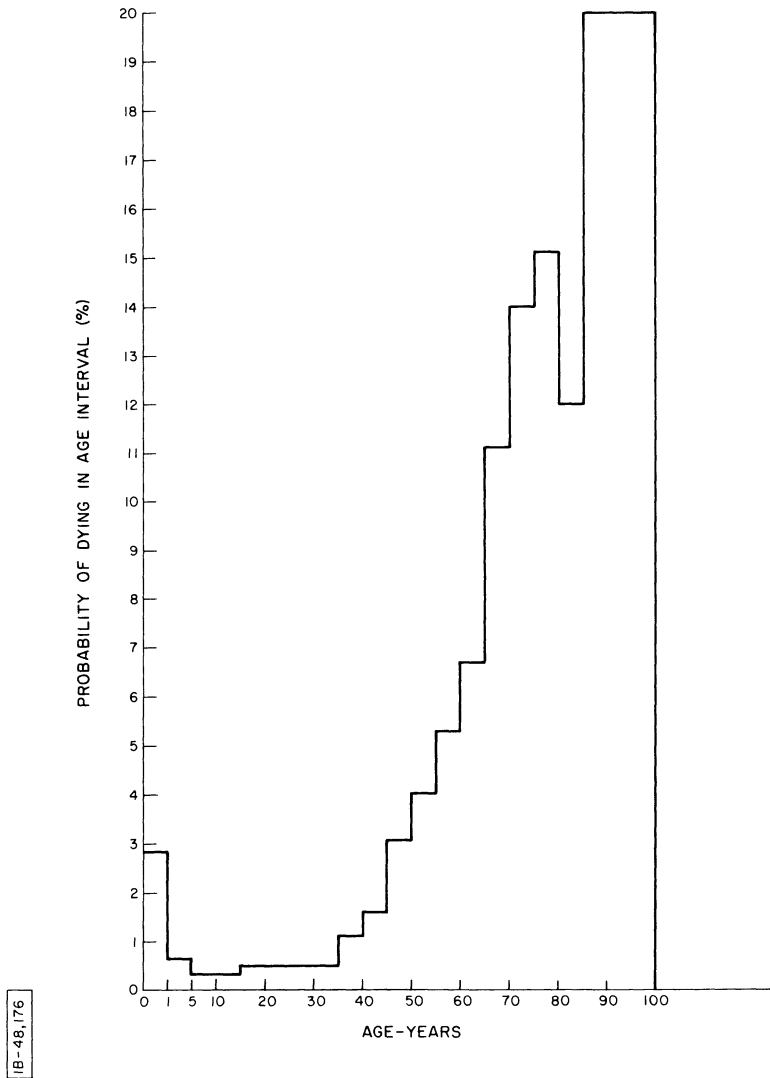


Figure 4. Probability of Dying Within an Age Increment vs Age in Years

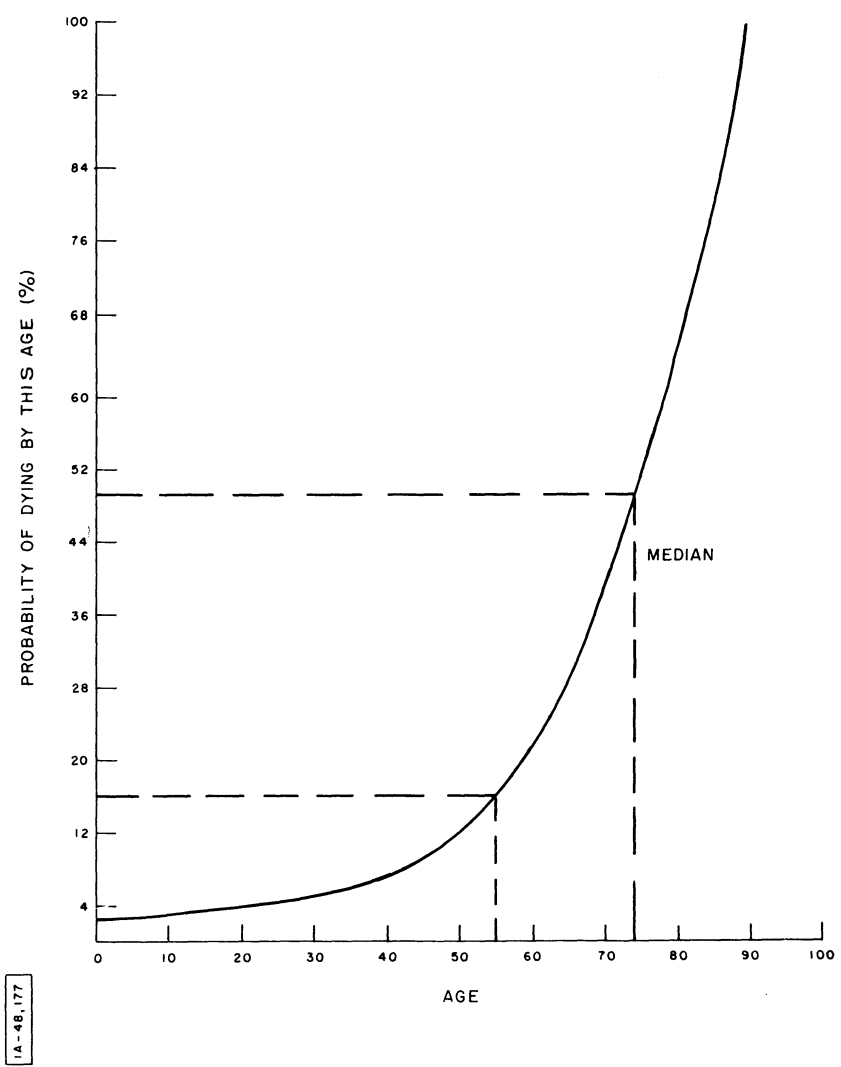


Figure 5. Cumulative Probability of Dying at Less Than a Specified Age

Therefore, it is recommended that the requirement for birth/
death matching be:

PROCESS AND MATCH ALL DEATH CERTIFICATES OF PERSONS
WHO WOULD BE "X" YEARS OF AGE OR YOUNGER IF THEY
WERE ALIVE TODAY.

The lower limit of "X" is determined by the estimate that most
false ID criminals are in the 18 to 40 age bracket; therefore, "X"
must be at least 40 years of age.

The upper limit of "X" is a function of how many "years of safety"
is considered adequate against impersonation, and how rapidly the
cumulative probability death curve rises. Common sense and Figure 5
indicate that an upper limit of 55 yields adequate safety and still
excludes the major portion of deaths.

The number of death records per year that must be processed on a
current basis can be calculated by multiplying the cumulative probability
of dying at age "X" or younger (Figure 5) by the total number of deaths
per year. A similar calculation can be used to compute the number of
people who died in past years but would be "X" years old or younger if
still alive. The birth and death records of these people should also be
correlated to prevent impersonation; the number of records that must be
"backdated" in this fashion is given by:

Total records = sum of all deaths per age group multiplied by
("X" minus age at death)

For example, if "X" is chosen to be 55 years, the total would include
records of all people who died five years ago at age 50 or younger,
those who died ten years ago at 40 or younger, and so on to include
records of infant deaths (only) that are 55 years old. Calculations
have been made of the number of records to be matched on a current basis
and "backdated" for various values of "X". These calculations are
presented in Table I below:

Table I
Maximum Matching Age Vs. Number of Annual Records

Maximum Matching Age	# of Deaths/ Year (Below Age "X")	Total Records Matched (backdated)	Total Records Backdated Interstate Without Infant Death Matching
40	140,000	4.5 million	1.6 million
45	180,000	5.3 million	2.1 million
50	240,000	6.5 million	2.9 million
55	320,000	8.0 million	4.05 million

The number of death notices which must be transmitted and processed each year is modest, varying from 140,000 to 320,000 depending upon the maximum age used. However, the backdating of information requires the processing of between 4.5 million and 8 million death records. The processing of these records will cost the nation an amount approximately equal to a year's issuance of birth certificates.

Infant deaths (under one year of age) affect the backdating cost in an unusual way and can be put in a separate category for the following reasons:

1. Infant mortality rate is higher than any other age group up to the age of 60 (Figure 3).
2. There is an excellent probability that these infants were born and died in the same state.
3. A program of intrastate infant birth/death matching for statistical purposes has been independently initiated over the years in several states.

If infant deaths are not backdated on a national basis but left as an independent state activity, then the interstate birth death backdating process is reduced by a factor of between two and three. These results are shown in column four of Table I.

The results previously obtained for backdating are inherently imprecise (although valid) because:

1. It was assumed that the death statistics were time invariant.
2. An "average" value of population equalling 200 million was used in combining all the death calculations.
3. The population distribution was assumed to be constant, and the 1970 distribution was used.

Using the individual death and population statistics, it was possible to recompute the nation's correct total annual death rate, which lends credence to the general validity of the results.

In Summary:

- The concept of matching births and deaths for only those persons who would be 55 years old or younger if alive at present appears to be practical and effective.
- The backdating processing costs are comparable to the cost of the nation's annual issuance of birth certificates. This does not include the search procedure needed to find the applicable death certificates (see section V). This cost can be still further reduced if the states do independent intrastate infant death matching. This is a "one time" operation.
- The continuing annual cost is based on the need to match only about 300,000 certificates per year.

SECTION IV

TRANSMITTAL AND PROCESSING OF DEATH CERTIFICATES

This section describes two practical procedures for matching the death certificate of a person with his birth certificate. There may be no relationship between where he was born, where he lived, and the place he died; his birth certificate(s) are stored in the state capitol and the local township and/or city of his birth. The birth/death matching problem cannot be solved as an isolated situation because there are many other documents and items of information which are sent state to state and state to Federal government. To be practical, any suggestion must incorporate the matching process into the existing network of information interchange.

DOCUMENTATION INTERCHANGE

Figure 6 is a flow diagram of the present method of transferring vital statistics documents between states and to the Federal government. The exchange involves the following:

1. The appropriate officials deliver the original vital statistics documents to the local registrar; for example, funeral directors supply death certificates and hospitals supply birth certificates. There is enough data on the death certificate to locate the deceased person's birth certificate (birth state, date of birth, etc.) and usual residence.

2. The local vital statistics registrar makes copies of these documents and, once a month, mails or delivers them to the state capitol.

3. At the State Vital Statistics Office, all the "state recorded events," which include births, deaths, marriages and divorces, are microfilmed. A common microfilming procedure is to put the documents into an automatic feeder machine and have the feeding process continually trip a 16 mm, black and white camera. A roll of 1200 negatives can be exposed in an hour and the total cost of the process is about \$10 for film and developing plus 2 hours of clerical time. The states are paid 4¢ per image and for many years, all states plus Washington, D.C. have been making and sending the microfilm to the National Center for Health Statistics, U.S. Department of Health Education and Welfare (HEW). The film is developed in-house or sent to a photographic company and mailed directly to HEW. There is no

subsequent feedback from HEW to the states except in the form of national vital statistics studies.

4. All the "state-recorded events" (births, deaths, etc., that happened in the state) are sorted into two groups: events that happened to in-state residents and events that happened to out-of-state residents. In this way, statistics of all the states can be published on the basis of all residents. Note that this sorting, and subsequent processing, has nothing to do with the birth state or birth certificate. A copy of the non-resident data is made and sorted into 50 files by subject's state of "usual residence". Every month, each state mails these data to the other 50 states for a total of over 2500 mailings. If no event in State A affects State B, no message is sent, leaving some uncertainty as to whether no event transpired or whether someone was negligent in State A.

In practice, major transmissions are between a state and its three or four immediate neighbors because a person is most likely to die or get married close to where he lives. However, this makes it all the more likely that an "event" in a remote state will be missed.

5. The state registrar combines the in-state resident events with the resident events received from the other 50 states to form a "total corrected resident" data file. Data from this combined file are punched on computer cards and require about three cards per entry event. Although identification data can fit easily on one card, much of the data is medical in nature and requires the extra space.

6. The cards are converted to magnetic tape via a computer. Magnetic tape stores data more efficiently than cards and can be read more rapidly by a computer. About 29 states now send HEW magnetic tape in addition to microfilm. It is anticipated that magnetic tape will replace the cards punched from the microfilm for HEW input data when complete agreement is reached on coding of "cause of death" for all conditions.

7. The states use this data to update their own records and do state statistical studies.

8. HEW receives the microfilm and magnetic tape data; the microfilm data are keyed and processed by computer. The magnetic tape data is used for demographic data, and the microfilm is used for "cause of death" data and for demographic data when magnetic tape is not available. Names are not included in the data processed by HEW computers.

9. HEW publishes many volumes of national statistical information annually which are used for medical studies, sociological studies, and by the states for comparative studies.

MODIFICATIONS OF THE PRESENT SYSTEM TO INCLUDE BIRTH/DEATH MATCHING

State-to-State Matching Birth/Death Linkage

In Figure 6, all "in-state events" were separated into resident and non-resident events by each state for all the other 50 states. An additional sorting and copy could be accomplished at this time, adding the death certificates of persons of appropriate age to the file of their birth state. Note that in this mobile society, there is little correlation between the birth state and present residence state. When mailing the non-resident event data, the death data for state of birth could be mailed in the same envelope, which would involve a minimal change, since no new information paths need be added.

Once a state receives notification of death, they must appropriately mark the birth certificate. Since the actual stamping (or making coded scratches on microfilm) takes very little time, the problem is primarily one of birth certificate location. The death certificates could be ordered (probably by computer) by date of birth or alphabetically, whichever was more convenient for the birth certificate search*. The cost of marking a birth certificate can be estimated, conservatively, as equal to the cost of issuing a birth certificate requested by a random applicant.

As previously mentioned, many states permit local registrars to issue certified copies of birth certificates. Thus, to prevent imposters from obtaining certificates of dead persons through local offices, these states would have to transmit a copy of the death data to the local issuance offices or legislate against local issuance. It is obvious that there is no point in matching births and deaths at 51 offices and not at the other 7000.

Federal Government Feedback of Death Certificate Information to the States

A centralized alternative to the interstate cooperative procedure is presented below.

*All states do not have the same filing procedure, which would require (ideally) a separate program in each state for each state. Although HEW has programs tailored to each state, it would not be practical to have separate programs in each state.

At the present time, the analysis performed by the National Center for Health Statistics is statistical only; it is impossible to identify any individual from these studies. By agreement, HEW can not use individually identified data for its statistical studies. In some cases, the tapes supplied by the states do not have the name of the individual; in all cases, HEW makes new tapes containing no name from the states' tapes and microfilm. The original tapes and microfilm are sent back to the states or destroyed within three years.

It is a simple software problem to use these data to generate death certificate listings which are organized by birth state if name data were included. These listings (and/or tapes) can be organized in whatever manner is most convenient for the individual state. Some states have their birth records sorted by birth date, some by county, some alphabetically. The program would determine the age of the deceased from birth date and death date and decide if the deceased was young enough to warrant birth/death matching; if so, the death record would be stored by birth state and a file for each state established. After all the data have been processed, the data for each state can be sorted so as to simplify the subsequent birth certificate search procedure. This sorting would not be practical on a state-to-state basis.

Although this procedure is practical and economical, there are several non-technical problems which must be resolved before it can become a reality. These are:

1. Each and every state must approve the sorting by HEW of death certificate data by name and birth state.
2. The format of the tapes supplied to HEW must be changed to include individualized name data.
3. The legislative rules governing HEW methods and procedures must be modified. The National Center for Health Statistics was chartered in July 1974 by an act of Congress, Public Law 93-353. This law must be studied to see if any revision is needed so birth/death matching can be coordinated centrally.

This procedure is attractive because the computer processing is done centrally, the data are available at the computing site, and the transmission paths between the Federal government and the states exist. The states will still have to search for and mark the birth certificates and solve the problems of distributing the death data to local issuance offices.

Interstate Transmission versus National Processing Center

Figure 7 is a gross simplification of how the birth/death data are transmitted and communicated intrastate, interstate, and to the National Statistics Center. In the drawing, only four states are used for illustration. A more accurate representation would show 55 jurisdictions* each having 54 lines going to the other states and 54 lines entering from the other states; a total of almost 3000 connections.

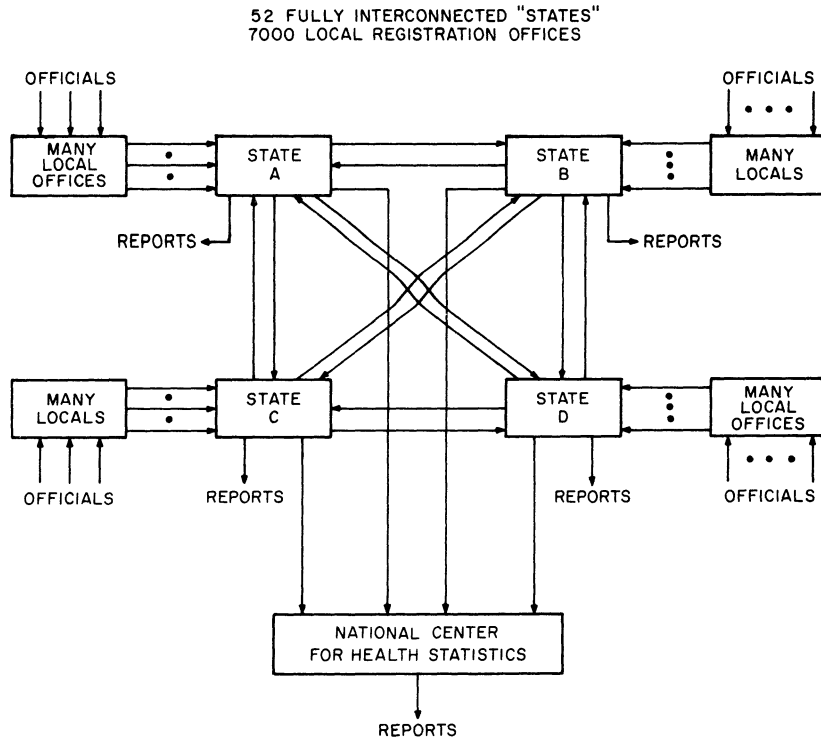
The interconnections between states are a source of unreliability and great expenditure because:

1. There are over 2900 potential individual sortings and mailings.
2. Each state must merge the inputs from the other states.
3. The formats of the data received are not consistent or optimum.
4. If no data is received from State Z, it is never known if State Z had no events to send or someone was negligent.
5. If several states fail to mail events, a conscientious state registrar may feel foolish doing all this work without receiving an equal amount of data, which may lead to loss of conscientiousness on his part, further reducing system reliability.
6. With the states doing the sorting for birth/death matching, another 2900 connections would be needed unless the "resident events" were sorted at the same time and the mailings coordinated.

In contrast, using a centralized source has these advantages in processing data:

1. The National Center already receives the data (except for names on some tapes). The data is used for health statistics and would be further needed if a National Death Index is established.
2. There is always an event in each state every month, so the National Center expects mail from each state; in the absence of mail, a query can be sent. Every state would receive complete data every month.

*New York City's files are independent of New York State; the other independent Registration Areas are the District of Columbia, Puerto Rico, Virgin Islands, and Guam.



IA-48,179

Figure 7. Information Exchange of Vital Statistics

3. Data processing is more economical in a large centralized facility.

4. HEW already has 55 individual programs "tailored" to each state's input format. Additional programs can be written to "tailor" the output.

5. In addition to death record sorting by place of birth, all resident events could be sorted and returned to the states, which saves state computer time and manual effort.

6. 110 mailings replace 2970 or 5940 mailings.

It appears reasonably clear that when birth/death matching is implemented, the flow of statistical data should be directly into HEW and HEW should mail all sorted deaths with other resident events directly to each state. For example, if a person who was born in Utah and resides in Texas dies while traveling through Arizona, Arizona would transmit death certificate data to HEW. At HEW, it would be sorted and a computerized record (list or data card) would be sent to Texas as the state of residence and Utah for birth/death matching. This new flow is depicted in Figure 8.

Modification of Local Issuance Offices

As discussed, birth/death matching may necessitate an additional 7000 monthly mailings from state to local offices because certified copies are issued from birth certificates stored in these local offices.

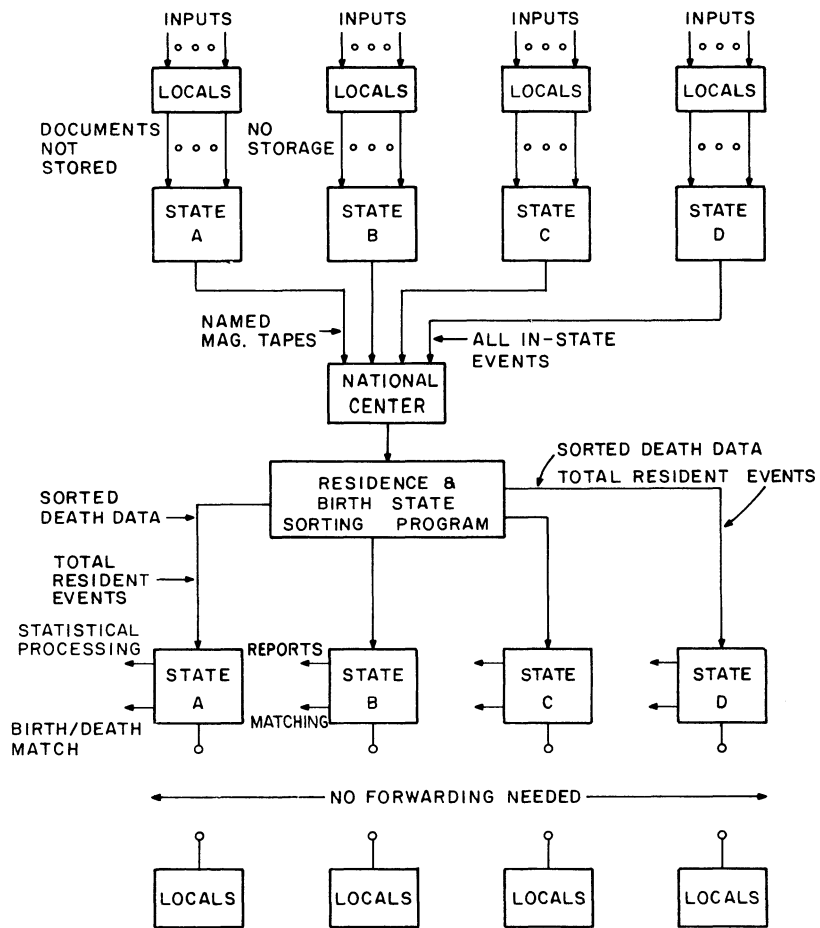
The arguments for state-only issuance and for state-plus-local issuance are listed below:

Arguments for State Issuance Only

1. Except for three New England states, the states have the original certificates (with birth number) and are presently issuing certified copies. More secure copies can usually be made from these original certificates.

