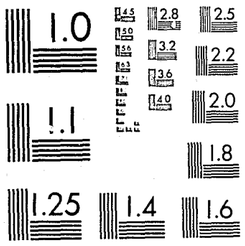

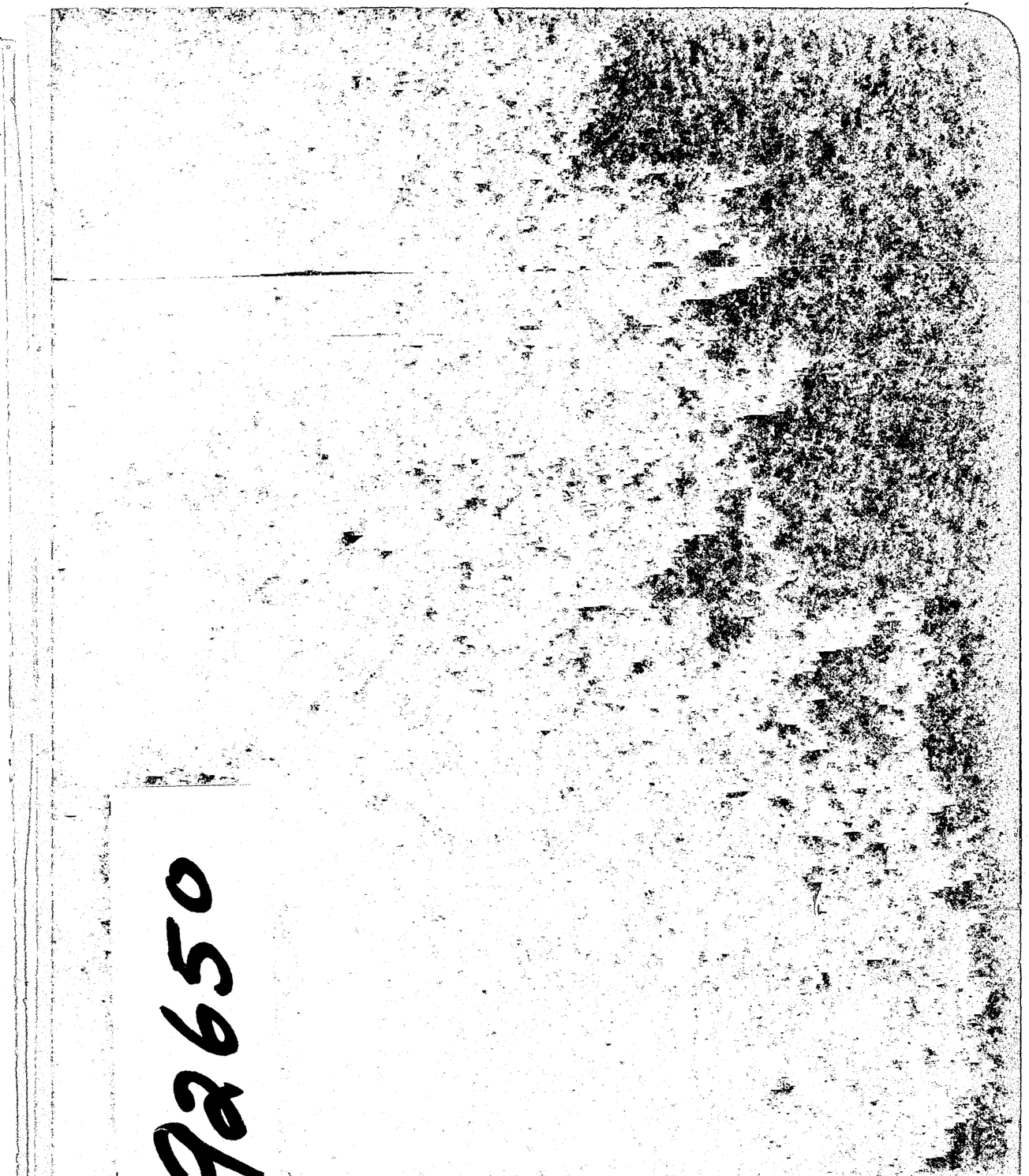

U.S. Department of Justice
Bureau of Justice Statistics

MF-1

Bureau of Justice Statistics
Special Report

Electronic Fund Transfer and Crime

February 1984

Recent developments in automation have revolutionized operations within the business community. Accompanying these changes, concern has arisen about the potential for criminal abuse of the automated systems that support major financial, commercial, and governmental functions.

Such concern focuses largely on the abuse of recently developed payment systems that control the flow of vast sums of money on a national and international basis.