2. Many states will computerize their certificate search and issuance procedures in the near future. This will lead to increased efficiency. It is not economical to computerize a small local issuance office.

3. There will be greater uniformity of birth certificate issuance. Redundancy and possible update errors will be eliminated. Death notices will not have to be sent to local offices.



IA-48,160

Figure 8. Simplified Information Diagram for Centralized Processing

Arguments for Local Issuance

1. Retention of local records offices and issuance is a strong political issue in many areas. The fees collected for certified copies are of course important to the counties and cities although they do not cover the cost of local offices.

2. There are fewer records per office, leading to a simpler search procedure.

3. The closeness of the office to some applicants permits more personal applications, fewer errors, and fewer mailings.

The public convenience could be served if the local offices accepted applications that they previously would have serviced and forwarded them to the state. Collecting applications in groups and forwarding them daily or semi-weekly to the state office would be more economical. The local community could receive a part of the fee for each application (say \$2 local and \$1 state), which would satisfy local revenue needs. Birth certificate files could be forwarded to the state or destroyed, saving office space that could be used in a more productive manner. By using this or a similar mechanism the states would be relieved of the task of forwarding death data monthly to 7000 local offices.

Backdating

The old vital statistics data does not exist in machine-readable form; HEW has not stored it, and the states have destroyed the punched cards and erased the tapes. No alternative exists but to manually search through volumes of data and repunch cards; the magnitude of this task is described in Section V.

SECTION V

PROCEDURES AND COSTS FOR DEATH RECORD CODING

This section defines the information needed for birth certificate/death record matching and specifies a coding procedure for economical, unambiguous matching. The flow of data from the states to the national government, back to the states, and then to local issuance offices is described together with realistic processing procedures and costs at each location.

INFORMATION CONTENT OF BIRTH AND DEATH CERTIFICATES

A "typical" birth certificate contains the following data:

1. Birth Certificate number (state issued only)
2. City, County, State of birth
3. Name of hospital
4. Family address
5. Full name of child
6. Date of birth
7. Sex
8. Type of birth (single, twin, triplet)
9. Length of pregnancy (complete weeks)
10. Birth weight
11. Father's full name
12. Father's race
13. Father's birthplace
14. Father's age
15. Father's occupation

16. Father's place of business
17. Mother's full maiden name
18. Mother's race
19. Mother's age
20. Mother's birthplace
21. Previous number of children in family
22. Doctor's name
23. Doctor's address

The death certificate contains the following data:

1. Death certificate number (no relationship to birth certificate number)
2. Full name
3. Complete address at death
4. Length of time lived in city or state
5. Marital status
6. Date of birth
7. Age
8. Usual occupation
9. Social Security number
10. Place of birth (State--not city or county)
11. Citizenship (which country)
12. Father's name (especially needed if deceased is a married woman)
13. Mother's maiden name

14. Name, address, relationship of informant
15. Place and time of death
16. Sex
17. Race
18. Cause of death (natural or type of illness)
19. Doctor's name
20. Burial location

A comparison of the two lists leads to the following list of parameters that might be used for matching purposes:

1. Full name
2. Date of birth
3. Sex
4. Father's full name
5. Race
6. State of birth
7. Mother's maiden name

Since use of term "race" is ambiguous and usually sensitive in nature, it is recommended that this parameter not be used. Therefore, a "match" can be made by the agreement of the above remaining six parameters.

CODING OF MATCHING DATA

Although it is anticipated that the birth/death matching procedure will be merged with the present transmittal of death data to the National Center for Health Statistics, the two requirements are not identical. The present death data stresses medical history and specifically eliminates personal identification. The birth/death matching requires identification but does not make use of the cause of death, therefore, the coding and costing is discussed independently from the present coding of death statistics. Pricing the coding costs in this manner is a conservative point of view, and a major fraction of the cost will be saved when the two activities are integrated.

A single data card can be punched (at HEW or under contract by the states) from the death certificate which contains the above six parameters. This card can be used for sorting by state, listing and duplication if needed. Such a punched card is shown in Figure 9, which represents a typical input.

- Columns 1-6 are the date of birth.
- Column 7 is the sex.
- Columns 8-10 are the abbreviation for birth state.
- Columns 11-80 represent the full name of decedent,
mother's maiden name,
father's full name.

The commas (,) are delimiters and this variable field technique should enable almost any sequence of three names to fit in 70 columns.*

Data processing centers have different procedures for punching cards. The three common sequences are:

1. Write data long hand on standard 80-column form from source certificate.
2. Punch card from standard form.
3. Verify card from standard form.

Since the policy at HEW allows card punching directly from the micro-filmed certificate, step 1 would be omitted from cost calculations.

From personal experience and consultation with a data processing center, an 80-column card can be punched in about one minute (average for an 8-hour day). Verifying the card takes the same time as punching the card. Using a loaded salary rate of \$8/hr or \$16,000/year:

one punched card costs 2 man minutes = 25¢ .

*There are numerous techniques for handling names that overflow a single card; however, overflow is unusual and does not affect the probable costs considered here.

DATA PROCESSING COSTS

Actual time in the computer to read and sort the data is negligible and any additional programming is a one-time cost that can be ignored in long-term cost calculations. No additional permanent computer storage is required.

Locating the Birth Certificate at the State Capitol

The mailing of the listed and sorted data from the National Center can be done at the same time the original microfilm is returned to the state capitol. This list can be used to locate and mark the birth certificate.

In an automated microfilm system, it takes about one minute to locate the birth certificate for an over-the-counter request. A coded scratch is used on the microfilm to denote death. When the certificates are stored in bound volumes, the search time varies from 2 minutes to 15 minutes, based on the correctness of the original data. Since the lists should be error-free and are already sorted in the most desirable way, the search time should be reduced from that of the present, random request procedure. Using an "estimated" search (and stamp) time of 4 minutes:

One located certificate at the state capitol costs
4 man minutes = 50¢

Communication with Local Issuance Offices

As described under "Transmittal and Processing of Birth Certificates," it is hoped that local offices will cease issuing birth certificates; in that case, no other costs would be incurred. However, if local offices do continue to issue birth certificates, the state must forward the death information to the local offices. Because the National Center only deals with the state capitols and the death certificate does not contain the information needed to specify the local issuance office, the National Center cannot sort data according to local office.

As the issuance clerks locate and stamp a specific birth certificate, they must record the identifying data from the birth certificate, which must then be sorted into bins that represent the address of the local offices. This duplicate copy (data) can be obtained by several procedures:

1. The clerk can make a copy of the newly stamped certificate and put the copy in the appropriate local office bin.

2. The clerk can record the six parameters longhand on a data card and file it.

3. When the national computer has sorted the data by states, a duplicate data card can be machine punched, which can be filed by local office.

The cost of this procedure is small, estimated:

One state sorted certificate for local issuance
= < 1 man-minute = 10¢

The sorted cards or certificates are mailed to the appropriate offices and then a local search must be made. Since the local records are less voluminous than those at the state offices, it is estimated that on the average

one local certificate search costs 3 man-minutes = 40¢ .

Cost Summary

The costs for matching a single birth and death are summarized in Table II. These figures are believed to be conservative and the costs below the dotted line will not be incurred if local offices do not issue birth certificates.

Table II

Birth/Death Matching Costs

<u>Activity</u>	<u>Man Minutes</u>	<u>Equivalent Cents</u>
National Center card punch	2	25
State birth certificate search	4	50

State sorting for local	< 1	10
Local search	$\frac{3}{10}$	$\frac{40}{\$1.25}$

The card punching procedure required of the National Center would also not be needed if the magnetic tapes presently supplied by the states contained personalized identifying data. Therefore, the cost of a single birth/death match probably will be between 50¢ and \$1.25.

Backdating Death Records

It is unfortunate that the computerized death certificate data from previous years are not available. It will be necessary to repunch death certificate data using original bound volumes as the source of the information, and the search and selection procedure is different from finding a randomly requested death certificate. Approximately 100 million people have died in the last 55 years and these death certificates are stored in each state by date of death. A clerk in each state office must scan through all the death records to determine if a record is suitable for birth matching. Assuming that infant deaths will be matched only within a state, it follows that:

- If a dead person was born in the year of that volume, the clerk should copy or mark data for subsequent intrastate search.
- If the person was born less than 55 years ago, the death record should be copied for central processing.*

This process does not require any arithmetic computation and can be accomplished almost as rapidly as the birth date can be read.

A simple experiment was performed to see how long it takes to read a number on a page and then turn to the next page. A comfortable decision-making rate equals one page in four seconds. In view of this figure, the entire nation's death records could be sorted at the following expense:

100 million sorted death records would cost 50-man years or an average of 1 person working a 40-hour week for a year in each state.

About 3 million (see Table I for 50-55 year cutoff age) dead people will meet the logic established for central death matching and there will be 3.5 million intrastate infant death matches. The 3 million centrally processed matches can be treated in the same manner as the monthly submissions of recent deaths. The "infant death" birth certificates can be stamped "Dead" when searched for and found, and a copy of the certificate can be made for sorting and mailing to the

*There is still another step possible. The clerk can check whether the deceased was born in the home state. It will require some practical experience to determine if this additional step saves or loses time. There is no data available as to how many people are born and die in the same state. Note that this decision does not have to be consistent for each state.

appropriate local offices. It is estimated that it will take 15 seconds to move the volume to a nearby copying machine and make a copy. The above discussion is summarized in Table III.

Table III

Costs for Backdating Birth/Death Matches

<u>Procedure</u>	<u>Man-Years</u>	<u>Cost</u>
Total Search (100 million)	50	\$800,000
Copy birth certificate (6.5 million)	14	\$220,000
Central card punching from microfilm of interstate deaths	50	\$800,000
States locate birth certificate from central return and infant deaths	200	\$3.2 million

Local search	150	\$2.5 million

The cost items under the dotted line would not exist if local offices did not issue certificates.

In summary, the annual national cost for birth/death matching would be between 10 man-years and 25 man-years. This estimate is based on 300,000 deaths per year, requiring between 4 and 10 man-minutes processing time. Major questions to be resolved are:

- How will birth/death matching be incorporated into the present death certificate transmittal procedure?
- Will local records have to be updated?

The one-time backdating costs will be between \$4.8 million and \$7.4 million (300 to 464 man-years); the largest variable is the need for updating of local office files. Even if the questions were resolved, the cost figures must be treated as rough estimates. Large variations are anticipated.

REFERENCES

1. Boston Museum of Science (Population Displays).
2. Charles F. Westoff, "The Populations of the Developed Countries," Scientific American, September 1974, pp. 109-120.
3. Haycocks, The Analysis of Mortality and Other Actuarial Statistics, Cambridge University Press, 1970.
4. Statistical Abstracts of the U.S.-1975-U.S. Dept. of Commerce, p. 51.

APPENDIX D3

**RECOMMENDED FEDERAL GUIDELINES FOR
IMPROVED DRIVER'S LICENSE SECURITY**

M. Selvin

**The MITRE Corporation
Bedford, Massachusetts**

May 1976

This project was supported by Contract Number J-LEAA-014-76 awarded by the Law Enforcement Assistance Administration, U.S. Department of Justice, under the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Points of view or opinions stated in this document are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice.

TABLE OF CONTENTS

<u>Section</u>		<u>Page</u>
	LIST OF ILLUSTRATIONS	D-108
	LIST OF TABLES	D-108
I	INTRODUCTION	D-109
II	RECOMMENDATIONS	D-111
	To Reduce Fraudulent Applications for Driver's License or State ID	D-111
	To Improve Document Security	D-112
III	STATE DRIVER LICENSING SYSTEMS	D-115
	Identification Procedure in Applying for a Driver's License	D-115
	System Constraints	D-119
	Recommendations for Reducing Issuance of Fraudulent Licenses	D-120
IV	DOCUMENT TYPES AND ISSUANCE PROCEDURES	D-127
	Characteristics of Existing State-Issued Driver's Licenses	D-127
	The Case for Photo Licenses	D-130
	Processing Methods for Photo Driver's Licenses	D-133
	Counterfeit and Anti-Counterfeit Techniques	D-141
V	COMPUTER USE	D-145
	DMV Computer Data Storage	D-145
	Status of On-Line Communications Terminals	D-146

TABLE OF CONTENTS (concluded)

<u>Section</u>		<u>Page</u>
VI	INFORMATION EXCHANGE	D-149
	Driver's License Control and National Driver Register	D-149
	National Crime Information Center (NCIC)	D-152
	National Law Enforcement Telecommunica- tion System	D-153
ATTACHMENT 1	DRIVER'S LICENSES AS PERSONAL IDENTIFICATION	D-157

LIST OF ILLUSTRATION

<u>Figure Number</u>		<u>Page</u>
1	General License Format	D-129

LIST OF TABLES

<u>Table Number</u>		<u>Page</u>
I	Cost Assessment for Color Photo License	D-132
II	Cost of On-Line Terminals in Ohio and Florida	D-147

SECTION I

INTRODUCTION

In 1974 the U. S. Attorney General established the Federal Advisory Committee on False Identification (FACFI) to study the cost to society of false ID crimes and to formulate potential solutions for reducing the number of these crimes. FACFI has evaluated over 50 preliminary solutions and has approved those found to be effective suggestions and rejected those that were either ineffective or impractical.

In studying the problem of providing U. S. residents with a secure identification document, the Committee reached these conclusions:

- A federally-controlled national identification system is undesirable.
- Existing state-controlled and state-administered document systems should be improved to produce reliable identification documents.
- The participation by any state in upgrading document systems should be voluntary.
- Applications for documents by any citizen should be voluntary.
- The driver's license is one of the two (the other being the birth certificate) most common de facto identification documents and should be recognized as such. An improved ID system should be a modification of the present driver licensing system.
- The Federal government should provide guidelines to the states defining characteristics of the system that will improve its secure identification function. These guidelines must be compatible with the present issuance procedures of the State Departments of Motor Vehicles (DMV).

- The Federal government should provide financial assistance to encourage state compliance with these guidelines.

In attempting to establish initial guidelines, FACFI recommends adopting the most secure procedures presently followed by some states. This report suggests guidelines for actions by the states that:

- Enhance license security,
- Do not incur excessive costs,
- Are compatible with current state practices,
- Enhance personal privacy.

Many agencies and corporations associated with the nation's motor vehicle system supplied valuable information to the FACFI. They are:

National Driver Register (NDR)
National Crime Information Center (NCIC)
National Highway Traffic Safety Administration (NHTSA)
National Law Enforcement Telecommunications System (NLETS)
Department of Public Safety - Boston, Mass.
DMV - Woburn, Mass.
DMV - Albany, N.Y.
DMV - Washington, D.C.
DMV Computer Center - Boston, Mass.
Polaroid Corporation
DEK/Electro Corporation
3M Corporation
IData Corporation
American Bank Note Company

Although their assistance was indispensable, their cooperation should in no way be viewed as an endorsement of either this report or its recommendations.

SECTION II

RECOMMENDATIONS

Summarized below are the major recommendations proposed in this report for improving the security of existing state driver licensing systems. Sections III through VI examine present systems and procedures and identify modifications that improve the systems without compromising privacy rights, imposing excessive costs, or significantly inconveniencing the general public.

TO REDUCE FRAUDULENT APPLICATIONS FOR DRIVER'S LICENSE OR STATE ID

- Since no single document is foolproof, all applicants for a new driver's license or state ID should be required to provide several documents as proof of identity. Requiring a multiplicity of documents adds materially to an imposter's cost and trouble. A list of relatively secure IDs should be established by state consensus or a Federal agency to guide local registrars. A tentative list is suggested in Section III of this report, but a training program is also needed to sensitize registrars to false ID techniques.
- Temporary licenses should not be issued except in emergencies because these licenses are very subject to false ID abuse; some of the recommended changes in procedures should obviate the need for their issuance.
- All license renewal applications should be made in person, which will help eliminate perpetuation of a false ID.
- The identification procedure for renewal, out-of-state, and lost licenses should require a handwriting check against a signed identification document as well as a computer verification of the applicant's identity. The computer record should contain personalized information not listed on the license and therefore not available to anyone presenting a stolen or forged document.

- A duplicate license should be marked DUPLICATE and a computer record made of its issuance, making a stolen original license "unrenewable".
- Schools should encourage students in driver's education classes to register in groups for driver's licenses or state ID cards, thus increasing the efficiency of identity checks through school records and teacher endorsement.
- Whenever practical, address verifications should be made a standard part of the personal identification procedure.
- The application form should explicitly state that false identification and use of a false ID are crimes; the form should also specify the legal punishment for such crimes.

TO IMPROVE DOCUMENT SECURITY

Anti-Counterfeit Measures:

- A color photograph of the driver should be a mandatory feature of all state driver's licenses. A photograph is effective for imposter detection and makes counterfeiting more expensive.
- Every state's driver's license should uniformly include this personal data: full legal name, address, date of birth, height, weight, eye color, license number, sex, signature, and expiration date.
- Anti-counterfeit features should be explicitly evaluated when vendors submit proposals for license forms. This could also provide an economic incentive for improving anti-counterfeit technology. However, the Federal government should not recommend specific anti-counterfeit characteristics, which will vary as technology changes and which are a function of vendor production procedures.

Requirements for State DMV Computer:

- States should adopt the parameters for computer storage recommended by the American National Standards Institute (ANSI) with the addition of two "hidden" personalized parameters--the mother's maiden name and name of high school or grade school attended. Such data should be contained in computer printouts requested by inspectors. Public knowledge of this "hidden check" could act as a deterrent to imposters.
- A code which is a function of the personal data should be used to generate the license number.
- Although on-line terminals are valuable for rapid intrastate computer verification, each state has specialized needs; therefore, no Federal standard can be established.

Interstate Information Exchange:

- Because two applicable computerized information systems--the National Driver Register (NDR) and the National Crime Information Center (NCIC)--store data only on the "exceptional" citizen, they cannot realistically be expanded to include all-inclusive false ID information.
- Use of present interstate regional agreements and Federal guidelines such as the National Driver Compact, Uniform Vehicle Code, and National Highway Safety Program is desirable and encouraged; however, additional guidelines for preventing impersonations should be developed.
- A study should be made of the practicality of including all state licensing offices into the National Law Enforcement Telecommunications System (NLETS) on a real-time basis. Such an arrangement would permit almost instantaneous (computer-to-computer) interstate exchange of motor vehicle and driver information, and if publicized could act as an additional deterrent.

TO ACT AS AN INCENTIVE, the Federal government should implement a cost-sharing procedure that will cover the start-up expenses of instituting a more secure driver licensing system. The cost sharing should be in proportion to the number of guidelines

followed by a state, and their opportunity to participate in such a program should terminate after a few years, which will act as an impetus to immediate action.

SECTION III
STATE DRIVER LICENSING SYSTEMS

IDENTIFICATION PROCEDURE IN APPLYING FOR A DRIVER'S LICENSE

Identification is the process of linking a person with a set of documents that "prove" the bearer has the necessary characteristics and qualifications to be entitled to the privileges and benefits for which he or she is applying. Applicants must be correctly identified at the application stage to be in one of the five categories listed below.

New Applicants

Included in this category are those applicants who have never before had a driver's license. Although a large percentage of these applicants are between the ages of 16 and 18 and are not likely to be false ID criminals, some older individuals also apply for a license for the first time. A new applicant is required to prove his ability to drive by taking a driving test, a written test, and an eyesight test. In addition, he must verify his name and age by presenting an identification document. The birth certificate is the most common document accepted as proof of name and age; forty-seven states require verification with a birth certificate. The successful applicant is issued either a final license or a temporary license, depending on the type of issuance system used by the state.

The birth certificate is not, however, a secure document because:

- There are no personalizing characteristics on a birth certificate that relate to an individual as a mature individual; infant footprints and fingerprints contained on some hospital certificates are useful for only a short time for identification purposes.
- In most cases, certified copies of the original certificate are made on ordinary paper, which is easily counterfeited.
- Because birth certificates are stored in the state, city or county of birth, often remote from the applicant, most applications are made by mail; therefore, the issuer never has an opportunity to validate the legitimacy of the applicant.

- The certificates have been, and in many cases still are, considered public documents, available for public scrutiny; therefore, an imposter has little difficulty finding enough information for filing a fraudulent application.
- There is almost no correlation between birth and death certificates; a criminal can find enough information from tombstone data or obituary columns to apply for and receive the birth certificate of a dead person.
- There is a wide diversity of birth certificate formats due to the multiplicity of non-centrally controlled issuance stations, making it virtually impossible for an inspector to spot an invalid format.

In summary, it is quite easy for an imposter to present a fraudulent birth certificate to a motor vehicle inspector and obtain a valid driver license. FACFI is aware of these loopholes and has approved recommendations to minimize these loopholes; however, it will be some time before these recommendations become a reality, and even then, a serious imposter will be able to "beat the system".

Applicants with Temporary Licenses

In some states (Massachusetts for example) a temporary license is issued prior to processing and possibly computer verification for a permanent license. For all practical purposes, the temporary license serves as identification until the applicant receives his permanent (2-4 year) license. If he receives his permanent license by mail, he is requested to destroy the temporary license.

A temporary license is printed on ordinary paper without any security features. Since the temporary license is often not collected after the permanent license is issued, it is often discarded in a haphazard manner. An imposter could easily fill out a fictitious temporary license or obtain a carelessly discarded temporary license. These temporary licenses are often accepted as proof of identity by merchants and, in addition, can be used within a reasonable time after their expiration to cause the issuance of a permanent license without further computer checks.

Applicants for Interstate License Transfer

In this mobile society, people are continually moving from one state to another. A new resident is usually required to apply within 90 days for a license in his new state. When he applies, his old license is accepted (in 47 states) as proof of identity and usually as proof of driving ability. The transfer applicant commonly takes a written and eye test and is granted a license as rapidly as the issuance procedure allows. In 45 states,¹ the old license is confiscated, to be either returned to the state of issuance for an update of their records or destroyed.

Sixteen states (Alabama, Arkansas, Connecticut, Illinois, Iowa, Maine, Maryland, Nebraska, New Jersey, New York, Pennsylvania, Tennessee, Vermont, West Virginia and Wisconsin) use a piece of data processing card, without photo, for their permanent license. In many states, only minimal anti-counterfeit techniques are employed to make the license secure. By forging or stealing one of these licenses--made easier by the lack of anti-counterfeit feature--a criminal can obtain a valid photo license in another state. In 43 states a transfer license is issued before any computer check is made with the home state; an impersonator has, therefore, an easy route for obtaining a valid photo license in someone else's name.

If a state does not observe the Uniform Vehicle Code, or the Highway Safety Program #5, or the Driver License Compact--all of which recommend confiscating an out-of-state applicant's old license and returning it to the state of issue--an impersonator gains both the old fraudulent license as well as a new officially-issued license. However, some states destroy confiscated licenses, which then eliminates any further possibility for an investigation.

If a stolen license is used by an imposter to obtain a transfer license and then returned to the home state, the home state computer record of the person being impersonated is updated to reflect the ostensible move out of state. This means the legitimate licensee may not receive the normal renewal notice. More seriously, however, he can receive traffic violations made by the imposter. New York State receives about 100 complaints a week from people who are falsely accused of breaking the law.

If a returned license is detected by the home state as a forgery or the name used is fictitious, the license is returned to the new state. At this point, however, there is little possibility of tracking down the impersonator.

Applicants for License Renewal

When a valid license expires, a driver is informed by mail or is expected to be aware of the fact that it is about to expire (often four years from the date of issue, on his birthday). In a state using a photo license, the driver reapplies in person and receives his new license by just presenting his old license as identification. He is given an eye test, and if he is elderly or has an obvious physical handicap, is given special attention.

In a state without a photo license, an applicant receives a computer card in the mail informing him that his license will expire on a certain date. The driver makes the necessary correction to his computerized record and returns the form (with fee) to the motor vehicle bureau. In a few weeks, the license card is remailed to him officially stamped. He rarely makes a personal appearance at the DMV.

Once an impersonator successfully penetrates a system which relies on mail renewal, he will probably continue to receive valid licenses in his falsified name. Also, if a criminal steals a renewal notice from the mail, the form can be altered and the new license mailed to the criminal's post office address.

Applicants for a Duplicate License

About 10% of the licenses issued each year are duplicates,² replacing lost or stolen licenses. In cases where a wallet has also been lost or stolen, the victim may also have lost all his identification papers (credit cards, Social Security card, library card, etc.). An applicant can, in this case, be identified by filling out an application blank and having the data checked against the DMV computer record, which is convenient and effective if the registry has on-line terminals. The applicant then receives his license (or temporary license in some cases immediately).

Without immediately available computer verification, the registrar can make the applicant wait for computer verification or issue a temporary license on trust; this procedure is followed in some cases simply because of a person's immediate need of a car for making a living. The alternative is to delay issuing the license, which may cause a serious hardship to the applicant.

SYSTEM CONSTRAINTS

When studying the driver licensing system from the viewpoint of preventing false ID, it is possible to lose perspective and recommend rigid safeguards to prevent impersonation. Such safeguards could have a harmful effect on other aspects of the system and not satisfy the requirements of applicants. Before recommending techniques for preventing the issuance of false driver's licenses, the following realities must be considered:

- There are no reliable figures on the number of fraudulent licenses issued. There are 128 million drivers in the country; proposed solutions should not "punish" the vast majority of honest people in an effort to prevent abuse.
- In a typical motor vehicle bureau, long lines often cause public annoyance and waste many man-hours. Any solution that impedes the normal processing procedure will be unpopular with the public.
- After satisfying all requirements for licensing, an applicant for a new or a transfer license often waits several weeks to receive the license because of computer verification. Additional delays of this nature would be undesirable.
- The Federal government is in debt, and many states are finding difficulty paying their bonds. Recommendations that require large capital investments would be unrealistic.
- People in different socio-economic levels carry differing amounts and types of documentation. Recommendations for identification requirements cannot be tailored to conform to just the "middle class".
- Driving a car is technically a privilege, not a right; however, strict adherence to this distinction is a denial of reality. Many people cannot shop for food or get to work or do their job without a car. Denying a person a license because his documentation is not in accordance with the "letter of the law" is unjustifiable.

There may be no method of eliminating all fraudulent license issuances, certainly no cost effective technique acceptable to the public. Therefore, all recommendations must be evaluated on the basis of the following criteria:

- How effective is the recommendation in minimizing the likelihood of fraudulent issuances?
- What effect does the recommendation have to the public in terms of cost, convenience and privacy?

RECOMMENDATIONS FOR REDUCING ISSUANCE OF FRAUDULENT LICENSES

Documentation

It is the intent of this report to make recommendations to convert the driver's license, whose sole purpose ostensibly is to verify the driving privilege, into a more secure identification document. This modification is motivated by the absence of any other secure ID and the fact that the birth certificate is an inadequate identification document. Since no single document can assure valid identification for application, the following is recommended:

ALL APPLICANTS FOR A NEW DRIVER'S LICENSE OR STATE ID SHOULD BE REQUIRED TO PROVIDE SEVERAL DOCUMENTS AS PROOF OF IDENTITY. A LIST OF RELATIVELY SECURE IDs SHOULD BE ESTABLISHED BY STATE CONSENSUS OR A FEDERAL AGENCY TO GUIDE LOCAL REGISTRARS.

This requirement is still open to some abuse because through alteration an impersonator can still beat the system. However, requiring consistency among several documents makes the imposter's problem more difficult. The State of Massachusetts has already anticipated such a procedure and requires at least three identification documents³ in applying for a lost or duplicate license.

The following documents are listed as an interim guide for motor vehicle registrars to aid in applicant identification. The list is not exhaustive and the ratings are heuristic.

Relatively Secure Documents

color photo driver's license
passport
military discharge papers
home mortgage or lease papers
transcript of school records
non-resident alien registration document
birth certificate
military ID
state-issued photo ID
police pistol permit (photograph and fingerprint)
Federal agency employee ID

Moderately Secure Documents

divorce papers or court order
expired picture license
car registration
student ID
employee ID (with photograph and signature)

Insecure documents

non-photo driver's license
cancelled check with signature
checkbook with name and address
bankbook
insurance papers
marriage certificate
bills with name and address
Christmas club account
welfare card
charge card personalized with signature
baptismal certificate
gun owner permit (no identifying information)
Social Security card

There may be situations where no documentation is available, such as: a person who has lost his wallet and needs to drive to make a living, or a poor person who works at odd jobs and has never established credit, entered the Social Security system, filed an income tax return or opened a bank account. In such unusual cases, a verbal or written endorsement (identification) by a known public figure (e.g., school teacher, doctor, clergyman, selectman, etc.) may be acceptable. Also, the identification

Renewal & Duplicate Licenses

Renewal by mail reduces highway safety. There are many licensed drivers whose physical condition has deteriorated. Their vision may have deteriorated; their reflexes may have slowed down due to age or a disease; they may have been crippled by a stroke or accident. A license to drive should not be granted in perpetuity; it is therefore recommended:

ALL LICENSE APPLICATIONS SHOULD BE MADE IN PERSON.

This procedure will permit the applicant's eyes to be examined and any obvious physical incapacities observed, thus increasing highway safety. This procedure is already being followed in all the photo license states.

Those states that issue renewals by mail have the least secure systems against impersonations. Presently, once an imposter successfully penetrates the system, the system continues to perpetuate his false identity indefinitely. It is possible that the renewal notice has fallen into the hands of a criminal; or that the criminal uses a specific false license for criminal activities and uses his real identity in normal activity. Naturally, the renewal notice and old license will serve as one identification document, but requiring additional identification may trap some false ID criminals.

When it has been determined that a license has been lost or stolen, a duplicate license must be issued. It is recommended:

THE IDENTIFICATION PROCEDURE FOR RENEWAL, OUT-OF-STATE, AND LOST LICENSES SHOULD REQUIRE A HANDWRITING CHECK AGAINST A SIGNED IDENTIFICATION DOCUMENT AS WELL AS A COMPUTER VERIFICATION OF THE APPLICANT'S IDENTITY. THE COMPUTER RECORD SHOULD CONTAIN PERSONALIZED INFORMATION NOT LISTED ON THE LICENSE AND THEREFORE NOT AVAILABLE TO ANYONE PRESENTING A STOLEN OR FORGED DOCUMENT.

and:

A DUPLICATE LICENSE SHOULD BE MARKED "DUPLICATE" AND A COMPUTER RECORD MADE OF ITS ISSUANCE.

These procedures will be most effective in catching a criminal trying to renew a stolen license.

data in the driver license file should be accessed and his name and address cross-checked through the telephone book.

Temporary Licenses

Temporary licenses serve very little purpose and are a potential source of fraudulent application. The following is therefore recommended:

TEMPORARY LICENSES SHOULD NOT BE ISSUED EXCEPT IN
EMERGENCIES BECAUSE THESE LICENSES ARE VERY SUBJECT
TO FALSE ID ABUSE.

If a person is a new applicant, his life style is such that he can be without driving privileges for another week or two without hardship. If a person is an applicant for interstate transfer of a valid license, he has 60 or 90 days to apply for a new license and can therefore apply for his new license early while continuing to drive with his old license. Application for a license transfer can be initiated by mail or telephone, so that the necessary interstate checks can be made on the validity of the current license without requiring a visit to the DMV. Once these checks have been completed, the applicant can be scheduled for a single visit and provided with a permanent license as quickly as the license manufacturing process will permit. Temporary licenses do not appear to be essential for either new licenses or license transfers.

In the case of a renewal, the old license should be considered valid until the new one is issued. The old license should always be returned to the DMV. In the case of a lost license, a duplicate license can be issued immediately after computer verification (on-line terminal or telephone) of the application for a replacement license. Such cases should be given priority treatment to avoid the need for temporary licenses.

Some unusual circumstances may still require a temporary license. Every effort should be made in such cases to minimize the time required for photographic processing and computer verification. The applicant should be required to return the temporary license in person to receive the new permanent license.

Name Verification

Almost all schools have a driver education program for students between the ages of 16 and 18. It is particularly easy to verify the identity of these young people because the instructor knows the students and the student's record can be used to prove his age. It is recommended:

SCHOOLS SHOULD ENCOURAGE STUDENTS TO VISIT THE DMV AND REGISTER IN GROUPS FOR DRIVING PERMITS, LICENSES OR STATE ID CARDS.

This procedure would be instructive to students and increase the efficiency of identity checks.

Address Verification

The home or mailing address of the licensee appears on the driver's license issued by all states except Kentucky; the address is considered to be a valuable item of information by businesses which use licenses as identification when cashing checks or extending credit. The address is also important in the enforcement of traffic laws (e.g., to permit serving of summonses and other legal notices) and to assist in locating relatives should the driver be involved in a serious accident. To be consistent with the philosophy that the license should contain only that identification information which has been verified by the issuing agency, we recommend:

ADDRESS VERIFICATION SHOULD, WHEREVER PRACTICAL, BE MADE A STANDARD PART OF THE PERSONAL IDENTIFICATION PROCEDURE.

States which mail each permanent license to the address given by the applicant receive an implicit verification of address. In this case, address errors are usually corrected only through applicants' complaints of non-receipt. However, such non-receipt could result not only from an incorrect address but also from such factors as mail delay or theft by a third party. These problems are avoided when the license is presented to the applicant in person at the DMV; in this case, however, additional verification of address is very desirable. Address verification can be obtained by requiring the applicant to present a postmarked envelope bearing his address. (If a card is mailed to the applicant to arrange for license examinations or pickup, it is convenient to request that the card be brought to the DMV.) If the applicant has a home telephone, his address can usually be verified through a local directory. Although Post Office boxes serve many people as legal mailing

addresses, they are usually not regarded as satisfactory descriptions of home address. A local address should be requested in addition to P.O. box number, verified whenever possible, and should appear on the license as well.

We recognize that these simple precautions can be overcome by persons who intend to move (without leaving a forwarding address) when they have received their licenses. However, we believe that address verification is generally useful and will enhance the reliability of the driver's license as an identification document.

SECTION IV

DOCUMENT TYPES AND ISSUANCE PROCEDURES

CHARACTERISTICS OF EXISTING STATE-ISSUED DRIVER'S LICENSES

The following list accounts for the data that can be found on various state-issued driver's licenses.

- Full name is included in all states.
- Present address is included in all states but Kentucky.
- Date of birth is included in all states.
- Driver's license number is included in all states.
- Signature is included in all states.
- Expiration date is included in all states (renewal period 2-4 years).
- Sex is included in all states but Massachusetts, Pennsylvania, Missouri, New Mexico and Minnesota.
- Height is included in all states but Michigan, North Carolina and Pennsylvania.
- Weight is included in 41 states.
- Eye color is included in 38 states.
- Hair color is included in 20 states.
- Fingerprint is not included in any state.
- Race is no longer used in any state.
- Thirty states list the Social Security number; in 11 of these states, the SSN becomes the license number.

License Number

Each state has a unique numbering scheme for their license. The numbers may contain alphabetic characters and up to 15 digits. Usually the number is sequentially assigned without any coded meaning. In 17 states, the license number has a coded relationship to the registrant's personal identifiers (name, address, birth date, etc.). These codes can be easily memorized by inspectors and are correspondingly easy for any tamperer or counterfeiter to break. However, coding of the license number helps detect and possibly deter amateur counterfeits.

Since no central coordinating computer is recommended, there is no need to recommend any specific driver license numbering scheme. However, some numbering schemes (Soundex* for example) use the personal data to generate the license number. This is an excellent procedure because it provides the inspector additional ability to detect tampering or counterfeit. It is therefore recommended:

A CODE WHICH IS A FUNCTION OF THE PERSONAL DATA
SHOULD BE USED TO GENERATE THE LICENSE NUMBER.

Tamper Resistance

There is almost a perfect correlation between a license being tamper resistant and the license having a color photograph. Almost all licenses are made of heavy paper (two are embossed plastic) but when a photo is added, the paper is laminated in plastic. Although this is done to protect the photo, it serves the important additional function of making it difficult for any alteration to go undetected. As of February 1976, none of the licenses were made of a specially designed secure substrate.

*A coding scheme that converts personal data to a reduced number of alphanumeric characters.

Color Photo and Non-Photo

A tabulation of use of these two types of license shows:

<u>Type</u>	<u>Number of States + Washington, D.C.</u>
Non-photo	15
Color Photo	36

Although the format of the licenses differs in detail, the general formats are similar. They are a convenient wallet size and contain (as shown in Figure 1):

- A photo in one corner.
- Name and address.
- Personal data, expiration date plus license type.

ANSI Standard Dimensions	Photo 1" x 1½"	Name Address
	Signature	Height, weight, sex Expiration date, Hair color License #, birth date Type of vehicle permit

Figure 1. General License Format

The primary differences between the photo driver's license and the non-photo driver's license are:

- Although non-photo licenses could be laminated in clear plastic, they have not been, presumably in the interest of economy. This makes it much easier to tamper with the non-photo-license, making the data on the license or ownership more suspect than the laminated photo license.
- The size of the non-photo license is not completely standardized; however, the majority of the licenses measure 2½" x 3 3/8". The longer dimension conforms to one dimension of a standard data processing

card (3¼"), which simplifies the computer processing procedure, and is still convenient for wallet insertion.

- The format of a non-photo license is more varied than the photo license because the size is larger. The information content is similar.

These differences generally apply also to state ID cards where they are used. Thirty-three states offer a state ID card and nine additional states have introduced legislation to offer its residents this ID.

THE CASE FOR PHOTO LICENSES

There are 36 states that presently issue a photo driver's license. Five additional states have passed legislation enabling the Commissioner of Motor Vehicles to issue photo driver's licenses, and seven more states are actively considering legislation that would enable the issuance of photo driver's licenses. Considering the fact that 20 years ago there were no photo driver's licenses, the popularity of their use is evident. The advantages of a photo license have become apparent to the public and their political representatives; however, since 16 states still issue "computer print-out" non-photo licenses, it is necessary to compare the two types in order to show the superiority of the photo license for decreasing fraudulent license use.

There are two advantages of a non-photo license.

- The incremental cost of each license is about 2¢, compared to an incremental cost for a photo license of approximately 50¢.
- The renewal procedure can be accomplished completely by mail. Although it is theoretically possible for a photo license to be renewed by mail, it is not done in any state.

The advantages of a photo license are overwhelming. Opinions expressed by law enforcement personnel verify this. "People no longer hire professional driving test stand-ins to obtain a license," an inspector explained. Before the photographic license was adopted, he relates, people who felt they could not pass the driving test, or would be refused a license for some

other reason, would hire someone to obtain a license for them. The photo license has stopped this practice.

A spokesman for the Highway Patrol in North Carolina also credited the photo license with reducing the number of people who would be driving with a revoked or suspended license. He says:

"The photograph just makes it too risky. These people used to drive with a borrowed, stolen, or counterfeit license, and we had no way of knowing it. Since we began issuing licenses with the driver's photograph on them, the number of drivers using counterfeit and borrowed licenses has been reduced by about 60 percent."

The photo license also makes the officer on patrol feel more secure, according to the Highway Patrol. One patrolman expressed it this way:

"When I look at a license that has the driver's photograph on it, I can be pretty sure that the guy I'm talking to is the guy that the license says he is. When I check him out with my dispatcher and get a good report on him, I know I'm not going to have any problem. Before, you could never be sure who you were talking to or what kind of trouble you were going to have with him."

The highways are safer when a state issues a photo license and reexamines the renewal applicant for obvious physical defects (eyesight, partial strokes, loss of capability due to age). A Polaroid Corporation study estimated:

"An analysis of the traffic fatality rate per 100 million miles traveled by private passenger vehicles in 1970 and 1971 shows that states combining driver reexamination with photographic driver's licenses have reduced traffic fatalities much more than states that do not reexamine, or which do reexamine but do not issue a photographic license."⁴

Approximately 50% of the serious automobile accidents are directly or indirectly involved with alcohol, and insurance rates reflect the fact that young people have more accidents per capita than older people. Motor vehicle officials claim that young men alter their non-photo license so that they can appear to be of drinking age. They also borrow their older brother's license to go drinking. It is inherently easier to impersonate

someone if the identifying document does not have a photo, and non-photo licenses are easier to alter than laminated photo licenses. For the same reasons, it is also easier to defraud a merchant with a non-photo license for identification.

A study was made for the State of Florida⁵ of costs incurred by changing to a color photo license. Each applicant was assessed an additional 50¢ at renewal or initial license application. The computation of cost was conservative and included factors such as address verification, driver history verification, and additional renewal processing costs. Almost no savings from improved procedural techniques was included in the accounting procedure; therefore, the results of the study were conservative with respect to the 50¢ fee (once in 4 years) being adequate.

The results are listed in Table I below:

Table I
Cost Assessment for Color Photo License (Florida)

<u>Year</u>	<u>Annual Surplus (Deficit)</u>	<u>Cumulative Surplus (Deficit)</u>
1973	(\$208,000)	(\$208,000)
1974	(\$184,000)	(\$392,000)
1975	\$193,000	(\$199,000)
1976	\$213,000	\$ 14,000
1977	\$238,000	\$252,000

The figures show conclusively that an additional cost of 12½/year per driver adequately covered the cost of a color photo. The initial costs were recovered in 4 years.

Since it is doubtful that any Commissioner of Motor Vehicles or legislator would argue against the desirability of a photo license, why don't all states have photo licenses? The answer is money. Although the driver's license fee adequately covers the cost of the license, the fee for it goes into the state's general fund. In fact, there is not a net cost but a net saving to the public. Highway safety and false ID crime is reduced by use of a photo license. The problem is finding a suitable financing mechanism that considers the political relationship between the Federal government and the states, and the scarcity of state money. It is recommended in this regard:

THE FEDERAL GOVERNMENT SHOULD IMPLEMENT A COST-SHARING PROGRAM THAT WILL COVER THE "START UP" EXPENSES OF INSTITUTING A MORE SECURE DRIVER LICENSING SYSTEM. THE COST SHARING SHOULD BE IN PROPORTION TO THE NUMBER OF FEDERAL GUIDELINES FOLLOWED BY A STATE AND THEIR OPPORTUNITY TO PARTICIPATE SHOULD TERMINATE AFTER A FEW YEARS, WHICH WILL ACT AS AN IMPETUS TO IMMEDIATE ACTION.

Some cost sharing should also be applied to those states that have already anticipated these Federal guidelines and are presently using photo licenses with anti-counterfeit features.

In summary, a photo license is desirable from the standpoint of:

- Highway safety,
- Law enforcement, and
- Reduction in false ID crimes.

Also, we have shown that cost effectiveness is not at issue in making a change to the photo license. In a very short time, the public saves many times the additional cost of issuing a photo license.

PROCESSING METHODS FOR PHOTO DRIVER'S LICENSES

Slightly more than half of the 36 states which issue photo licenses use a "centralized photo negative" process and the remainder use an "instant photo positive" process. Both the "central" and the "instant" process are produced with photographic equipment having a feature called "split optics" which has the capability to simultaneously record, on a single photographic medium, a portrait of the license applicant along with information and signature from a data card or license application. Although this photographic method is the same for both processes--central and instant--significant differences exist in the methods of photographic development and license distribution.

In the central process, an application or data card is generated during the course of the applicant's examination or renewal procedure. This card is then placed into the camera where a composite image of both the applicant and the data card is recorded on roll film. The applicant is then given a temporary permit, which he utilizes to exercise his driving privilege

until such time as the state is able to complete license processing at a central location and mail the finished permanent license to the applicant.

In the "instant process", a data card or application is similarly prepared during the course of the examination or renewal procedure. This card is then placed in the camera and a composite photograph is made of the applicant and data card. The "instant" time now required for completion of the license is sixty (60) seconds for print development and approximately one minute more for operations concerned with the cutting, lamination and sealing of the photograph into a finished license. The license is handed to the applicant, and records are subsequently processed and files updated at the state's central records repository.

Both processes have their advocates and both satisfy the licensing needs of the individual states. In this section we will itemize the advantages and disadvantages of each with respect to:

- License security,
- Public acceptance, and
- Law enforcement and administration.

No conclusion will be drawn, however, about the superiority of one system over the other.

License Security

Temporary Permits

With the central process it is common to issue applicants a temporary permit until such time as they are able to receive a completed license. The disadvantages of a temporary permit have been discussed previously.

Temporary permits are not generally required in an instant process. However, in at least one state (Massachusetts), in spite of the presence of on-line terminals and an instant photographic process, a temporary permit is issued for 60 days for new applicants, out-of-state applicants, and for duplicate licenses. This delay permits the check of the applicant's file by mail with the National Driver Register. Subsequently, the applicant

must revisit the DMV to be photographed and receive his photo license. The advantage and convenience of an instant process can only be realized, therefore, if suitable computer terminals and/or communications facilities are available and used for license verification.