At the Federal level, these issues have been addressed by several Executive Branch agencies and the Congress. State legislation has also been enacted in the area of computer crime control.

Over the past several years, the Bureau of Justice Statistics has supported studies to identify key issues in computer crime and to develop preliminary techniques to analyze the nature and extent of such crime. This Special Report represents the first BJS publication dealing with this issue.

The report is intended to highlight the impact of automation on financial transactions, to identify potential areas of abuse, and to discuss issues relevant to collection of data measuring EFTS crime. Additional Special Reports will be issued as more specific data become available; these will address both computer crime and the response of the criminal justice system to it.

Steven R. Schlesinger
Director

During the past decade, the Nation's banking or payment system has become increasingly dependent on rapidly evolving computer-based technologies. Collectively known as electronic fund transfer (EFT) systems, these technologies can be grouped into three categories, according to whether they benefit primarily the retail (i.e., individual consumer or small business), corporate (i.e., large public or private organizations), or internal banking sectors of the economy (figure 1).

The most common and fastest growing retail EFT technology is the now familiar automated teller machine (ATM). Other retail technologies include the point-of-sale (POS) terminal, the telephone bill-paying (TBP) service, and the newly introduced home banking service. The primary corporate EFT technologies are the wire transfer services, automated clearing houses (ACHs), and cash management services. Finally, internal bank EFT technologies include the online teller terminal and the computerized check processing system. In sum, EFT technologies encompass those payment systems in which the exchange of value, or information necessary to effect an exchange, is represented or facilitated by electronic messages.

Opportunities for crime in EFT systems

Although EFT technologies have been a boon to banks and consumers, they also provide an electronic environment that is potentially fertile for criminal abuse. In the ATM area, for example, abuse or fraud may take one of four major generic forms:

from a mailbox or wallet; obtained as the unanticipated byproduct of a burglary, street robbery, or larceny; or used without permission by a family member or friend.

The individual obtaining the card needs the personal identification number (PIN) to activate the ATM, but, not surprisingly, this number is often written down by the owner and kept with the card. A daily withdrawal limit (between $200 and $300 per account) prevents excessive losses in any given day, but often many days of withdrawals can be made before the bank is made aware of the fraud. Single ATM fraud losses have amounted to as much as $10,000.

procedures (such as fingerprints or voiceprints) can provide unscrupulous cardholders with the opportunity to commit fraud from their own individual accounts. A cardholder makes a complaint, disclaims any knowledge of the withdrawal, and persists with the claim in the face of skeptical bank officials. Current Federal law makes it difficult for banks to deny such a claim; in fact, if the "loss" was reported within two business days the cardholder is liable—under Regulation E of the federal law—for only the first $50 of losses.

• Insider manipulation. Vulnerabilities to fraud may exist in nearly every aspect of a highly complex banking operati- n like an

cards mailed and then "returned to sender" because of incorrect or out-of-date addresses. Cash may be stolen directly from ATM replenishment canisters or deposit envelopes by ATM maintenance or service team members. Further, a range of electronic attacks can be made on the host computer system, including software alteration, fraudulent account creation, and removal of security controls on "hot" or blocked accounts.

• Physical attack. Several types of attacks on automated teller machines and their users can occur. The machine, like a bank safe, can contain a large amount of cash and is a target for explosive attempts at entry. One ATM was dynamited, but unfortunately for the attackers, the money was destroyed along with the ATM. In addition, cardholders, especially those who use streetside or drive-in ATMs at night, are susceptible to robbery immediately following cash withdrawal. Many urban area police departments are becoming aware of this after-ATM-usage robbery pattern.

Preliminary analyses of fraud losses in the wire transfer area suggest three major types of frauds:

• "Erroneous" payment by authorized system officials. "Errors" made by terminal operators, clerks, bank account officers, or corporate officials can result in a wire transfer instruction that is
—made out to the correct beneficiary but for the wrong (and excessive) amount;
—made out for the correct amount but paid to the wrong beneficiary;
—paid twice, rather than once, to the correct beneficiary; or
—paid to the wrong account of a correct beneficiary with more than one account.
These and other simple errors can result in the sudden enrichment of an individual or corporation.

• Transactions introduced by unauthorized persons. Although only specified officials of banks and corporations are authorized to initiate a wire transfer instruction, an unauthorized person with knowledge of the procedures may gain access to the system and introduce a fraudulent payment instruction. In such cases, two additional steps must be undertaken: first, the funds must be converted to the thief's own use (e.g., withdrawn as cash, used to purchase goods, etc.); and second, the audit trails and fund balancing mechanisms that may point to the details of the fund transfer must be "erased." Although such frauds could occur whether or not EFT technologies are employed to convey the payment instructions, characteristics of the software and hardware that support wire transfer operations may assist skillful perpetrators in hiding their activities or in delaying the discovery of their misdeeds.