Central File Verification

Delay is inherent in the central process, so time is available to verify an application at a central location before a license is returned to the applicant. With an instant process, it is necessary to adopt special procedures and/or develop communications between examining stations and the central office so as to assure verification of an applicant's status prior to hand delivery of the permanent license. In practice, most states using a central process verify all applications, whereas states using an instant process may restrict this verification to selected types of license applications, such as originals and duplicates. For renewal applicants, states using an instant process verify the applicant's record before sending out the renewal notice.

Susceptibility to Fraud and Theft

Unless special efforts are devoted to consideration of the possibilities for fraud and camera/film theft, the instant process affords an opportunity for improper activities by virtue of the fact that the entire photographic process, e.g., the camera and validation plates, are located in numerous field stations throughout the state. The film used in the instant process is identical to the film used in recreational photography and therefore a tempting target for theft. In addition, with many people able to make complete, valid licenses, the probability of fraudulent issuance by dishonest employees cannot be ignored.

Conversely, the central process divides major components among several locations. Cameras are located in the field; validation is applied to photographic licenses during film processing; and licenses are laminated and completed at a central facility under close supervision. This dispersion of equipment and personnel minimizes the probability of fraud and theft.

In both processes, the all important identification procedure is done by a single employee. The remainder of the issuance

procedure is automatic and mechanical. If this one employee were dishonest, both systems would be compromised.

Address Verification

Some motor vehicle authorities believe that the mailing and subsequent delivery of the license to the applicant is proof that the address was properly given and recorded. Others believe that the successful delivery of the license is not significant because of the high mobility of the population and the ease of making prior mail-drop arrangements.

A more preferred procedure would be to validate the applicant's correct address before a license is issued. This additional check (of records or documents) is commensurate with the examiner's responsibility to verify the applicant's identity. Efforts to support this activity may be enhanced in an instant process if it is recognized that address verification is performed solely by the examiner. As discussed in Section III, other changes in documentation of application may be needed before this procedure can be accomplished expediently.

Mail Delivery

While it is not a common occurrence, licenses do get lost in the mail and may fall into unauthorized hands. The mailing of licenses is a primary characteristic of the central process. When loss occurs, the subsequent search for the appropriate negative is expensive and annoying.

Applicant Identification

If the identifying documents of the applicant are not carefully and thoroughly checked by the issuance inspector, the applicant may be granted a valid driver's license although he is impersonating a real or fictitious person. Both systems are vulnerable to inadequate initial identity verification procedures.

Anti-Counterfeit Characteristics

Forty-four states claim to have licenses that are counterfeit- and/or alteration-resistant; therefore, it is possible to use anti-counterfeit techniques in both central and instant issuance. However, a central process has the inherent advantage of centralized equipment. Specialized, high capital investment in photographic equipment can be employed because it does not have to be purchased in quantity; for example,

a high resolution film can be used that produces a photo positive of a quality difficult for a counterfeiter to match. In California, a proprietary glass bead reflective laminate is bonded to the license in a production manner. This installation may be impractical or uneconomical to implement at a multiplicity of issuance stations. It is mandatory that the laminate be protected from theft, which is more easily accomplished with central processing.

Public Acceptance

Public Convenience

From the standpoint of public convenience, the instant process is more satisfactory than the central processing system. In an instant system:

- A qualified license applicant receives his license within two minutes of the picture taking.
- There are no temporary permits required.
- There are no licenses lost in the mail.
- An unsatisfactory photographic image is immediately obvious and the picture can be retaken. A camera malfunction is also immediately detected. There does not, however, appear to be any significant difference in the quality of the photograph from the two systems.

Two secondary disadvantages to the instant process are:

- The instant process requires a short time for cutting and laminating; an applicant can leave immediately in the central processing system.
- The majority of instant photos have two (or four) pictures per photo positive. When the issuance demand is low, an applicant may have to wait for the next applicant so that the issuance office does not waste half a photo positive.

Cost

From the viewpoint of the total cost necessary for production of driver's licenses, including systems ancillary to the document itself, analysis⁵ shows that the cost of both

systems is approximately equal. This analysis is supported by the observation that, in a highly cost-competitive market for state license contracts, each process has captured a substantial share. However, in the last three years mail costs have increased from 8¢ to 13¢ benefiting the instant process in competitive bids.

Exact costs will vary according to the specific product required by the state, the methods employed, and the issuance procedures followed. The price paid by the state to the vendor producing the license document is determined in a highly competitive bidding situation. This cost varies from 25¢ to 45¢ per license depending upon the exact specifications and annual volume. The total cost of the license issuing system includes additional factors such as rental of communication lines, computer time, building depreciation, office space, parking space, etc., costs that may exceed the incremental cost of each license and which are lumped together as "overhead". These items are usually not considered and are mentioned here so the reader will be aware of these "hidden" costs. Several components of both processes that affect total costs are listed below.

Address Verification. In both systems, the correct address is important for mailing renewals and activities related to law enforcement. In the central process, the correct address is necessary so that the applicant will receive the license on the first mailing. The cost for time to verify address and identity is well spent.

Internal Handling. The central process requires several steps not required in the instant process. These are:

- Mailing and receipt of film canisters from examining stations to the central office.
- Establishing records at both examining and central office regarding this mailing and receipt.
- Transmitting the film canister from the central office to the central laboratory with attendant records.
- After processing the film and printing the licenses, verifying and recording the fact that all appropriate licenses have been printed and that any licenses that should not be mailed have been pulled prior to insertion in envelopes.

- Performing a final quality control check at the time of license insertion into specially constructed envelopes for small-size documents.
- Sorting by zip code and calculating that the totals are correct.
- Stamping, final counting and mailing.

Mailing Costs. Mailing costs in the instant process are minimal. In a central process, the stamp costs are 13¢, the envelope costs 1¢, and the handling approximately 2¢. This adds up to between 40% and 50% of the cost paid to the vendor for producing the license. There are also additional costs for maintaining files of undeliverable licenses and "second time" mailings.

Examining Station Procedures. While the central process requires additional handling at the central office, the preparation and delivery of finished driver's licenses to qualified applicants at local examining stations using the instant process requires additional work, such as film development, cutting, and lamination. Film accounting procedures also necessitate additional recording of all photographs taken.

The net effect of performing the finished license production in the field is to utilize manual labor at numerous locations instead of high-speed production equipment at one central facility. In some stations, this necessitates hiring additional people, while other stations are able to absorb the increased workload. The extent of the cost increase for additional personnel can only be determined on a station-by-station basis with consideration of existing and projected workloads. The central process does not require a similar increase in work effort at examining stations since film processing and final license manufacture is performed at the central laboratory.

Law Enforcement & Administration

An important characteristic of central processing is the existence of a file of negatives of the licenses issued.* Law

*This could be accomplished with an instant process by having a conventional camera photograph the subject (or finished license) at the same time that the instant picture is made, which would increase the license cost by approximately 25¢. Alternatively, a back-up instant print could be taken and filed, which would be expensive and not have the flexibility of a negative.

enforcement and issuance agencies view this file as an advantage for the two reasons described below.

Criminal Identification Photos

If the owner of a driver's license is suspected of a crime, the negative of the license can be accessed and another copy made. In addition, the picture portion can be enlarged (to 8" x 10" for example) so that the officer can obtain a clear, easily identifiable print. This procedure is expensive and time consuming and is done primarily for persons suspected of committing felonies. It is possible, however, to use a 16 mm black and white auxiliary system since the higher quality 35 mm photograph is not necessary for this function.

Lost Licenses

If a person loses his license, he can request a duplicate license without being rephotographed. The negative can be accessed and a new license printed and mailed to the applicant. This is not a cost-effective procedure as it may take several hours from the initial request to locate the negative; however, it has the potential of eliminating the inconvenience of a personal appearance. Minnesota is the only state that presently reissues licenses in this manner.

Although a new license could be reissued without a new photograph, normal changes in a person's appearance, address, change, and reissue dates make use of a negative for renewals undesirable. Having an applicant apply for a license in person permits reinspection and simplifies the information content of the photographic negative. All photo license states require in-person renewals. An important advantage of in-person renewal is reexamination to determine if the applicant is still fit to drive.

It should be noted that a part of the public may view the central file of negatives, accessible to law enforcement officials, as an invasion of their privacy.

Summary and Conclusions

The principle advantages of the instant process are:

- Public convenience in immediate receipt of license.
- Saving of postal fees.

- Security in elimination of temporary licenses.
- Convenience and cost savings in eliminating applicant recall due to "eye blink" and equipment malfunction.

The principle disadvantages of an instant process are:

- Difficulty of performing adequate computer checks at license issuance, a situation that could be improved with the increased use of an on-line terminal.
- The absence of a negative file of licenses (an advantage if considering loss of privacy).
- Lack of equipment security and temptation to fraud inherent in a complete process located in many places.
- The difficulty of performing superior photography and counterfeit protection in a distributed environment in contrast to a specialized centralized facility.

The advantages and disadvantages of a centralized process are the inverse of the instant process. Both systems require adequate inspection and identification procedures in the application phase of license issuance.

The choice of which issuance procedure to use depends upon individual state requirements and the subjective opinion of motor vehicle officials as to which advantages are important and which disadvantages are unimportant. The present competition is advantageous to the public. Both systems generate attractive, durable licenses at a modest cost. The competition is now being extended to include security against counterfeit and we can be confident of technological improvements in the near future. It is anticipated that more companies will enter the competition and more states will change to photo personalized driver's licenses.

COUNTERFEIT AND ANTI-COUNTERFEIT TECHNIQUES

At present, there are so many loopholes in the license application procedure that it is easier to obtain a valid license using a false identity than to counterfeit a license. As soon as these loopholes are tightened, counterfeiting will appear more attractive to impersonators. There are several generally accepted truisms associated with counterfeiting. They are:

- Any technique will suffice against the non-observant inspector or clerk.
- An expert with adequate equipment and time can almost always spot a phony document.*
- In a realistic environment with heavy traffic and time pressure, any document can be counterfeited. It is only a question of the amount of time and money the counterfeiter is willing to invest.
- It is almost always easier to counterfeit a complete card than make partial alterations.
- The "name of the game" is to make the counterfeiter's cost exceed the street value of the document.

A professional artist described his technique for duplicating both a non-photo and photo license. It was impressive how easily it could be done and how small the capital investment was. It is inappropriate to itemize the counterfeiting steps he took, but a cost summary for counterfeiting is presented below:

Non-Photo License: A 5-color separated artwork of complex design takes about 40 hours including photography. Ten thousand copies can be made for \$15 and sold at a street price of \$5 each.

Photo License: It is considerably more difficult and expensive to counterfeit a license with a mix of photographic data and printed data because the counterfeiter must create personalized printed material early in the process. All subsequent operations on the document must be repeated for each license. Unlike the non-photo license, it takes about 4 hours to make each precise counterfeit photo license; therefore, the street price of such a license is in excess of \$100.

*A professional artist was not willing to accept this limitation. Some expertly counterfeited documents may be indistinguishable from officially issued valid documents.

The general requirement for making counterfeiting non-cost-effective is to produce a document that uses hard-to-get materials, requires large capital investment and employs difficult technology. Specifically an issuer should:

- Use hard-to-get paper (or plastic) with imbedded particles, watermarks, designs, etc.
- Keep a careful account of the material.
- Use inks that are difficult to color separate.
- Print designs with fine lines of the order of .001 inches.
- Provide accurate registration of fineline multicolor designs.
- Provide circular targets printed with highly accurate (.003") registered multicolors.
- Put many designs in the image area.
- Use high-resolution film not readily available to the public. Include a resolution chart in the image area.

It is very desirable that a person be able to detect the counterfeit using only his normal senses without the aid of computers or optical or mechanical devices.

There are at least three techniques used on some driver's licenses specifically designed to foil the counterfeiter. They are:

- Intaglio Printing, which is a high precision raised printing made with a high pressure steel press.
- Retro-Reflective beads, which are coated so that specific complex designs appear when observed under a directional light.
- Polarized Strip, which changes appearance when viewed with polarized light.

These techniques definitely increase the cost of counterfeiting; even so, "acceptable" counterfeits of two of the above techniques have been observed.

Attachment 1 describes possible additional anti-counterfeit and personalizing features of the driver's license. Fingerprints have not been recommended in this report because of the issue of personal privacy and the cost and complexity of verifying an applicant's fingerprint.

To improve document security it is recommended:

A COLOR PHOTOGRAPH OF THE DRIVER SHOULD BE A MANDATORY FEATURE OF ALL STATE DRIVER'S LICENSES.

EVERY STATE'S DRIVER'S LICENSE SHOULD UNIFORMLY INCLUDE THIS PERSONAL DATA: FULL LEGAL NAME, ADDRESS, DATE OF BIRTH, HEIGHT, WEIGHT, EYE COLOR, LICENSE NUMBER, SEX, SIGNATURE, AND EXPIRATION DATE.

ANTI-COUNTERFEIT FEATURES SHOULD BE EVALUATED WHEN VENDORS SUBMIT PROPOSALS FOR LICENSE FORMS.

SECTION V
COMPUTER USE

DMV COMPUTER DATA STORAGE

A subcommittee of the American National Standards Institute (ANSI) has studied the problem of which data elements should be stored in state DMV computers. Listed below, with any necessary explanation, are the 11 items recommended by ANSI under the heading of driver identification. Where ANSI considered the data element "optional", it is so noted. Forty-five other data elements that cover the areas of license control and status, history of driving violations, punishments and corrective measures are also recommended by ANSI for inclusion.

Identification Parameters

The data elements ANSI recommends be stored are:

1. Full name.
2. Present residence address.
3. Driver License Number. See recommendation in Section IV relative to tamper detecting algorithm.
4. Social Security Number (optional). In some states items 3 and 4 are identical. Because some state laws forbids the use of the SSN as a license number and because it has no error detecting capability, it is recommended that item 3 be distinct from item 4.
5. Sex.
6. Date of Birth.
7. Height (updated at renewals).
8. Weight (updated at renewals).
9. Eye color (optional).

10. Hair color (optional).

11. Race (optional). It is recommended that race not appear on the license.

The DMV computer record should also include at least two personal items which do not appear on the license. These items should be of the type that all applicants would know but which would be difficult for a potential impersonator to obtain. When the license issuance officer verifies the applicant's computer record, he would have this additional data to check with the applicant. It is suggested that the two pieces of personal data be:

- Mother's maiden name, and
- Name of high school or grade school attended.

In order to standardize computer storage at state DMVs, it is recommended:

STATES SHOULD ADOPT THE PARAMETERS RECOMMENDED BY ANSI WITH THE ADDITION OF THE TWO "HIDDEN" PERSONAL ITEMS.

STATUS OF ON-LINE COMMUNICATIONS TERMINALS

The advantages of receiving real-time response in from two seconds to two minutes from a computer are self evident. If a police officer must check the record of a speeding driver, he cannot hold the driver for several days waiting for mail verification from the computer. Similarly, it is more convenient for both the applicant and the DMV to minimize the license issuance delay by reducing computer verification time.

Different states have solved the problem of communication between field issuance stations and the DMV central computer with various degrees of sophistication and cost, such as:

- Ten states* have on-line terminals at all issuance stations.
- Five states are planning terminals at all issuance stations in the next two years.

*Florida, Maine, Maryland, Massachusetts, Michigan, Ohio, Oklahoma, Tennessee, Virginia, Washington, D.C.

- Twenty-two states have some on-line terminals.
- Nineteen states do not have any on-line terminals.
- Seventeen states have intentions of acquiring on-line terminals.

Without on-line terminals, the inspector does have the option of telephoning the computer center for a rapid check of a license application, but this option is rarely exercised. The actual monthly costs of rental for the terminal and dedicated telephone lines for two states are given in Table II. The cost difference on a per-terminal basis is due largely to the fact that Ohio's terminals are equipped with cathode ray tube (CRT) displays, which are easier to use but are more expensive.

TABLE II
Costs of On-Line Terminals in Ohio and Florida

	Ohio Terminal <u>with CRT</u>	Florida Terminal <u>No CRT</u>
No. of offices	212	96
No. of terminals	214	150
Total terminal rental cost/mo.	\$77,680	\$23,100
line costs/month	\$25,000	\$ 8,500
rental cost/terminal/mo.	\$360	\$154
total cost/terminal/mo.	\$500	\$210

Although on-line terminals are valuable for rapid computer verification, each state has specialized needs for intrastate data communication; therefore, no Federal standard can be established.

SECTION VI
INFORMATION EXCHANGE

DRIVER'S LICENSE CONTROL AND NATIONAL DRIVER REGISTER

Driver's License Control

Both interstate cooperation and Federal guidelines have established legal controls in the issuance process to verify that the license is actually issued in the true name of the applicant. The National Highway Traffic Safety Administration (NHTSA) Highway Safety Program Standard No. 5, Driver Licensing,⁶ requests the states to seek positive proof of full name, date and place of birth prior to issuance of the initial driver's license. Currently 47 states⁶ claim to comply with this provision, but inadequate computer storage capacity sometimes restricts the retention of place of birth.

Another interstate control of licensed drivers available to the states is in the form of the Driver License Compact (DLC) authorized by Congress in 1958. Twenty-nine states presently are members of the Compact,⁶ which requires member states to forward records of out-of-state traffic violation convictions to the driver records agency in the home state of the driver. Upon issuance of a driver's license in any state, the Compact requires that all previous current valid licenses be surrendered to the new state of issuance and returned by the driver licensing officials to the previous state of issuance. Section 6-101(c) of the Uniform Vehicle Code (UVC) also provides that out-of-state drivers surrender their old licenses. Eight additional states claim compliance with this section of the UVC. It is likely, however, that some states do not comply totally with the DLC and UVC provisions.

Many states have formed local regional agreements with respect to driver violations. In some cases, if a driver receives a speeding ticket while driving out-of-state, this violation is forwarded to his home state and entered in his computer record. Other agreements restrict these actions to more serious violations such as drunken or reckless driving. All of these control features are desirable and should be retained.

In Section III, we pointed out that applications for interstate transfer of driving privilege are particularly vulnerable to false ID fraud. A person presenting a stolen or counterfeit out-of-state license as identification can obtain a new and valid license through such a transfer application. To detect such a fraudulent transaction, it is necessary to check the license files of the state which purportedly issued the old license. At present, such fraud is detected some time after the fact (if at all), when the transferred license is returned by mail to the state of origin. To check all transfer applications for validity by interstate mailing before issuing new licenses would require a substantial increase in effort by the licensing agencies, would increase significantly their cost of operation, and would introduce new and undesirable delays in the licensing process. In order to increase the security of the license transfer process without introducing these problems, we propose a system through which computerized inquiries could be made by a license examiner in one state to the driver's license files in any other state. This would permit validation of transfer applications in a matter of seconds. A great deal of the hardware required to implement this proposal is already in operation. The license files are computerized in all states; as discussed in the last section, most states either have or are planning to obtain the on-line terminals which are also required for "instant" verification of license transfer applications. The remaining major element that would be required is a nationwide data communication system linking state DMV offices. The cost of such a system would be decreased greatly if it were made an "add-on" to an existing data system. The following subsections describe three operational nationwide data systems that could conceivably be adapted to this purpose: the National Driver Register, the National Crime Information Center, and the National Law Enforcement Telecommunications System.

National Driver Register (NDR)

The United States Congress established the National Driver Register (NDR) to assist each state in locating the records of drivers who had violated certain laws and had their licenses taken away regardless of where in the U.S. the violations occurred. The NDR provides a central driver records data base containing the names of drivers whose licenses have been denied, suspended, or revoked for any reason (except denial or withdrawal for less than six months due to a series of non-moving violations).

Although NDR is a voluntary service, full participation by every state is essential if it is to serve all the states effectively. Full participation includes the checking of all driver's license applications through the Register and the prompt transmittal to the Register of information concerning the denial or withdrawal of licenses by the states. This checking service enables state and Federal officials to avoid the issuance of a license or permit to an individual whose license has been denied or withdrawn by another jurisdiction.

If a driver has his license revoked in State A, this revocation is recorded with NDR. If the driver applies in State B for a license, State B requests a copy of his driving record from NDR. Upon learning of the revocation, State B is free to take whatever action it deems appropriate. The NDR is an information exchange and clearing house and does not dictate enforcement procedures to the states.

The NDR has listed about 5 million names of drivers whose licenses have been revoked. Each day it receives the names of about 5,500 people who lose their license, (often for lack of insurance payment). The NDR answers about 85,000 inquiries per day.

The activities of the NDR have been investigated by the Congressional Subcommittee⁸ on Constitutional Rights. It has been concluded that the NDR provides a valuable function in terms of traffic safety and does not conflict with any privacy laws.

The Safety Management Institute performed a study in December 1973 to determine how the NDR could be made more effective. They made several recommendations of major significance. They recommended that the NDR:

- Provide on-line terminals so state inputs and queries could be satisfied in minutes rather than days.
- Change the nature of the record storage to conform to a pointer/index record of revocations. The record would then provide the location of the revoked driver record rather than the record itself.

It is important to note that the NDR will detect only those drivers whose licenses have been revoked and who apply fraudulently for new licenses in their true names. An imposter using a stolen or counterfeit license to apply for a new license would not be detected by an NDR check. Only a check of the complete license files of the state which purportedly issued the license would detect such a fraud. It is not economically feasible to expand the NDR, which is designed to provide information on the "exceptional" driver only, to include the much larger number of valid license holders.

NATIONAL CRIME INFORMATION CENTER (NCIC)

The NCIC is a computerized information system established in 1967 as a service to all law enforcement agencies--local, state and Federal. The system operates by means of computers, data transmission over communication lines, and telecommunication devices. Its objective is to improve the effectiveness of law enforcement through the more efficient handling and exchange of documented police information.

The NCIC computer connects to 86 law enforcement terminals located in all 50 States, Washington, D.C., Puerto Rico, and Canada. Inquiries about criminals and stolen property can be made from any control terminal throughout the country with a response received in a few seconds. The NCIC is also connected to the NLETS system (discussed below) via a high data rate line; NCIC lines to Puerto Rico, Alaska and Hawaii help connect these out-of-continental locations into the NLETS system.

The NCIC computer has stored 5.6 million items of information⁹ in eight categories:

- Stolen securities - 1.7 million
- Stolen motor vehicles - .82 million
- Missing persons - .64 million
- Wanted persons - .16 million

- Stolen boats - 12,000
- Stolen license plates - .28 million
- Computerized Criminal Histories (CCH) - .79 million

Inquiries for information in one of these categories is meant to assist in the apprehension of criminals who commit crimes in more than one state. Seventy percent of rearrests are within the same state; therefore, the NCIC does not replace the need for a state criminal file.

As with the NDR, NCIC files apply to the "exceptional" individual and would not detect impersonation of a valid license holder.

NATIONAL LAW ENFORCEMENT TELECOMMUNICATION SYSTEM

System Description

The National Law Enforcement Telecommunication System (NLETS) is a computerized, high-speed message switching system created for and dedicated to the criminal justice community. Its sole purpose is to provide for the interstate and/or interagency exchange of criminal-justice- and criminal-justice-related information. The NLETS does not maintain computer files in the NLETS message switcher; a magnetic tape log of all transactions is kept to provide system statistical reports and management information. No message text information is retained in the magnetic tape log.

A computer system located at the Arizona Department of Public Safety in Phoenix, Arizona, supports the NLETS. The system has the capability to receive, store, and forward message traffic from and to all its user agencies. Message traffic includes administrative data from one point to one or more points. In addition, it supports inquiry into state motor vehicle and driver's license data bases.

The heart of the NLETS system is a pair of Communication Systems Computers located at Phoenix. High-data-rate telephone lines are used to provide direct computer connection to individual state computer networks. The state computers in turn are connected to state, county, and city networks. Users who are not yet ready to connect to their state computers are serviced by individual low-data-rate lines to a (Model 37ASR) teletype terminal. Irrespective of the line type, NLETS terminates their lines with a single Point of Entry (POE) to each state-

level user. The distribution of messages from the POE to individual end users is a state responsibility. A high-speed line also connects the National Crime Information Center (NCIC) to NLETS, and the U.S. Customs Treasury Enforcement Communications System (TECS).

Although NLETS is a national system, it is directly controlled by the 50 member states. Each state appoints an active member to represent it in the NLETS organization. Several states that have a regional community of interest are grouped together to form an NLETS Region. There are eight NLETS Regions. The state representatives in each Region elect a Chairman each year, and he represents the Region on the NLETS, Inc. Board of Directors.

The NLETS Network, with fully redundant hardware and software is operational 24 hours per day, 7 days a week to provide near-instantaneous response to inquiries originated at any point in the United States. The network was designed to handle up to 26,000 messages per hour distributed over 50 high-speed lines. Some large-scale users, such as California, Pennsylvania, Florida, Illinois and Texas, are currently sending and receiving over 50,000 to 70,000 messages per month. A total of 1.5 million messages were exchanged in January 1976 with 110,000 messages involving driver's licenses.

Applicability of NLETS to Driver's License Security

NLETS is a high-performance communication service that enables law enforcement agencies anywhere in the United States to exchange vital information within seconds. Because it already provides direct computer access to state DMV files, NLETS appears to be the most logical system to adapt for interstate validation of license applications.

As of May 1976, 37 states and 27 Federal agencies could obtain fully automated responses to driver's license inquiries, which means any on-line terminal connected to the NLETS system can access the individual driving record of an out-of-state licensee. Sixty percent of all driver records are available on this computer-to-computer basis. The driver's record and his physical description can be printed without any intermediate human intervention.

Fourteen states and one Federal agency are connected to NLETS via teletype. With these less sophisticated terminals, a human must intervene before the message is put on the NLETS system. This intervention may take the form of typing a few character approval codes or inserting a "torn tape" teletype message into the DMV computer. Although these are simple operations, because of personnel shortage and equipment tie up, they often have a major impact on message time. In an experiment two law enforcement administrators from two different states requested out-of-state driver records from six to seven other states. In automated states, the responses arrived within one minute. In two non-automated states, the responses took between 45 minutes and one hour. NLETS personnel believe non-automated responses often take even longer.

In states without any terminals, NLETS can still be accessed. The registrar can telephone the state location where the NLETS line terminates, make a verbal request, and subsequently receive a telephoned verbal reply. This procedure is awkward and is therefore almost never done.

In order to make rapid, nationwide interstate driver ID checking by local issuance offices a practical reality, the non-automated states with on-line terminals must make software modifications to permit fully automated responses and states without on-line terminals must obtain them. The capacity of the NLETS system must be analyzed to assess the impact on system performance that would result from adding routine license verification requests to the present message load. The system's primary purpose will remain the handling of high-priority law enforcement inquiries; significant delays in this service must be avoided. This could be done by instituting priority classes for NLETS traffic and by adding any necessary capacity to the network.

A STUDY SHOULD BE MADE OF THE PRACTICALITY OF INCLUDING ALL STATE LICENSING OFFICES INTO THE NLETS ON A REAL-TIME BASIS. SUCH AN ARRANGEMENT WOULD PERMIT ALMOST INSTANTANEOUS (COMPUTER-TO-COMPUTER) INTERSTATE EXCHANGE OF MOTOR VEHICLE AND DRIVER INFORMATION, AND IF PUBLICIZED COULD ACT AS AN ADDITIONAL DETERRENT.

ATTACHMENT 1

THE DRIVER'S LICENSES OF THE STATES AS
PERSONAL IDENTIFICATION
DOCUMENTS: SUGGESTED DOCUMENT SECURITY ELEMENTS

PREPARED FOR:

Mr. William Duggan, Chairman
Task Force IV
Federal Identification Documents of the
Federal Advisory Committee on False Identification (FACFI)

PREPARED BY:

Department of the Treasury
The Bureau of Engraving and Printing
Washington, D.C. 20228

June 21, 1976

INTRODUCTION

The de facto usage of a driver's license as a means of personal identification in day-to-day marketplace transactions by the general public is well known and, in a practical sense, transcends in frequency its usage as an identifier to the issuing and police authorities of the states.

Recognizing the general use of the driver's licenses of the states as primary identifiers, the Federal Advisory Committee on False Identification (FACFI) has recommended that Federal support be given the various states to lessen fraudulent usage of bona fide documents, deter counterfeiting, prevent alteration of the genuine issues, and diminish second party usage.

In recommending support for the establishment of standards to deter the fraudulent usage of driver's licenses, FACFI has recognized that not only are the intrinsic features of the license document of paramount importance, but that the systems interface relating to issuance, reissuance, and identity data authentication play a very important role. Concomitant to these factors, and conceivably in certain instances of greater importance to the individual states, are the procedures developed and in current use which best meet their requirements, not the least of which are those which relate to public acceptance and total systems cost.

In order to assist Mr. William Duggan, Chairman of FACFI Task Force IV, Federal Identification Documents, this Bureau has been requested to suggest general requirements for state driver's licenses which will address standardization of document security features to aid in greater deterrence of fraudulent usage. In this regard we recognize that such recommendations could entail a very high order of document-automated systems interfaces which may be approached in future, but which may be rejected by various states for a variety of reasons, including excessive cost, as well as procedural and public acceptance constraints. Therefore, in further recognition of the myriad of document production methods which could be proposed by various producing commercial organizations, an attempt shall be made to list those requirements of document security which may afford various orders of security dependent upon the desires of individual states, but which can also be interpreted as a genesis for the time effective development of minimal standards of acceptance to aid in thwarting a very real loss of million of dollars due to false identification.

GENERAL RECOMMENDATIONS FOR DRIVER'S LICENSE DOCUMENT SECURITY

The driver's license documents issued by the 50 states should provide protection against the following:

1. Fraudulent duplication-counterfeiting;
2. Alteration-forgery and changes in elements other than signatures and vital personal statistics of the bona fide holder, e.g., substitution of a photograph; and,
3. Second-party usage by consent of the bona fide holder, loss, or theft.

The procedural issuance, reissuance, and authentication procedures have been discussed. Important as these considerations are to a total system, the recommendations which follow pertain primarily to intrinsic features of the document.

A number of devices to enhance the intrinsic security of the document can be envisioned. Certain of these could interface with various automated systems ranging from a simple ultraviolet light to detect fluorescence to a "blackbox" detector to authenticate at authoritative levels. However, it is realized that one of the primary areas of consideration is the use of the driver's license for low level identification related to the visual aspects of the document. For example, for use in point-of-sale identification of the bearer paying for a purchase with or cashing a check, or by the highway patrolman in identifying the driver of a motor vehicle.

At these levels of detection, the document format must be one that is recognizable and still affords a high order of security against counterfeiting, forgery, and alteration. Attendant sophisticated features of the document will assist authoritative investigation of fraud, but in general, if interfaced with sophisticated detection-automation systems, will not provide first instance assurance of authenticity.

The inclusion of a simple specialized visual detection aid can attract the attention of the public to such an aid only. If the public does not look at all features on a document, but concentrates its attention on a particular device in the document, then this can serve as an inducement to counterfeiters to make a reasonable simulation of such a device. Therefore, the selection of such document deterrent devices must be made with care.

Construction of the Document

Dimensions. The document should be of a size which readily fits most wallets and billfolds, e.g., the size of certain credit cards.

Substrate. The substrate sheet material can be paper, card stock, or plastic of types not readily available in the marketplace. Examples are specially water-marked paper stocks, or substrates having visibly included colored fibers, planchettes, or other devices.

Front and Back Outer Surfaces. The substrate should be laminated with a durable plastic material. Consideration should be given to the imposition of an embossed design imparted to the plastic surfaces in the laminating process. This may aid in thwarting low-level photo reproduction by conventional means or with color copiers. It may also be desirable to emboss the holder's license number. This would permit merchants having credit card imprinters to imprint the license number on the back or face of a check being presented to him. The laminating system should be designed to prevent or make exceedingly difficult alterations to the license.

Design Format

The face and back of the substrate should bear well-executed multicolor printed designs which provide an order of protection against photo reproduction to force even the more sophisticated counterfeiters to use arduous hand-work techniques in attempting simulation of the documents. The unique characteristics of intaglio renderings from line-engraved plates can afford a high order of protection. Fine line multicolor offset or letter press visible and fluorescent printings can serve as an adjunct to intaglio or, if properly designed, can afford a lesser order of protection. If compatible with the laminating system and nature of the substrate, visible background tint printings executed with inks sensitive to chemical and solvent eradication techniques could be included to aid in thwarting alterations to signatures and other data.

Personal Vital Statistics

The name, address, and personal data relating to the bona fide bearer should be clearly imprinted, ideally with an indelible ribbon ink.

Personalization Devices

The obvious, readily discernible devices are the photograph, fingerprint, and signature of the bona fide holder. (Computerized tape memories related to the license number or vital statistics of the holder are valuable for investigative purposes. However, unless keyed for instant data retrieval by the merchant, these do not provide an expeditious aid to authentication. It is conceivable to provide restricted key listings of numerical relationships to the marketplace and police authorities for low-level investigative purposes, but one would suspect that this could be generally ignored by the busy merchant or highway patrolman.)

The photograph of the bearer should be current and a true likeness, preferably in color. It should be bound to the substrate in such a fashion to preclude the danger of removal and substitution. Another approach to impair photo substitution is to make the bearer's photo an integral part of the substrate. Envisioned approaches are: a photo-sensitive emulsion coating over the entire face surface of the printed document upon which a transparent type photo of the bearer completely covers the document face area; or, coating only that portion of the face surface of the printed document with a photo-sensitive emulsion coating upon which the photo of the bearer is to be confined. For a lower level of document security, a photo-presensitized unprinted substrate could be used to photographically reproduce design and other required elements as well as the photo of the bearer from photo negatives.

A fingerprint of the holder serves as an identifying feature. For low-level detection, it is subordinate in effectiveness to a photo. However, if possible, it should be included on the document to further attest to the identity of the bona fide license holder.

The signature of the bona fide holder should be on the document, preferably over a portion of the holder's photo.

CONCLUSION

The forgoing recommendations for the document security features which are suggested for inclusion in the driver's licenses of the 50 states are, in the main, addressed to assisting in the ready identification of the license holder at the primary level of detection by merchants, police, and others. These suggestions generally relate to what could be termed minimal

document security features. They have been put forth in addressing the nationwide necessity of reducing false identification transactions by those not having specialized detection devices, but only the use of the unaided human eye.

If requested, designated personnel of this Bureau will consult with the authorities of Federal and state agencies concerned with document deterrents to fraud.

APPENDIX D4

**A PROPOSAL TO UPGRADE THE
SECURITY OF THE STATE-ISSUED
DRIVER'S LICENSE**

**Ronald R. O'Connor
Polaroid Corporation
Cambridge, Mass.**

April 1976

D-163

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	D-167
PROBLEM STATEMENT	D-168
POTENTIAL SOLUTION	D-172
DRIVER LICENSING SYSTEM AND PROCEDURES	D-174
THE POLAROID PORTRAIT IDENTIFICATION CARD	D-180
ATTACHMENT 1 - DMV SURVEY	D-182

INTRODUCTION

The purpose of this paper is two-fold: one, to philosophically examine the roots of the present problem of false identification and the necessity in our society of personal identification; two, to present a potential solution to the general identification problem with the advantage and disadvantage inherent in the proposed solution.

It becomes necessary at this point to preface this document with a policy statement as to the position of the Polaroid Corporation on photographic identification cards. As one of the world's largest manufacturers and suppliers of photographic films and equipment we have been, since 1966, directly involved in the sale of equipment designed to make identification cards. As a result of our being a major supplier of identification systems we have developed a policy pertaining to the sale of our identification systems which reflects our concerns with the use of identification cards as they might effect the freedom and privacy of the individual.

On December 4, 1975, Peter Wensberg, Polaroid's Senior Vice President of Marketing, issued the following statement as to Polaroid's position on a national identification card:

"We (Polaroid) are neither opposed to nor supportive of the idea of a national identity card. If Congress were to enact legislation for such a program we would support it only if we felt the rights of individuals were fully protected. If there were the possibility of misuse of such a program, such as availability of copies for other purposes, citizen information files, etc., we would not support it.

A card with a picture and a signature is useful to the individual as a means of positive identification. Our concern is with the possible misuse of information beyond the purposes of identification."

PROBLEM STATEMENT

Since the closing of the American Frontier, dated at 1890 by some historians, our society has been expanding inwardly, and the need for an increasingly complex socio-economic system has been created.

In 1890 the United States population was 63 million. The gross national product was \$26.1 billion (1890 dollars). In 1975 the population had expanded to 215 million and the gross national product had risen to \$1400 billion.

This inward population expansion coupled with the material creativeness of our technological society and 20th century mobility changed the nature of social and commercial interaction from a system primarily relying on personal recognition of an individual to our present situation where 215 million people commercially interact in an uncountable number of times each day in a system which out of necessity cannot rely on personal recognition.

This system which has developed over the last 200 years, has produced a society which offers its inhabitants a standard of living unsurpassed anywhere else in the world. Educational, financial opportunities, social services, a free society, and the higher per capita income in the world make the U.S.A. a magnet to the rest of the world's population.

In the history of human societies there has always been a criminal element, a small percentage of the population who attempt to violate the accepted social and commercial customs for their own gain. In simple societies criminal acts and penalties are rudimentary (e.g., if you steal from your neighbor, and are caught, your neighbors might cut your hand off).

The degree of criminal activity in any society seems to be determined by a number of factors which include the following:

- The availability and amounts of goods and services.
- The size of the population.
- The numbers of opportunities, and avenues available for illegal gain.
- The severity of punishment weighed against the odds of being caught and punished.

If the above criteria are correct America in 1975 presents the optimum in fertile ground for criminal activity aimed at financial gain.

Most criminal activities aimed at financial gain require measures on the part of the criminal to get around the safeguards which have been, over the years, built into the commercial system being attacked. Almost universally a primary safeguard used to protect the commercial and government services from criminal incursion has been the ability of the requestor or user of those services to identify himself as the legal recipient of that particular service.

The degree of protection built into any system of services has traditionally been dependent, among other considerations, on the cost effectiveness of the safeguard system; e.g., you spend only enough to discourage the vast majority of participants in the system. The absorption of the loss as a cost factor of the service has until recently been acceptable to the American economy when it was examined in relationship to that particular service system being effected.

But when the entire socio-economic system is examined in 1975 and the financial losses due to criminal practitioners utilizing false identification are considered, we find that the multitudinous numbers of services and systems that lend themselves to fraudulent use for gain multiplied by the numbers of abuses on each system or service produces a staggering overall financial loss to the nationwide community.

The direct financial losses to the total system represent only a portion of the cost. The loss of tax revenue on the money taken out of the tax stream must be considered; the cost of participation in the community services welfare payments, food stamps, unemployment benefits, transportation systems, public utilities and school systems by non-taxpayers represents other hidden costs. In addition the amount of time, money and effort dedicated by commercial institutions and the criminal justice system needed to define and contain the criminal problems created by the use of false identification add up to a staggering financial burden for the American economy.

Specific Problem

If we accept the fact that a large percentage of nonviolent criminal abuses of our systems and services rely on the criminal's ability to identify himself as one legitimately entitled to use of that particular service or system (e.g., cash a check, obtain a U.S. passport, enter the United States, collect a welfare check, use a credit card, etc.) we then must examine the forms and types of identification cards and documents used in the United States and the manner in which they are fraudulently used. The majority of the following cards and documents are not issued as personal identification documents but only as designators that the recipient is entitled to some specific benefit or service.

Types of identification cards and documents in use:

Issued by State and Local Government

Birth Certificates
Driver's Licenses
Citizen ID Cards
Student Identification Cards
Welfare and Medicaid ID Cards
Employee ID Cards
Gun Owner Permits

Issued by Federal Government

Passports
Visas
Immigrant Alien Identification Cards I-15
Mexican Border Crossing Card I-186
Military and Dependent ID Cards (DD2, 3)
Federal Agency Employee ID Cards
Social Security Cards
U.S. Merchants Service ID Cards

Issued by Industry and Commercial Institutions

Travel and Entertainment Credit Cards (American Express, Carte Blanche, etc.)
Bank-Issued Credit Cards (Master Charge, Bank Americard, etc.)
Oil Company Credit Cards (Texaco, Esso, etc.)
Airline and Retail Establishment Credit Cards
Employee ID Cards
Student ID Cards
Medical ID Cards
Social Club, Private Club ID Cards (Playboy Club, Boy Scouts of America, etc.)

(The above list is not complete but is meant to represent the numerous personal identification documents in use.)

There are two general motivations for the use of false identification:

Short-Term Financial Gain

- Fraudulent credit card use.
- Cashing of stolen or counterfeit checks.
- Fraudulent welfare and food stamp claims, cashing of stolen food stamps or checks.
- Medicaid, drug treatment programs.
- Smuggling, international narcotics traffic.

Long-Term Financial Gain

- Illegal entry of aliens into U.S.
- Criminal evasion (known criminal suspects create false ID to avoid capture and prosecution).
- Known criminals maintaining second identity (aliases) to mask activities and to travel incognito within and outside U.S.
- Agents of foreign powers illegally entering and/or residing in U.S.

Because of the size of our population and the necessity to interact commercially on an extended credit basis many forms of identity documents have become necessary to facilitate these interactions. These services must be provided and the need to protect and limit the availability of these services is necessary; therefore, many identity documents are and will continue to be necessary.

POTENTIAL SOLUTION

One solution to the general problem of false identification is to provide an unquestionable base document or group of base documents which are readily available to any and all citizens. These documents must be issued under stringent control to eliminate fraudulent application and must not be susceptible to alteration or counterfeit. Such a solution would necessitate the creation of a single unique identification document and require its use by each citizen. Upon examination we find these drawbacks to this solution:

- A new mandatory single document would require registration of all citizens.
- Individual and specific personal data would have to be collected and stored centrally under control of the Federal government or an agency set up by the Federal government.
- The program would require long lead-time to becoming operative and would duplicate existing registration systems.
- Most importantly, this approach would be unacceptable to the citizens of this country.

If after reviewing and analyzing all other potential solutions the adoption of a national identification card document were recommended, it would seem appropriate, before any congressional action be taken, that the proposition be placed before the American people. A decision, to implement a national ID card policy deserves the attention of the entire population and as such would deserve being placed on the ballot for national referendum, possibly in the upcoming November election.

IT IS THE AUTHOR'S OPINION THAT THE CREATION OF A NEW MANDATORY NATIONAL IDENTIFICATION CARD IS UNNECESSARY AND UNJUSTIFIABLE WHEN VIEWED FROM THE POSITION OF EITHER THE CIVIL LIBERTARIANS, THE BUSINESS AND COMMERCIAL INTERESTS, LAW ENFORCEMENT OR THE TAXPAYER.

The solution to the problem of a universally available system of identification documents already exists and the existing mechanism can be upgraded to provide the security necessary to form a solution to the false identification problem without any additional infringements on the civil liberties of the citizen of the United States.

There is no single identification document in use at present which is available to every citizen of this country, but there are two documents being issued of which one or the other is available:

- 1) The birth certificate and/or
- 2) The state-issued driver's license. IN POINT OF FACT, WHEN WE EXAMINE THE AVAILABLE INFORMATION ON THE TYPE OF FALSE IDENTIFICATION USED MOST PREVALENTLY WE SEE THAT THE VAST MAJORITY OF INCURSIONS REVOLVE AROUND THE USE OF EITHER OR BOTH THE BIRTH CERTIFICATE AND THE DRIVER'S LICENSE.

It seems most appropriate to concentrate our efforts on eliminating the loopholes in both of these areas as the solution to the false identification problem rather than attempting to create a new document. (As either one or both of these documents are used to generate illegal access to other forms of available identification and credit cards, they would most probably be used as identification prerequisites in any national identification card program, therefore compounding the identity crisis, not correcting it.)

The system of birth certificate issuance is not the author's area of expertise but must be dealt with, at least superficially, if this proposed solution is to be considered. Rather than attempt to describe the present systems of issuing birth certificates and then offer remedies, I propose the following remedies in such a manner as to make obvious the system's present problems.

- 1) Birth certificates should be nationally standardized and serialized as accountable documents. They should be produced on counterfeit proof non-alterable stock.
- 2) Unofficially-issued photocopies should not be acceptable as proof of birth.
- 3) A central agency should be given the responsibility of maintaining a cross-indexed file of all future births and deaths on a national basis.
- 4) Each state should centralize birth and death certificate information, cross-indexed, in a state vital records office.

- 5) All applicants for birth certificates should be required to apply for their certificate in person at a county seat, vital records office or police station.
- 6) All requests for birth certificates should be filed on a standardized application that requires information over and above date of birth and parents' names. This additional information should be of a nature not readily available to persons other than the actual individual.

The necessity of eliminating the avenues of obtaining a falsely issued birth certificate will become obvious when the reader realizes that the weakest link in the security chain of driver's license issuance is in those instances where driver's license issuing authorities must rely on a birth certificate as the sole form of pre-requisite personal identification.

THE AUTHOR'S RECOMMENDED SOLUTION TO THE FALSE IDENTIFICATION PROBLEM IS TO ACKNOWLEDGE THE STATE-ISSUED DRIVER'S LICENSE AS A PERSONAL IDENTIFICATION DOCUMENT. BEFORE THIS CAN BE DONE HOWEVER, CERTAIN STANDARDS HAVE TO BE APPLIED TO THE EXISTING DOCUMENTS, COUPLED WITH REFINEMENTS OF THE PRESENT SYSTEMS OF ISSUANCE.

The following section in this report attempts to describe the basic license issuing methods and to point out how these systems could be improved to alleviate the false identification problem nationwide. Attached at the end is a summary of the telephone survey conducted of each Department of Motor Vehicles. (Attachment 1)

DRIVER LICENSING SYSTEM AND PROCEDURES

If after reviewing this proposal the FACFI sees some potential merit in the proposed solution, it would be advantageous to convene a special committee composed of members of the American Association of Motor Vehicle Administrators to examine, define, and determine the viability and possible acceptability of this solution to the administrators of each of those state offices responsible for the issuance of the driver's license. It is obviously beyond the scope of the author to consider the myriad statutory, logistical and administrative problems which this proposed solution could present to the motor vehicle administrators.

Driver's License Information

The most requested, used, and accepted form of identification in use today is the state-issued driver's license. There are 215 million people in the United States; 120 million have been issued a driver license. The driver's license is issued as a privileged document the sole purpose of which is to enable an individual to verify that he has been authorized to operate a motor vehicle on public roads. It is not issued as an identification document. But the fact remains; because of the necessity of possessing a driver's license in our society and the issuance controls imposed by the state authorities, it has become the standard form of accepted identification. As testimony to the recognition of the driver's license as accepted personal identification, 34 states make available a citizens ID card, for non-drivers. The non-driver citizen ID card is generally issued by the same authority that issues the driver's license.

A recent examination of the U.S. population by age shows that the 120 million licensed drivers represent 83% of the adult population (145 million people 18 or older). If we can assume that the vast majority of criminal incursions utilizing false identification are perpetrated by those older than 18 and younger than 40, we find that this criminal element fits into the group of 120 million licensed drivers. If we accept the fact that the state-issued driver's license is the most acceptable form of personal identification in use today, we must conclude that it is also the document most often used as fraudulent identification by the criminal element. It follows then that we must examine the driver's license issuing systems to determine how a fraudulent driver's license is created.

There are four ways of obtaining a fraudulent driver's license:

- Alteration of information on a validly issued license.
- Use of a stolen or lost license by an individual posing as the original owner.
- Outright counterfeiting of the driver's license form.
- Fraudulent application leading to the issuance of a valid license.

To our knowledge there are no statistics available as to which of the above methods is used more often in crimes that utilize the license as false identification. An evaluation would depend on two factors: the seriousness of the crime (e.g., a minor buying beer, or a criminal perpetrating a \$1,000,000 bank fraud), and the inherent design security of the local license (e.g., non-photo paper license with typewritten

information vs. photo license with computer print, security validation and security lamination).

WITH THE APPLICATION OF PRESENT SECURITY DOCUMENT TECHNOLOGY THREE OF THE FOUR METHODS OF OBTAINING A FALSIFIED LICENSE COULD BE CLOSED.

License alteration can be eliminated by:

- More effective license design and production.
- Use of special type fonts not readily available to the public.
- Photographic reproduction of license data, reducing information to the point that it becomes virtually impossible to alter without detection.
- The use of background ghost seals and other verification features which, if alteration is attempted, become obviously effected.

Counterfeiting can be virtually eliminated by the production of licenses containing security verification features such as intaglio printing, retroreflective film, polarizing stripes, etc. These materials when incorporated into a license cannot be rephotographed to reproduce their verification capabilities. They also cannot be removed from a lost or stolen license to be incorporated into a counterfeit document, as they destruct when separation from the original license is attempted.

Stolen or lost licenses become valueless to anyone but the owner if they contain the subject's photograph and signature, and contain counterfeiting and alteration countermeasures.

The fourth method of obtaining a driver's license to be used fraudulently -- fraudulent application leading to the issuance of a legal document -- is the best and safest method to obtain an illegal but valid document. It is also the most difficult loophole to close. An understanding of the basic driver's license issuing system becomes necessary to the reader at this point.

License Applicants

There are three basic categories of driver's license applicant:

- 1) The renewal applicant. He presents a license that has expired to the issuing authority. The authenticity of the document is verifiable by examination of the old document by an assumedly capable individual, the license examiner. If it contains a signature and/or a photograph, the examiner can visually verify that the applicant is the owner of the document. The only problem area presented with the renewal applicant is the individual who has already obtained a legally issued license under a false name; he would theoretically be issued another illegal but valid license. (Approximately 70% of all license issuance fall into the renewal category.)
- 2) Duplicate license applicants. An individual that has physically lost his license obviously must apply for a duplicate. An application containing name, address, license number if known, date of birth and signature must be filled out. In most states the duplicate license is not issued until it is verified that a previous license has been issued and that the information on the application, including signature, matches the application on file. (Duplicate license applications represent approximately 10% of all applications.)
- 3) Original license applications. There are two categories for an original license application -- people moving from another state and residents of the state who have not previously been issued a driver's license.

When an out-of-state applicant requests a license, he must in most states (45) surrender the license in his possession from his previous resident state and fill out the standard application. In theory, all states verify the authenticity of the license surrendered with the issuing authority in the home state and run a revocation check with the National Driver License Register in Washington. Unfortunately, because of the long delays that can be encountered through inquiries by mail, many states issue original application licenses without waiting for verification from either inquiry.

State residents requesting a license for the first time must show proof of identity; birth certificates are usually required. Most applicants in this category are

teenagers and do not fit into the criminal profile. A 35-year-old man applying for an original license and stating he has never had a driver's license in any state should come under suspicion and be required to produce many forms of identification.

Attempts to obtain a valid but illicit driver's license are made in two ways:

- An original applicant, supposedly from out of state, affirms that he has never been issued a license in any state. Countermeasure: Verification of applicant's previous address; cross-matching of applicant-supplied information, description, etc. with previous state of residence; requirement for at least three forms of identification; and, after verification, mailing by non-forwardable mail of processed license to address given.
- For duplicate license requests, the fraudulent applicant relies on the known existence of an individual possessing a valid license. The fraudulent requestor hopes to have his signature and/or his photograph on a license with someone else's name. Countermeasure: All license applications should contain some personal data which does not appear on the issued license and which is only known to the actual applicant, e.g., mother's maiden name, father's first name; all requests for a duplicate license should be checked against original applicant's signature and require re-verification of generally unknown personal data mentioned above; requirement for at least three forms of identification; and, after verification, mailing of processed license by non-forwardable mail to address given.

If a decision should be reached to acknowledge the use of the state-issued driver's license as an identification card, the following measures should be instituted:

- Standardization of procedures to guarantee the authenticity of all license applicants.
- Standardization of driver's license numbering systems to simplify interstate cross-checking for verification of information.
- Computerization of each state's license data base for both alpha and numeric access.

- On-line terminal capability at each license issuing office for license applicant verification.
- Interfacing of each state's computer to allow verification of interstate applicants.
- Computerization of the National Driver's License Register with state inquiry access electronically.

The Physical Document should be protected:

- There should be standardization of information on all driver's licenses.
- All licenses should contain a color photo of the applicant.
- All licenses should contain a counterfeit-preventing verification material which is non-removable and non-photographable.
- All license documents should be serially numbered for cross-reference and accounting purposes.
- All licenses should contain applicant's signature.

In addition to the above, all states should make available a non-driver ID card which would be recorded and issued under the same stringent procedures as a driver's license and contain the same counterfeit and alteration proof verification devices.

In the author's opinion there is no way to totally satisfy the privacy advocates' and the civil libertarians' concerns in issuing an identification document, whether it is a driver's license or some other voluntary document. But the decision to offer such a card can be made to include some basic safeguards to the individual's liberties:

- The document to be issued should be offered on a voluntary basis.
- Citizens who decide to apply for an ID document must be made aware of how the personal information they are offering will be kept and used.
- If the card is to be personal ID document issued for the protection and benefit solely of the citizen who uses it, copies of the subject's photograph should not be surreptitiously kept on file. The public must be assured that the document will not be used as a vehicle to collect fingerprints and mugfile pictures which at some future date could be used for repression.

THE POLAROID PORTRAIT IDENTIFICATION CARD

The Polaroid identification card was designed to provide protection and convenience for the individual. Polaroid Corporation has developed and sold the systems that produce the card with this principle in mind. We have refused contracts or turned away from sales where we felt the individual's rights and needs were not of paramount consideration.

The Polaroid portrait card provides four forms of protection for the individual. The first two are common to any system which produces a color portrait identification card. The second two are uniquely associated with the Polaroid process. The card:

1. Helps to solve the broad problem, i.e., keeping unlicensed drivers off the road, preventing fraudulent use of credit cards, making it impossible to cash stolen checks.
2. Provides the only means of quick, positive identification. You can prove who you are; a number, a fingerprint, a written description, a computer card will not identify you on the spot.
3. Is virtually tamper proof. Your picture cannot be separated from the card without destroying it; the card cannot be changed or adapted to someone else's use.
4. Prevents secondary use being made of your picture. The Polaroid process is a one-step process; there is no usable negative. You carry the picture with you. You are protected from the existence of a negative file which might be used as an instrument of control or surveillance. Copies can be made of the picture, but the system is designed to produce a card for the use of the individual only.

Where local, state or national laws require that a negative or copy be made at the same time as the picture, Polaroid will participate in the program only if the individual is aware that a negative or copy of his/her picture is being retained.

The convenience of the Polaroid system is obvious. The picture can be taken and delivered to the individual on the spot. There is no chance for error or having an unsatisfactory picture, no need to return at a later date to have the picture taken over again.

There are legitimate concerns on the part of many today about identification programs that attempt to control rather than serve the individual. Polaroid Corporation shares these concerns. We have designed our system with the protection of the individual, his rights and his property uppermost in our minds. We have not sought to supply the system for uses that are indifferent or antipathetic to this goal. While we cannot control all the uses of the system, we have refused sales that seemed to threaten the rights of the individual, and we plan to continue to do so.

ATTACHMENT 1

State: _____

Driver's License Procedural Information:

		<u>Yes</u>	<u>No</u>	<u>Other</u>
What identification is required:				
Renewal license applications	Accept expired lic. or renewal notice.	43	6	2
Out-of-state original applicants	Accept valid out-of-state lic.	47	2	2
First time resident original applicants	Accept birth cert., passport, military ID	47	2	2

Do you hold up issuance to out-of-state original license application until verification is received from the National Driver License Register and the applicant's home state? yes 8 no 43

Is it mandatory that out-of-state original license applicants surrender their existing license? yes 45 no 6

Are the people who accept license applications state employees? yes 44 no 6 optional 1

If the answers to the previous questions is no, please describe who accepts applications: _____

Electronic Data Processing Capability

Are your driver license records computerized? yes 47 no 3 Opt. 1

If no, when will they be _____

Can you access license records both alpha and numerically? yes 44 no 6 no reply 1

Do you have on-line license inquiry terminals in field offices? yes 22 no 24 optional 2 no reply 3

If no are you planning eventually to have this capability? yes 17 no 8 no reply 4

License Document Description

Does your license contain the following?

Applicant's signature?	yes	<u>51</u>	no	<u> </u>
Date of birth?	yes	<u>51</u>	no	<u> </u>
Date of issue?	yes	<u>42</u>	no	<u> </u>
Date of expiration?	yes	<u>51</u>	no	<u> </u>
Height,weight,color of hair and eyes?	yes	<u>46</u>	no	<u> </u>
Applicant's address?	yes	<u>51</u>	no	<u> 1 </u>
Applicant's photograph?	yes	<u>32</u>	no	<u> </u>
Is the license on security paper?	yes	<u>25</u>	no	<u> </u>
Is your license laminated in plastic?	yes	<u>28</u>	no	<u> </u>

Does your license contain any alteration or counterfeit prevention materials or technique for? yes 44 no 7. Please describe

Does your license contain an accountable document serial number in addition to the driver license number? yes 28 no 22 opt. 1

How is your driver license number determined? _____

Does your driver license application form request any personal data, such as place of birth, mother's maiden name, wife's first name, fingerprint, blood type? yes 9 no 42. Please describe

Include personal data (other than blood type or medical)

Does your state offer a citizen ID card? yes 34 no 17

If not, has legislation been introduced in the past year to do so? yes 9 no 8

APPENDIX E
OTHER PERTINENT MATERIAL

This appendix contains material that is of interest in defining some of the problems of false identification but which could not be included in other parts of the report.

Appendix E1 contains excerpts from The Paper Trip, an anonymously authored manual that first appeared about 1968. It is likely that this underground publication is responsible for disseminating many of the techniques used in false identification by those eager to benefit from this illegal activity.

Appendix E2 reproduces a letter from Mr. G. Pat Bland of the Western States Bankcard Association that summarizes the early findings of Mr. Bland's investigation of false ID fraud in applications for bank credit cards. We feel that these findings represent an important indication of a type of fraud whose scope and impact are only now gaining recognition.

Appendix E3 is a summary of Federal laws that relate in some fashion to false identification. Compiled by Mr. Kenneth Gibson and two associates who served as legal consultants to the FACFI, it can serve as a resource to legal scholars and as an illustration of the present fragmentary approach of Federal law to the problems of false identification.

APPENDIX E1

**THE PAPER TRIP
(Excerpts)**

THE PAPER TRIP*

Although THE PAPER TRIP covers virtually the entire range of useful ID, very few persons ever need more than half a dozen or so at the most, even for the most elaborate schemes. Everyone must visualize for himself just what kind of person he needs to be, and from there set out to complete his profile by acquiring the most effective paper. It's actually bad to overdo the amount of ID forms, as the most essential element of good ID is completeness. Your ID has to "add up" to a reasonable person. Quality in the assortment must always come before quantity. Each person has to decide for himself his particular needs and image. There are no "magic formulas" inasmuch as people and situations vary in their demands for specified ID. With this in mind, let us begin our examination of the various kinds of ID and how they can be obtained.

BIRTH CERTIFICATES

ALL ID STARTS WITH A BIRTH CERTIFICATE. With this document, issued by the Government itself, one can obtain all the other forms of official ID such as Social Security cards, driver's licenses, police ID and passports. The secret to creating an alternate identity then, is to obtain a birth certificate in another name. THE PAPER TRIP will now give you the exact details of three different methods for obtaining a useable birth certificate directly from the government.

Please notice here at the outset, however, that the PAPER TRIP never recommends using government ID that is NOT issued by various agencies themselves. Forget using phoney birth certificates, stolen Social Security Cards, doctored driver's licenses and purloined passports. They're not worth the paper they're printed on, and are absolutely worthless for disappearing. The trick is to have the government issue you DIRECTLY the various forms of ID you need. And all the information you need to get started is on a regular birth certificate -- someone else's, that is.

But who is this "someone else"? Obviously it can't be someone who is now living, since you would be duplicating an existing set of ID, which could lead to an early and easy detection. The "someone else" must, then, be a person of your sex, race, and approximate age who is no longer living and, thus, has no further need of ID under his name. The problem lies in finding such a person and ultimately obtaining his birth certificate.

*Author unknown, undated (Circa 1968).

Three successful methods will now be explained, all of which enable you to receive an unquestionably valid birth certificate from any county recorder. It will be found filed in an official government archive and a copy marked "registered," "verified," or "certified" will be sent directly to you in the mail if you want.

OBITUARY METHOD

This first method lets you take over "living" for a person who has just recently died. Take any newspaper and scan the obituary columns, look for a person who has died within a few years of your present age. An out-of-state paper is sometimes safer, especially if you live in a small state. Many such papers can be found at the local library. Once you've located a good prospect, you should feel comfortable about the situation, place, and possible family connections before going after his birth certificate.

The next step is to write the funeral home, cemetery, or even the family, expressing regret that your old school friend, service buddy, or boyhood pal passed away, and that you'd like to be sure it was even him. If they would be so kind as to send you his birth date and place of birth, it would bring you greater peace of mind, etc. Any facts gleaned from the obituary notice would be excellent points of reference. Imagination in your letter of inquiry will gain you even more information regarding the person's background, life situation, etc.

When you get the facts you need simply write the clerk of the county where the person was born, using an appropriate title such as "Office" (or Department of "Vital Statistics," "County Records," "Bureau of Vital Records," "Birth Registrations," etc.), and request a certified copy of "your" birth certificate.

Enclose \$2 (the most common fee) and you should receive it in a few days through the mail. Incidentally, the county clerk or recorder will have his office and files at the county seat. A quick check of an atlas or good encyclopedia will tell you which city or town this is.

If assuming your new name for this purpose seems too direct or "up front," use a letterhead, such as that of an attorney or an investigating agency telling them you want the birth certificate for your company's group life insurance policy, you are requesting a certified copy of so-and-so's birth certificate for security clearance. Include the fee, naturally. You'll get it fast, no questions asked. Public documents are always available.

Of course, you can also request and receive the document in person particularly if the birth certificate is recorded in a large, populous county. You'll receive it all the faster this way. Avoid the personal appearance, however, if you're going after someone who was from a rural area. There's always a good chance the clerk might have known the person or have heard of his recent demise. Reason must always prevail.

In the Obituary Method you have to remember that if you use the birth certificate of someone who had already entered adult life, he more than likely had contracted debts, had Social Security number and registered for the draft. He might have been married, had a police record, or maybe even had a few outstanding warrants....

This type of birth certificate is strictly lightweight, in that you don't have much assurance of remaining hidden very long. It's good for a check or credit game, a wild weekend or two, or for disappearing in a hurry. By that time, however, you're ready for the master type of birth certificate and might as well have gotten it in the first place.

OLD NEWSPAPER METHOD

The birth certificate you obtain by using this method enables you to "become" a person who died long before he got entangled in the paper morass you're now trying to escape. Again, his birth date should be around your own, but you don't have to go tripping through graveyards to look him up. It's been done, and it works, but there's an easier way. Go to the main library of any large city, university or college, or a newspaper's principal office and take a look at the old newspapers recorded there on microfilm. Choose a year in which you would have been no older than ten and begin looking for articles in which a young child of your sex, race, and present age then was killed in some kind of accident like fire, auto, or drowning. The best possibilities would be those in which the entire family was wiped out, as there would be little remembered of them by now.

Check the obituaries too, especially for deaths of children under the age of five. Under this age, at least 90 per cent of those who die do so in the same county they were born. Make sure the date of the newspaper is such that the age of the deceased and your age, at that time, were roughly equal.

In writing for the birth certificate, unless the article or obituary states where the child was born, ASSUME that he was born in the same county where he died. Request a certified copy either as

that person, or an employer or investigator who requires it in order that you may hire that person, approve him for special clearance, or whatever. If that particular county has no record of the birth, try either a populous neighboring county or submit another name. You'll find, though, that many newspapers, particularly in rural areas, are amazingly complete in their details of tragedies in which a spectacular accident killed several or all members of a family. Everything you need to know will be right there in front of you.

While you're poring over the microfilm, it would be a good idea to compile a list of at least half a dozen good possibilities. A few might understandably prove useless for you (wrong race, for example), or you might want to construct multiple ID's.

The commercial applications of this scholarly invention are virtually inexhaustible. So long as conditions make it difficult for people to get by with their own names, there will be a continuing and increasing need to disappear by creating other ID's. Nuff said.....

GOVERNMENT-ISSUED I.D.

Social Security Card

Once you have a birth certificate you need, apply for a Social Security card at any Social Security office. All the information you need to complete the application card is right on the certificate, so merely fill in the appropriate blanks. The application can then be mailed in to the office whose address is printed on the back side, and your card should arrive within a week or so. There is no fee for this card.

If you apply in person and are queried as to why you haven't had a card before, tell the inquisitive bureaucrat that you have always earned a living by working on commission. Such salesmen are exempt. Remember, too, that if you are assuming the identity of someone who has died recently, you will more than likely be applying for a duplicate card, not a new one. Note on the application (Box 10) that the questions are designed to determine this difference. Since you may be uncertain about the appropriate answers indicate either "unknown" or take an intelligent stab at it. The result will be the same, your card will arrive shortly in the mail.

Driver's License

The driver's license has become the most commonly accepted form of ID in the U.S. Each state has its own administration for obtaining them under such titles as "Department of Motor Vehicles,"

"Transportation," or "Public Safety," etc., and its only requirement for eligibility is proof of age, for minors. A certificate of birth or baptism is always acceptable. Even if you have no ID, tell the clerk you lost your wallet or that you have simply never had a license before. Check your particular state's requirements and make sure you have the necessary papers and answers before applying. Your Social Security number is used on the license in Alaska, Indiana, Iowa, Massachusetts, and Mississippi. It does not appear on any of the other states' licenses.

As of 1971, a total of 29 states do NOT use a photo on their licenses, but that leaves 21 who do and here they are: Alaska, Arizona, California, Colorado, Delaware, District of Columbia, Georgia, Idaho, Louisiana, Massachusetts, Montana, New Mexico, North Carolina, Rhode Island, South Carolina, Michigan, Texas, Utah, Virginia, Washington and Wyoming.

An excellent book which provides basic information of each state's driver's license, including color reproductions of samples, is Driver's License Guide, \$3.95, which can be purchased by mail from Driver's License Guide Company, 1492 Oddstad Drive, Redwood City, California 94063.

This book is used as a basic tool by law enforcement and business men in combating criminal deception. To quote its introduction, "Increased mobility, and economy styled on the use of check and credit cards, and grossly in fraud-related crimes, demand improved control." (Emphasis is ours.) A word to the wise should be sufficient. ALWAYS get your Government ID from the government itself. Give them the paper they want and you will get the paper you want.

CREDIT CARDS

Professional ID inevitably includes the full range of commercial cards -- both paper and plastic. Although a few companies are beginning to use customers' photos on the card, as a class, they generally have no personal ID information whatsoever. Your name, signature, account number, and dates between which the card is valid are about as far as they go in providing individual data. The rest is stored in their computer file based on your original credit application.

In today's increasingly cashless society, credit cards are becoming the control-label link between people, income, and property. They are immediately accepted for a multitude of specific financial jobs and in most transactions, they are the only ID required. THE

PAPER TRIP considers them ID and, thus, includes here its own ideas on how to obtain them. What you do with them is of course your own business.

The first rule, unquestionably, is DON'T USE SOMEBODY ELSE'S CARD!!! Much too dangerous and criminal. Infinitely better is to get the credit card companies themselves to send you their cards, but under any name you choose. The credit companies and banks also issue these cards and are anxious for your trade, and doubly anxious to issue the real card to all those who qualify. So the secret is OBTAIN YOUR OWN CARDS LEGITIMATELY!!! You do this by studying their brochures and applications to determine more or less what they expect. Even though your new name will have no existing credit record, a \$400 minimum deposit at a large bank will put you on the road to a geometrically expanding credit rating. An excellent book which outlines this unbeatable method of obtaining credit is How to Have Triple A Credit Within Thirty-Days, Continental Advisor Manuals, Box J-200, Hallandale, Florida 33009 - \$8.98 by mail.

To make sure your credit application gets accepted, you must keep in mind what the lender is looking for. For his approval, he's generally going to want to be sure you have most of the following characteristics:

1. A savings account and/or a regular checking account. The \$400 minimum balance gives you a "medium" rating on your savings account, which is "good."
2. Income level of at least \$125 per week. Over \$15,000 a year, and the blessings of affluence are instantly yours with abundant, virtually unlimited credit.
3. Good credit history: regular payments and no "binges."
4. Employment with the same firm for at least the last three years.

NOTE: If you can't easily meet the credit and employment requirements of points 3 and 4, you might use this proven technique: Have someone answer two different phone numbers for you, one as your place of employment and the other as a creditor from whom you have borrowed. A call from the lender to verify how long you've worked for a firm (three to five years is perfect) and the kind of credit record you have (payments all made on time, even early) will result in approval for just about any credit card you wish. Department stores, furniture stores, oil companies, Master Charge, BankAmericard,

American Express, Diner's Club, Carte Blanche, et al, are lined up and waiting to have that new account of yours filed with the time purchases of whatever your heart desires. So help them out.

5. Long time residence in the area, preferably in your own house. At worst, no more than two moves in the last five years.
6. Age should be over 25 -- 35 to 65 is best.
7. Occupation in a professional category (all but aerospace, that is) -- executive, doctor, salaried sales manager, proprietor, minister -- all of these are good.

All of these characteristics, even age, can be constructed and supplied on demand. Give them whatever information they require and they'll put you in business. Provide two different telephone numbers, one to verify employment and the other to verify your credit rating and they are satisfied. Set up a proper bank account in advance and their credit check will be completed. Place of residence is almost never checked, so choose a suitable address and have the card mailed to you in care of your business address, which can be a P.O. Box.

Never worry about personal "references," either, because they are never checked out. The only reason they are ever requested is to make you feel more responsible for your actions. A psychological play. Provide them though, by listing first-class references such as doctors or ministers: get their names and addresses from the phone book, freezies.

Most credit applications can now be handled by mail, which is almost more than you could ask for. Supply the required information on paper, and they're delighted too. Once you get your cards, here are a couple little known facts worth remembering.

1. When a clerk accepts your card as payment for any merchandise, the title to the goods is then yours. Legally you are paying in full, not requesting a loan. What this means is important. You can now sell, trade, or even borrow against your new property without one word to the credit company. They have extended your credit on the basis of your ability to repay, not on the nature or amount of the property you own.
2. In the case of Master Charge and BankAmericard, you can own as many of these cards, under the same name, as there are banks to issue them to you. They must be different

banks, however, and not just branches of the same bank. If you qualify at one bank, why not just apply at the others as well? They all want your business. By having four such cards with billing dates a week apart, you can easily get 90 days free credit. Add another four and the banks will carry you free, for 90 days. The trick is in using the card with the most distant billing date, as well as taking advantage of the cards cash loan features. Ask your friendly banker all about it.

Credit is easy to get so use it. The pretty plastic cards put out by the credit merchants are marvelous, even impressive ID, and can be used in a most exciting manner when you know that YOU are always carrying the last trump that of taking the paper trip. Go by the rules and there's no way of their distinguishing between real accounts and constructed accounts. Only when you "disappear" does the reality of the Paper Society become apparent to those who push it the most. By then, of course, you will have already been notified that your application for the new account, under a "new" name, natch -- has been enthusiastically approved, and that your new card will be arriving shortly. Same song, second verse....

With credit cards in hand, you provide the finishing touches to unquestionably good ID. Credit cards are the Paper Society's ultimate cover of respectability, and the paper tripper now knows how to avail himself of their endless bounty.

HANDY HINT: In supplying credit references beyond the one which your friend will "verify," you should remember that some firms (especially department stores and credit unions) will not give out their credit ratings to anyone, so, if you supply one or several of these references, you can be fairly certain that they will not be checked out. The lender knows he can't verify your "reference," but he will definitely not tell you that he will base his lending decision on the assumption of your honesty....

You are the new person, and never doubt it! If you don't, no one else will either! Take it from a pro, who else would you be if you weren't "you"....?

WHY, YOU CAN EVEN PROVE IT, "CERTAINLY, JUST CHECK MY ID...."

APPENDIX E2

LETTER FROM

WESTERN STATES BANKCARD ASSOCIATION



12631 E. Imperial Hwy., Suite 107-B, P.O. Box 2767 Santa Fe Springs, California 90670 (213) 868-0531

May 11, 1976

Mr. David J. Muchow

Department of Justice
Criminal Division
Washington, D. C. 20530

Dear Mr. Muchow,

In January 1975, we formed the first, and possibly the only, investigative section devoted exclusively to combating the fraud application menace. Our primary thrust was in the early identification of the fraud application and the dissemination of the applicable data to the credit industry. Once identified and the losses curtailed, we could then focus our attention on the prosecution aspects.

We learned that there were numerous well organized groups operating in California with ties to other states. The majority of the activity appeared to be centered in Los Angeles County, however we have now found that there is considerable activity in most major metropolitan areas within the state. We have intelligence information indicating that operations were planned in Hawaii, Seattle and Portland. In checking the travel of some of the suspects, we found that they travel and communicate with persons throughout the United States. In one instance, one major violator has been in South America and no one knows the purpose of this trip. We do not know if a false passport was used during this trip.

These organizations are involved in the establishment of phoney credit files, loan fraud of all types and phoney businesses, some of which go so far as to file articles of incorporation to further their devious ends. Most of the better organized groups utilize fraudulent identification to insure success in their ventures.

One such business averaged in excess of \$5,000 per month in deposits on Master Charge Cards that were all obtained via fraud applications. Inspection of this "television store" revealed it to be a "store front" operation. A neighborhood canvass revealed that the business was never open and the stock visible through the window could in no way support deposits of that amount. One of the principals involved in this operation was discovered to have thirteen California Operators licenses issued to her, all with fictitious names. All the names

had been used to obtain credit with the combined losses being in the thousands of dollars. This female and her male counterpart were found to have deposited \$98,000 in savings accounts in 1974, alone. Of course, they drove Cadillacs and lived in a home valued at \$85,000, not bad for an un-employed engineer!

We found a suspect, who was wanted for murder in New York State, had used 37 identities to "cover expenses" while a federal fugitive. He lived well until his capture in the state of Idaho by the F.B.I.

Another "Paper Tripper" victimized a California Bank for \$26,000 in four months with only two cards. We could not prove that a false identity had been used thus the case was simply written off as a collection problem. Three men in their mid twenties operating out of Orange County, California victimized the credit industry out of \$220,000 in documented losses in less than two years via the paper trip method. We have a diary from one of the suspects showing that they travelled throughout Europe, South America, Australia, Canada, and the United States, All on our money. The first suspect, when arrested, pled guilty to grand theft and conspiracy. A strong plea by the District Attorney for a state prison sentence was denied by a Superior Court Judge who flatly stated that he would not even consider such a proposal. The man subsequently was sentenced to nine months in County Jail, served six months and was re-arrested shortly after his release by the F.B.I. At the time of his second arrest, he was in the company of the other two suspects in the original case. This time they were passing stolen American Express Travelers Checks and again, were using false identities.

Another of our fraud application cases involved a suspect with several aliases. Once confronted, this suspect made full and immediate payments on all credit cards obtained falsely. We knew that he was involved in some well paying scheme, however we were unable to obtain any investigative assistance from local law enforcement. This suspect was finally caught in a scam wherein he bilked I.R.S. out of \$565,000. It was interesting to note that he had worked for I.R.S. for sometime by submitting a "fraud application for employment".

These are but a very few examples of the problems we have encountered in just over a year of fraud application investigation. Our statistics show an increase in case load during this first year of 673% over 1974. Initially, our average loss per case was approximately \$2,800. After our first year of operation, we had reduced this average loss to \$405 per identified fraud application. We were able to identify 76% of all fraud application cases investigated prior to a card being issued and this was accomplished with only partial participation by our member banks. One of our major banks simply refuses to cooperate in our efforts and yet their losses as a result of fraud applications for credit cards and loan fraud are among the highest in the state.

We have found that the most measureable results are obtained when we have total participation by the credit industry. As you are aware, we are somewhat hampered in this respect by Federal Legislation prohibiting a free exchange of information between credit grantors.

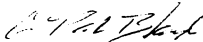
Another problem we face is that, once we identify a major fraud application ring, who handles the necessary follow up investigation? In one instance, 77 cases were presented to Postal Authorities for follow up. The assigned inspector was told to close the investigation due to the highly complicated nature of the cases coupled with a manpower shortage within his unit. This particular suspect was finally sent to federal prison for counterfeiting. At the time of his arrest he was in possession of over 3 million dollars in counterfeit bills, thus giving rise to the speculation that he was part of a large scale criminal cartel.

I feel that the best method to combat the combined problem is the formation of a task force comprised of specialists from industry and law enforcement. These units would be assigned on a regional "as needed" basis. One unit should be responsible for the collection and dissemination of all data concerning either fraud applicants or persons involved in securing false identities. We have found that a large percentage of persons with false identities support themselves via credit fraud. We know that some of the well organized militant groups use this method to support their covert activities and the same holds true of many organized criminal gangs.

We feel that there are literally thousands of fraud applicants in California alone and, in our opinion, the same situation exists in every major metropolitan area in the nation. We must have a joint effort between industry and law enforcement if we hope to curtail these activities to any appreciable degree. We would appreciate any suggestions you may have regarding this immediate and pressing problem.

I read with interest your preliminary proposals for the solution of the false identity problem and look forward to your final report. If we can be of any assistance on this or any other matter, please feel free to call.

Sincerely,



G. Pat Bland
Agent In Charge
Fraud Application Section
Western States Bankcard Association

CC: John Holland
Chief Special Agent

GPB/amb

APPENDIX E3

**FEDERAL STATUTES RELATING TO THE
USE OF FALSE IDENTIFICATION**

FEDERAL STATUTES RELATING TO THE USE OF FALSE IDENTIFICATION

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Agriculture (Warehouses)	7 Sec. 270	Use of forged, altered, counterfeited, simulated license, receipt, or certificate to obtain a loan or convert to his own use goods stored in licensed warehouses for which licensed receipts have been issued.	\$10,000 fine or 10 years or both or fine double the value of converted goods if over \$10,000 and owner of goods may be reimbursed out of fine.
Agriculture	7 Sec. 499	Making false statement for a fraudulent purpose in connection with transaction involving perishable agricultural commodity received in Interstate Commerce.	\$500 fine - 1 year or both. Civil liability to injured party suspend or revoke license of merchant or dealer.
Agriculture	7 Sec. 511	Tobacco inspector issue false certificate.	\$10,000 fine or 1 year or both.
Agriculture	7 Sec. 473c-1	Causing to be issued false certificate of classification of cotton.	\$1,000 fine or 1 year or both.
Agriculture	7 Sec. 85	Grain inspector issuing false or incorrect certificate.	Suspension, revocation, or refusal to renew license.
Agriculture (Commodities)	7 Sec. 9	Made false statement or willful omission of material fact in registration application or report required under this chapter.	Loss of contract market trading privileges, suspension or revocation of registration. Civil fine of up to \$100,000 per violation.
Agriculture (Commodities)	7 Sec. 12a	Gives Commission right to refuse to register any person who willfully makes a material false statement or willfully omission of a material fact in application for commodities license.	Refusal of registration.
Agriculture	7 Sec. 615 (6-3), (3)	Counterfeiting or possession of counterfeit tax payment warrant, stamp, tag, or other means of identification, or makes false statement in application for such warrant, or selling, using or possessing material for illegal manufacture of such items.	\$5,000 fine, 5 years or both.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Aliens	18 Sec. 1423	Misuse of any fraudulently obtained evidence of citizenship or naturalization.	\$5,000 fine, 5 years, or both.
Aliens	8 Sec. 1300	Filing application for registration containing knowing false statements or procuring registration through fraud.	\$1,000, 6 months, or both
Aliens	8 Sec. 1182	Counterfeiting alien registration, alien registration receipt card, or likeness.	\$5,000, 5 years, or both.
Aliens	8 Sec. 1251	Procuring visa or other documentation by fraud.	Loss of eligibility for visa and deportment.
Aliens	18 Sec. 1428	Entering into a marriage contract with intent to evade immigration laws.	Loss of eligibility for visa and deportment.
Aliens	8 Sec. 1353	Failure to surrender cancelled certificate of naturalization upon 60 day notice by the court for	\$5,000 fine, 5 years, or both.
Aliens	18 Sec. 2424	Knowingly making false statements under oath or give false evidence before immigration officer or employee.	Guilty of perjury under 18 USC Sec. 1621.
Aliens	8 Sec. 1185	File false statement with INS about an alien female brought into U.S. for the purpose of prostitution.	\$2,000 fine, 2 years, or both.
Armed Forces	10 Sec. 932 Art. 132	Knowingly making a false statement in application to enter or deport from U.S. during war or national emergency.	\$5,000 fine, 5 years, or both.
		Any person subject to this chapter who knowingly makes a false claim or who for the purpose of gaining approval, allowance, or payment of such false claim makes or uses a false oath, statement paper, or writing or forges or counterfeits any signature on any paper.	Court Martial.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Agriculture (Farm Labor Contractors)	7 Sec. 2044	Knowingly has made false statements in an application for a certificate of registration.	Refuse to issue or renew certificate of registration, revoke or suspend same.
Agriculture (Wheat)	7 Sec. 1379	Counterfeits or fraudulently possesses or uses a counterfeit marketing certificate.	\$10,000 fine, 10 years, or both.
Aliens	18 Sec. 1425	Knowingly issues, procures, obtains or applies for any certificate or evidence of naturalization or citizenship for himself or another.	\$5,000 fine, 5 years, or both.
Aliens	18 Sec. 1426	Counterfeiting, issuing, possessing, or selling any certificate or evidence of naturalization or citizenship or the materials or equipment to produce such certificates or evidence.	\$5,000 fine, 5 years, or both.
Aliens	18 Sec. 1427	Unlawful sale of citizenship papers.	\$5,000 fine, 5 years, or both.
Aliens	18 Sec. 1015	Knowing use of certificate of arrival, declaration of intention, certificate of naturalization, certificate of citizenship and other documentary evidence of naturalization or of citizenship obtained by fraud. False statements under oath in any case, proceeding or matter related to naturalization or citizenship.	\$5,000 fine, 5 years, or both.
Aliens	8 Sec. 1325	Illegal entry into U.S. by alien by evading immigration inspection or by willfully making a false statement or misleading representation or concealment of a material fact.	First offense--\$500 fine, 6 months or both; 2nd or subsequent offense--\$1,000 fine, 2 years, or both.
Aliens	18 Sec. 1424	Impersonation or use of a fictitious name in any naturalization or citizenship proceeding.	\$5,000 fine, 5 years, or both.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Armed Forces	10 Sec. 907 Art. 107	Any person who signs, with intent to deceive, any false record, return, regulation, order, or other official document knowing it to be false or knowingly makes false official statement.	Court Martial
Armed Forces	10 Sec. 6292	Minors enlisted upon false statement of age.	Discharge with pay and allowances with appropriate form of discharge--accountable to his service record.
Armed Forces (Coast Guard)	14 Sec. 473	Minors enlisted under false statement of age.	Discharged with pay and allowances and discharge certificate appropriate to service record.
Bankruptcy	18 Sec. 152	Knowingly and fraudulently conceals, destroys, mutilates, falsifies or makes a false entry in any document affecting or relating to the property or affairs of a bankrupt.	\$5,000 fine, 5 years, or both.
Commerce (Credit Cards)	15 Sec. 1644	Fraudulent use of a credit card in a transaction \$5,000 or more, affecting interstate or foreign commerce.	\$10,000 fine, 5 years, or both.
Commerce (Tariff Commission)	19 Sec. 1919	Knowingly making a false statement to influence the Secy. of Commerce or to obtain money, property or anything of value under this part.	\$5,000 fine, 2 years, or both.
Commerce (Securities Exchange)	15 Sec. 77ff.	Willfully making false statements in any report, application or other document required to be filed under this Chapter.	\$10,000 fine, 2 years, or both--except if violator is an exchange--\$500,000 fine.
Commerce (Investment Co.'s)	15 Sec. 80a.- 48	Willfully making false or misleading statements in any application, report, account, record or other documents required under this chapter.	\$10,000 fine, 2 years, or both.
Commerce (Small Business)	15 Sec. 687a.	Knowingly making false statements in any written statement required under this subchapter for the purpose of obtaining the license.	Suspension or revocation of the license.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Commerce (Utility Holding Companies)	15 Sec. 792-3	Knowingly making false statements or entries in any application, report, document, account, or record filed under this chapter 's rules or regs. or alters or falsifies the same.	\$10,000 fine, 2 years, or both-- except if violation be by a holding company--\$200,000 fine.
Copyrights	2 Sec. 142 b. & d.	Officers and employees of Library of Congress accountable to Government for incorrect payments resulting from false, inaccurate, or misleading certificate made by him.	Civil liability.
Counterfeiting and Forgery	18 Sec. 506	Falsely makes, forges, counterfeits, mutilates or alters the seal of any U.S. department or agency or uses, affixes, or impresses such seal on any certificate, instrument, commission, document, or paper of any description or possesses such seal with fraudulent intent.	\$5,000 fine, 5 years, or both.
Counterfeiting and Forgery	18 Sec. 642	Embezzles or steals any tools or materials to counterfeit any document, or paper issued by the U.S. (equipment, paper, and blank forms included).	\$5,000 fine, 10 years, or both.
Counterfeiting and Forgery	18 Sec. 493	Knowingly passing, uttering, or publishing any note, bond, debenture, coupon, obligation, instrument or document falsely made forged, counterfeited or altered.	\$10,000 fine, 5 years, or both.
Counterfeiting and Forgery	18 Sec. 499	Counterfeiting, forging, or altering military pass or permit or fraudulent use or possession or false personation or loaning pass for unauthorized use.	\$2,000 fine, 5 years, or both.
Counterfeiting and Forgery	18 Sec. 498	Forging, counterfeiting, altering or uses, possesses, or exhibits and military or naval discharge certificates knowing the same to be false.	\$1,000 fine, 1 year, or both.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Counterfeiting and Forgery	18 Sec. 505	Forging signature or seal of any judge, registrar or other officer of any court of U.S. for the purpose of authenticating any proceeding or document or tendering such into evidence.	\$5,000 fine, 5 years, or both.
Counterfeiting or Forgery	18 Sec. 500	Passing, uttering or publishing forged or altered money order knowing material signature or endorsement to be false or any material alteration to have been made.	\$5,000 fine, 5 years, or both
Counterfeiting and Forgery	18 Sec. 495	Falsely makes, alters, forges or counterfeits any deed, power of attorney, order, certificate, receipt, contract, or other writing, for the purpose of obtaining or receiving for himself or another person from U.S. any money or with intent to defraud the U.S.	\$1,000 fine, 10 years, or both.
Counterfeiting or Forgery	18 Sec. 494	Falsely makes, alters, or counterfeits any bond, bid, proposal, contract, guarantee, security, official bond, public record, affidavit, or other writing for the purpose of defrauding the U.S. or transmits or presents such writing to any officer of the U.S. knowing it to be false.	\$1,000 fine, 10 years, or both.
Counterfeiting or Forgery	18 Sec. 507	Counterfeiting ship's papers, certificate of ownership, pass or clearance granted vessel under U.S. authority or the knowingly uttering, publishing or use of such fraudulent papers.	\$1,000 fine, 3 years, or both.
Counterfeiting and Forgery	18 Sec. 1158	Counterfeiting Indian Arts and Craft Board trade mark.	\$500 fine, 6 months, or both--enjoinder.
Customs	18 Sec. 545	Smuggling goods into U.S. by means of false invoice or other document or paper, or knowing possession or handling of such goods.	\$10,000 fine, 10 years, or both.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Customs	18 Sec. 542	Importing or introducing goods into the U.S. by means of false invoice, declaration, affidavit, letter, paper, or by means of any fraudulent statement, written or verbal without reason to believe such statement or willful omission of any material fact in such statement or document.	\$5,000 fine, 2 years, or both.
Customs	19 Sec. 1592 C.R. 18 Sec. 542	Introducing goods into U.S. by means of false statement or any false invoice, declaration, affidavit, letter, paper or any fraudulent practice or application.	Forfeiture of related goods.
Customs	19 Sec. 2316	Knowingly makes a false statement of material facts to obtain or increase any payment for adversely affected workers who require retraining or replacement under section 19 Sec. 2311.	\$1,000 fine, 1 year, or both.
Draft Classification Cards	50 APP Sec. 462	Knowingly transfers; delivers; possesses; forges; alters; destroys; mutilates; changes; photographs; prints or copies a likeness of any certificate issued pursuant to this title for the purpose of aiding the making any false identification or representative (covers registration certificate, alien's certificate of non-residence, etc.)	\$10,000 fine, 5 years, or both.
False Personation	18 Sec. 914	Impersonates person entitled to any annuity, dividend, pension, wages, or other debit due from U.S. and transfers or receives the money of such person.	\$5,000 fine, 5 years, or both.
False Personation	18 Sec. 912	Impersonating officer or employee of the U.S.	\$1,000 fine, 3 years, or both.
False Personation	18 Sec. 913	Impersonating officer, agent, or employee of the U.S. and detains, arrests or makes illegal search.	\$1,000 fine, 3 years, or both.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
False Personation	18 Sec. 911	Impersonating U.S. citizen.	\$1,000 fine, 3 years, or both.
False Personation	18 Sec. 917	Impersonating Red Cross members or agents for the purpose of soliciting, collecting, or receiving money or material.	\$500 fine, 1 year, or both.
False Personation	18 Sec. 915	Impersonating with intent to defraud the U.S., a diplomatic, consular or other official of a foreign government duly accredited as such to the U.S. and obtains money, paper, document or other thing of value.	\$5,000 fine, 10 years, or both.
False Personation	18 Sec. 916	Impersonating 4-H Club members or agents with intent to defraud.	\$300 fine, 6 months, or both.
Federal Grants	42 Sec. 3792	Knowingly and willfully falsifies or conceals a material fact in application for or records required under an IEAA Grant.	Subject to prosecution under 18 Sec. 1001 USC.
Federal Grants (Economic Opportunity Act)	42 Sec. 2703	Employee of program under this chapter obtains money from a grant or contract of assistance by fraud.	\$1,000 fine, 1 year, or both.
Foreign Relations (Foreign Agents)	22 Sec. 612 22 Sec. 618	Willful false statement or omission of a material fact in registering as an agent of a foreign power.	\$10,000 fine, 5 years, or both.
Foreign Relations (Notarizations)	22 Sec. 1203	Forging or counterfeiting the seal or signature of the Secretary of embassy or legation, or consular officer.	\$3,000 fine and 1-3 years (misdemeanor).
Fraud	18 Sec. 1001	Whoever, in any matter within the jurisdiction of any department or agency of the U.S., knowingly and willfully falsifies, conceals or covers up by any trick or scheme, or device a material fact, or makes any false, fictitious or fraudulent statement or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry.	\$10,000 fine, 5 years, or both.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Fraud	18 Sec. 1002	Knowing possession with intent to defraud the U.S. possesses any false, altered, forged or counterfeit writing or document enabling another to obtain any sum of money from U.S.	\$10,000 fine, 5 years, or both.
Fraud	18 Sec. 1017	Fraudulent use of seal of U.S. department or agency or use, sale, procurement, purchase, or transfer of any document, paper or writing upon which such seal has been fraudulently affixed.	\$5,000 fine, 5 years, or both.
Fraud	18 Sec. 1018	Knowing issue by public officer of fraudulent certificate or other writing or certificate, etc. with false statement.	\$500 fine, 1 year, or both.
Fraud	18 Sec. 1003	Knowingly and fraudulently demands or obtains or transfers, sells, assigns, conveys, any annuity, dividend, pension, wages, gratuity, or other debt of U.S. by virtue of a false, forged or counterfeit power of attorney, authority or instrument.	\$10,000 fine, 5 years, or both. Less than \$100--\$1,000 fine, 1 year, or both.
Fraud (HUD & FHA)	18 Sec. 1010	Making false statement or use of false or counterfeit documents to obtain a loan or an advance of credit from any person, partnership, association or corporation with intent that loan or advance should be offered to HUD or FHA for insurance.	\$5,000 fine, 2 years or both.
Fraud	18 Sec. 1016	Authorized officer making false acknowledgement of oath on behalf of U.S.	\$2,000 fine, 2 years, or both.
Government Claims and Benefits	18 Sec. 286	Conspiracy to defraud the government by claiming or obtaining payment or allowance of any false or fictitious claim.	\$10,000 fine, 10 years, or both.
Government Claims and Benefits	18 Sec. 287	Knowingly making false claim to government.	\$10,000 fine, 5 years, or both.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Government Claims and Benefits	31 Sec. 231	Knowingly makes a false claim or presents a false cause for payment or for the purpose of obtaining or aiding to obtain payment of such claim knowingly makes or uses any false bill receipt, voucher, roll, account, claim, certificate, affidavit, or deposition, etc.	\$2,000 fine and double damages of U.S.
Government Claims and Benefits (Food Stamps)	7 Sec. 2023	Knowingly, use, transfer, purchase, alteration, possession, or presentation for payment of unauthorized coupon or authorization to purchase card.	Less than \$100, \$500 fine, 1 year or both. \$100 or more--\$10,000 fine, 5 years, or both.
Government Claims and Benefits (Med. Asst. Programs)	42 Sec. 1396(h)	Knowingly and willfully making a false statement or representation of a material fact in any application or determination of rights under any State plan approved under this subchapter or fails to notify the proper authorities in the event of a change in eligibility.	\$10,000 fine, 1 year, or both.
Government Claims and Benefits (Supplemental Security Income)	42 Sec. 1382a	Knowingly and willfully making false statement or representation of a material fact in any application or determination of rights or continuation of eligibility for any benefit under this subchapter.	\$1,000 fine, 1 year, or both.
Government Claims and Benefits (Old Age, Survivors and Disability Ins)	42 Sec. 408	Knowingly making false statement or representation of a material fact in any application for any benefit, payment or disability determination made under this subchapter.	\$1,000 fine, 1 year, or both.
Government Claims and Benefits (Health Insurance)	42 Sec. 1395 (y & nn)	Knowingly and willfully makes or causes to be made any false statement or representation of a material fact in any application or determination of rights or continues to receive benefits knowing that some occurrence has changed his eligibility.	\$10,000 fine, 1 year, or both.
Government Claims and Benefits (Unemployment Comp.)	18 Sec. 1919 also Sec. 1920	Knowingly makes a false statement or material representation of fact to obtain or increase unemployment benefits.	\$1,000 fine, 1 year, or both.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Government Claims and Benefits (VA Benefits)	18 Sec. 289	False claim or fraudulent misrepresentation of fact in VA Pension Claim.	\$10,000 fine, 5 years, or both.
Government Claims and Benefits (VA Benefits)	38 Sec. 3503	Knowingly makes or presents false or fraudulent affidavit, declaration of certificate, statement, voucher or paper concerning any claim for benefits under VA.	Forfeit all rights, claims, and benefits.
Government Claims and Benefits (VA Benefits)	38 Sec. 787	Knowingly make or present false or fraudulent affidavit, declaration, certificate, statement, voucher, or paper, or writing purporting to be such concerning any application for insurance.	\$1,000 fine, 1 year, or both. Sworn statement--\$5,000 fine, 2 years, or both.
Government Claims and Benefits (RR Unemployment Ins.)	45 Sec. 354 45 Sec. 359	Knowingly making false statement to cause benefits to be paid.	\$10,000 fine, 1 year, or both. Loss of benefits during that registration period.
Government Claims and Benefits (RR Retirement)	45 Sec. 228m	Any officer or agent of employer knowingly making or aiding in making a false statement or report under this subchapter for the purpose of causing a payment.	\$10,000 fine, 1 year, or both.
Government Claims and Benefits (Worker's Comp. Longshoreman's and Harbor)	33 Sec. 931	Willfully make a false or misleading statement for the purpose of obtaining any benefit or payment under this chapter.	\$1,000 fine, 1 year, or both.
Government Employee Benefits (Unemployment Compensation)	5 Sec. 8507	Provides for repayment of compensation resulting from false statements or (knowing) failure to disclose as material fact.	Repayment required or deduct from future payments.
Government Employee Benefits	5 Sec. 8315	Right of government to refuse retirement or annuity pay to employee who made a material false statement in his employment application.	Lose benefits.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Government Claims and Benefits (Employees outside U.S.)	42 Sec. 1713	Knowingly make a false statement or representation of a material fact in any application for any payment of benefits under this subchapter.	\$1,000 fine, 1 year, or both.
Government Claims and Benefits (VA Benefits)	38 Sec. 1780	False statements to defraud VA with complicity between educational institution and veteran or person.	Refer to A.G. for appropriate action.
Government Claims and Benefits (Post Office)	18 Sec. 288	Knowing false claim for loss of any registered, or other article or matter or the contents thereof.	\$500 fine, 1 year or both--if claim is under \$100 only a fine shall be imposed.
Health & Safety (Coal Mines)	30 Sec. 819	Knowingly makes a false statement, representation or certification in any application, report, record plan, or other document filed under this chapter.	\$10,000 fine, 6 months, or both.
Health and Safety (OSHA)	29 Sec. 6666	Knowingly makes a false statement, representation or certification in any application, report, record, plan or other document filed under this chapter.	\$10,000 fine, 6 months, or both.
Health and Safety	42 Sec. 1857-c-8	Knowingly makes a false statement representation, or certification in any application, record, report, plan or other document or who falsifies, tampers with, or knowingly renders inaccurate any monitoring device...	Fine not more than \$10,000 or jail--6 months or both.
ID Cards	18 Sec. 701	Manufacture, sale, or possession of any badge, identification card or other insignia used by any department of the U.S. or any colorable imitation photograph, print, or any other means of making a likeness thereof.	\$250 fine, 6 months, or both.
Identification Documents (Merchant Seamen Certificate of Identification)	46 Sec. 643	Regulates issue of and provides penalties for making false statements in application for Merchant Seaman's continuous discharge book and certificate of identification.	\$1,000 fine, or 1 year (for false statement)

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Identification Documents Seamen	18 Sec. 2197	Manufacture, forgery, alteration, sale, transfer, knowing use or exhibition, or possession without lawful excuse of a federal certificate, license or document issued to vessels, officers, or seamen by any officer or employee of the U.S.	\$5,000 fine, 5 years, or both.
Internal Security (Organization Registration)	18 Sec. 2385	Knowingly making false statements or material omissions of fact in required registration under this chapter.	\$20,000 fine, 20 years, or both. 5 years ineligible as government employee.
Passport and Visas	18 Sec. 1543	False making, forgery, counterfeiting, mutilation, alteration, use, or furnishing for another's use of any passport.	\$2,000 fine, 5 years, or both.
Passports and Visas	18 Sec. 1546	Counterfeiting, altering, use or possession of fraudulent visas, permits, and other entry documents or the equipment or materials to manufacture them.	\$2,000 fine, 5 years, or both.
Passports and Visas	18 Sec. 1542	Willfull making of a false statement in an application for a passport.	\$2,000 fine, 5 years, or both.
Passport and Visas	18 Sec. 1544	Wrongful use of a passport of another or in violation of the conditions or restrictions therein contained.	\$2,000 fine, 5 years, or both.
Passports and Visas	18 Sec. 1541	Knowing issuance by official to person not owing allegiance to U.S. or by person impersonating official.	\$500 fine, 1 year, or both.
Perjury	18 Sec. 1621	Knowingly making false statement under oath.	\$2,000 fine, 5 years, or both.
Records and Reports	18 Sec. 641]	Embezzles, steals, purloins, or knowingly converts, sells, conveys, or disposes any record, voucher, money, or thing of value of U.S. or receives, retains or conceals the same knowing it to have been embezzled, stolen, etc.	\$10,000 fine, 10 years, or both. Less than \$100--\$1,000 fine, 1 year, or both.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Records and Reports	18 Sec. 2071	Willfull concealment, removal, mutilation, obliteration or destruction (or falsification by custodian of record) of any record, paper, document, filed with U.S. court or public office.	\$2,000 fine, 3 years, or both (loss of eligibility for public office if custodian)
Regulated Substances (Explosives)	18 Sec. 842	Knowingly make false statement or material omission or to furnish or exhibit any false, fictitious, or misrepresented identification, intended or likely to deceive for the purposes of obtaining explosive materials or a license, permit, exemption or relief from disability under this chapter.	\$10,000 fine, 10 years, or both.
Regulated Substances (Firearms)	18 Sec. 922 & 18 Sec. 924	Make any false statement oral or written or to furnish or exhibit any false fictitious or misrepresented identification to acquire any firearm or ammunition from a licensed manufacturer, licensed dealer, or licensed collector.	\$5,000 fine, 5 years, or both for false statement; \$10,000 fine, 10 years, or both for intent to use to commit crime; 1-10 years for use in commission of a felony; 2-25 years for subsequent use in commission of a felony; no sentence may run concurrently with the felony sentence nor can the sentence be suspended or probationary in the case of a second or subsequent offense.
Regulated Substances (Firearms)	18 Sec. 923	Willful false statements or failure to disclose a material fact in connection with license issued under this section.	\$5,000 fine, 5 years, or both.
Regulated Substances (Firearms)	26 Sec. 5661	Making a false entry on any application required in this chapter (firearms).	\$10,000 fine, 10 years, or both.
Regulated Substances (Food & Drugs)		Forging or altering, etc., any official device mark or certificate which indicates official U.S. meat inspection.	\$1,000 fine, 1 year, or both-- distribution, adulterated food or intent to defraud--\$10,000 fine, 3 years, or both.

<u>SUBJECT AREA</u>	<u>CITATION</u>	<u>OFFENSE</u>	<u>PENALTY</u>
Regulated Substances (Food & Drugs)	21 Sec. 458	Forging any official device, mark, or certificate which indicates official U.S. poultry inspection or alter official devices, mark or certificates.	\$1,000 fine, 1 year, or both-- if intent to defraud \$10,000 fine, 3 years, or both.
Regulated Substances (Food & Drug)	21 Sec. 1037	Forging or altering etc. any official device, mark, or certificate which indicates official U.S. egg products inspection.	\$1,000 fine, 1 year, or both, distributing of adulterated food or intent to defraud--\$10,000 fine, 3 years or both.
Tax	26 Sec. 7206	Knowingly making material false statements on income on any return, statement or other document which is verified by a written declaration made under the penalty of perjury.	\$5,000 fine, 3 years, or both-- statute of limitations 6 years (26 Sec. 6531)
Tax	26 Sec. 7207	Willfully, and knowingly making a false statement or presents fraudulent or false documents to the Secy. or his delegate.	\$1,000 fine, 1 year, or both-- Statute of limitations 6 years (25 Sec. 6531)
Transportation (Pilot's Licenses)	49 Sec. 1472	Knowingly and willfully forges, counterfeits, or alters any certificate authorized to be issued under this chapter.	\$1,000 fine, 3 years, or both.
Transportation (Ship's Papers)	19 Sec. 1581	Any master of a vessel knowingly presenting forged, altered or false document or paper to the examining officer.	\$500-\$5,000 fine.
Transportation (Shipping)	46 Sec. 62	Knowingly makes, utters or publishes any false Mediterranean Passport or certificate of registry or knowingly avails himself of such documents.	\$5,000 fine
Voter Registration	42 Sec. 1973(1)	Knowingly and willfully giving false information as to name, address, or period of residence for the purpose of residence for the purpose of establishing his eligibility to register or vote, falsifying, making or using fraudulent documents within jurisdiction of the examiner.	\$10,000 fine, 5 years, or both.

APPENDIX F
ALTERNATE VIEWS

A statement of the findings and recommendations of the FACFI, in substance and form similar to that of the Executive Summary of this report, was published in the Federal Register on June 16, 1976. The item included a request for public comment. Of the comments received, the overwhelming majority expressed strong agreement with the conclusions of the FACFI. In this appendix, we present three responses that were received which express strong disagreement with specific findings or recommendations.

Appendix F1 contains a statement by Deane L. Huxtable in support of Federal control over vital records and of adopting a national identification document, concepts that the FACFI considered and rejected. Mr. Huxtable is a member of the FACFI and State Registrar of Vital Statistics in the Commonwealth of Virginia.

Appendix F2 contains the text of a letter by Dr. Paul Lehmann, Chairman of the American Committee for Protection of Foreign Born. Dr. Lehmann's remarks address the FACFI's conclusions in the area of illegal immigration. Appendix F3, which also addresses this area, includes excerpts from a letter by H. Gerald Malmud, President, Association of Immigration and Nationality Lawyers.

Finally, Appendix F-4 presents an anonymous letter received by the Committee concerning lax driver's license issuing procedures. Although it is impossible to verify its authenticity the thoughts expressed in it bear notice. To protect the writer's identity the name of the State mentioned therein has been deleted.

APPENDIX F1

**STATEMENT TO THE FACFI IN THE
MATTER OF A MINORITY RECOMMENDATION**

**STATEMENT TO THE FEDERAL ADVISORY COMMITTEE ON FALSE IDENTIFICATION IN THE
MATTER OF A MINORITY RECOMMENDATION**

The only way that a person can prove who he is, that he is a citizen, that he has rights to certain benefits—or conversely, the only way that it can be proven that a person is not what he claims—is through the record keeping system of this country. No matter what action is taken by this committee, no matter what suggestions are made, any positive results will only depend on strengthening and re-organizing our deficient, decentralized, and demoralized record keeping system regarding personal data.

Personal data start with the birth certificate. Citizenship is within the mandate of the Federal government—this is right. Hundreds of towns, counties, cities, and states issue documents as evidence of citizenship—this is wrong. Standardized documents controlled and issued from central sources, proving personal facts and identity, would be the primary resolution of the problem facing this committee. This is the best way that law-abiding citizens can have protection for their names, their identity, and their personal and private rights.

No matter how many minor actions are proposed, no matter how many punitive or non-punitive suggestions are made, the real matter boils down to two major conclusions:

1. On a decentralized basis (to the states), the Federal government should assume responsibility and operational control over the vital statistics registration system in this country; and
2. At the age of 18, or some arbitrary age to be established, the system should issue unique, numerically designated identity cards to the American public. (Note: The card is not to be considered as final proof of identity. It is, however, the numerical key to querying the system at any time by any agency requiring verification.)

To establish a system for identifying our citizens in a democratic society may cost us a minor degree of personal freedom. Not to do so may cost us all of it.

Deane L. Huxtable
July 20, 1976

APPENDIX F2

**LETTER FROM THE CHAIRMAN OF THE
AMERICAN COMMITTEE FOR PROTECTION
OF FOREIGN BORN**

TEXT OF LETTER BY DR. PAUL LEHMANN, CHAIRMAN, AMERICAN COMMITTEE FOR PROTECTION OF FOREIGN BORN, 799 Broadway, Suite 233, New York, N.Y. 10003

We wish to comment on FACFI's proposed Findings and Recommendations, as printed in the Federal Register of June 16, 1976. We agree with the stated purpose of FACFI. Appropriate measures against false identification are needed to protect the public and to help insure the proper carrying out of government functions.

We wish to address our remarks to Sec. IV, subhead 2 (Illegal Immigration), a subject within the expertise of our organization, which has been functioning in the immigration field for 44 years. As regards illegal immigration, on its face this refers to those who enter the United States by (1) evading inspection ("border jumpers") or (2) using false documents. Immigration and Naturalization Service statistics indicate that the vast number—over 90 percent—of illegal entrants (across the Mexican border) do so by evading inspection. Elsewhere in the United States, the problem centers on non-residents who enter legally (visitors, students, seamen, etc.) and then overstay their authorized time.

Your brief reference to the immigration aspect of the overall problem of false identification makes no distinction between the types of entrants, and thus concludes—without any substantiation whatsoever—that "the use of false IDs by illegal aliens...is substantial and increasing."

FACFI states that "independent consultants" to the Immigration and Naturalization Service estimate the tax burden caused by the presence of illegal aliens to be in excess of \$12 billion a year. However, the Lesko report (10/15/75) for the INS points out that "actual data regarding the number of illegal do not exist within the INS" or any government agency. Furthermore, the Linton Report (11/17/75) for the U.S. Labor Department indicates that 77% pay social security taxes, 73% pay Federal withholding taxes, but only 4% had received unemployment compensation, 4% had children in schools, 1% had received food stamps, and only .5% had received welfare. "Illegals" are augmenting social funds rather than benefiting from them.

In view of these data, the FACFI references to illegal aliens burdening public services are inaccurate and, at the very least, tendentious. In addition, the problem of nonresidents not in status results, to a considerable degree, from the discriminatory quota and admission requirements for Western Hemisphere entrants, as well as from basic economic problems endemic to both sides of the U.S.-Mexico border. These problems have been the subject of extensive Congressional hearings, and remedial legislation is pending.

False identification is at most a peripheral facet of the problem of aliens not in status. We accordingly urge that your Findings and Recommendations place the problem of false identification in the sphere of immigration in proper perspective.

DR. PAUL LEHMANN
Chairman
July 12, 1976

APPENDIX F3

**LETTER FROM THE PRESIDENT OF THE
ASSOCIATION OF IMMIGRATION AND
NATURALIZATION LAWYERS**

**EXCERPTS FROM LETTER DATED JULY 2, 1976 BY H. GERALD MALMUD, PRESIDENT,
ASSOCIATION OF IMMIGRATION AND NATIONALITY LAWYERS, 30 Central Park South,
New York, N.Y. 10019**

"...I thought you might be interested in two recent items offering a different point of view regarding the employment of aliens not in official work status. The first is . . . an editorial from the *Wall Street Journal* of (June 18th, 1976, p. 8). It states that the Federal government . . . 'is obviously getting more than it gives,' and that ' . . . the same is probably true for the local economies in which these immigrants work.' The *Wall Street Journal* also suggests that the problem be attacked by an increase in the Western Hemisphere quota and legalizing the immigrants, resulting in . . . 'putting the law to work protecting them rather than persecuting them.'"

The other item is a copy of an article from the May 1976 issue of *Commentary* magazine. You will observe that (at page 34) in a discussion of the impact of (illegal immigration) upon New York City's economic situation, it is concluded as to those aliens that ' . . . far from being a burden to the City, they may well be playing a crucial role in keeping alive large segments of the City's economy.' "

H. Gerald Malmud
President

APPENDIX F4

ANONYMOUS LETTER FROM

AN EMPLOYEE OF A

STATE DRIVER'S LICENSE

AGENCY

July 25, 1976

Mr. David Muchow, Chairman,
Federal Advisory Committee on False Identification,
Department of Justice,
Washington, D.C.

Dear Mr. Muchow:

I was very interested in your work on false identification. Here at the (deleted) Department of Motor Vehicles we issue drivers licenses and I.D. cards all day. You have no idea what goes on.

Birth certificates are accepted without anything to connect them with the bearer. If he says it is his, that is final. Uncertified photostats are accepted as conclusive, and you know what can be done with any document in a photostat machine. In the case of a female, only the first name need match, as she says she is married.

We see the same faces getting licenses and I.D. cards in different names all the time; for the purposes of welfare fraud, and illegal alien fraud.

Why do we do nothing? Because all employees are terrified of courtesy complaints. The attitude of supervision is, "Don't rock the boat; your job is to issue." Employees who expose fraud in identity face real, and I mean real trouble. Avoiding courtesy complaints is the foremost aim of the Department, and always was.

We are keeping our fingers crossed for you and your group. We have no interest but seeing this farce corrected.

If it were known who wrote this to you, the Department would try to bring dismissal charges against me, civil service notwithstanding; and therefore I cannot sign this letter. Please believe we are almost all fed up with what is happening.

Sincerely and best wishes,

(Signed with an X)