• Transactions altered in processing. As data processing technology rapidly improves the efficiency of wire transfer operations, allowing a much higher volume of activity to be processed per unit of time and manpower, the operating software and hardware are increasingly exposed to manipulation by knowledgeable individuals. Bank officers with high-level password access can override the segmentation of functions that provides security at the terminal-operator level; in-house programmers can conduct any one of a number of attacks on system integrity; and outside criminals can "tap" the system and obtain access code and account information. Wire transfer systems that transmit billions of dollars each working day are tempting targets for fraud; however, reports of such incidents are few, if any, in any specific year.

Fig. 1. Categories of electronic fund transfer systems

Retail:	
Automated teller machine (ATM)	Remote terminal linked to a financial institution's account records. ATM users (i.e., account holders) may carry out several simple financial transactions, including deposits, cash withdrawals, account transfers, balance inquiries, mortgage and loan payments, and other bill payments.
Point-of-sale (POS) terminal	Remote terminal that links a retail store to one or more financial institutions. POS users (i.e., retail stores) may verify check payments, authorize credit purchase, or transfer funds from a customer's account to a merchant's account for payment of purchase.
Telephone bill paying (TBP)	System that allows an account holder to give instructions for financial transactions by keying on a touch-tone telephone (some systems use human operators). TBP users (i.e., account holders) may instruct their bank to pay merchant and utility bills, as well as to make mortgage and other bank payments.
Home banking	Service that permits account holders to access their account records and to initiate financial transactions using their TV and a control box (or through a personal computer). Home banking users (i.e., account holders) may access account information (balance, transaction history, canceled checks, etc.), make payments, or transfer funds between accounts.
Corporate:	
Wire transfer	Service that allows large dollar value transfers between and among financial institutions, the Federal Reserve, and corporate customers. Such transfers are made through a communications network.
Automated clearing house (ACH)	Service that takes magnetic-tape based transaction information from originating financial institutions, sorts it, and then transmits it to receiving institutions. ACH is primarily used for direct deposit of payroll and government checks.
Cash management	Service that allows corporate customers to access their records electronically. In addition to receiving account balances and history, customers may transfer funds between accounts and initiate wire transfers.
Internal:	
On-line teller terminal, computerized check processing system, etc.	Systems that allow financial institutions to process their transactions electronically.

Criminal statutes

Although much EFT abuse has the same fiscal consequence as a traditional theft, the existing criminal law does not, in many cases, directly address the unique elements of EFT crimes. Theft statutes typically stipulate the taking of physical property, but does generating an electronic signal or executing a computer routine that changes an account balance constitute "taking"[1]? Do the contents of a computer memory constitute property? Further, fraud statutes require willful misrepresentation to a person—are computers persons?

At present, as listed in figure 2, there are 22 States with computer crime or EFT-related statutes. At the Federal level, the laws applicable to EFT crime include specific sections of the Electronic Funds Transfer Act of 1978 and the wire fraud and mail fraud provisions of the Criminal Code.

Because almost all State computer crime statutes were enacted within the past 5 years, little data exist regarding the impact of the legislation. BJS, however, is supporting a project to identify and analyze prosecution experiences under this recently enacted legislation.[1]

Impact of automation

As EFT technologies come to play an even more dominant role in the Nation's payment system, criminal justice professionals will need to recognize opportunities for and incidence of EFT-related criminal activities. A recently completed study sponsored by BJS[2] surveyed and analyzed the current state of knowledge about the nature and extent of EFT crime. Some findings of this study are highlighted herein, together with recent statistics on the automation of financial transactions.

[1]The project is being undertaken by Donn Parker of Stanford Research International and Susan H.

Fig. 2. State computer crime or EFT-related legislation

	Year legislation enacted
Alaska	1983
Arizona	1978
California	1979
Colorado	1978
Delaware	1982
Florida	1978
Georgia	1980-81
Illinois	1979
Kentucky	1977
Massachusetts	1983
Michigan	1979
Minnesota	1981-82
Missouri	1983
Montana	1981
New Mexico	1979
North Carolina	1980-81
Ohio	1981-82
Rhode Island	1979
Tennessee	1983
Utah	1980-81
Virginia	1978
Wisconsin	1982

Crime concerns heightened as EFT systems grow

The potential for crime in EFT systems is underscored by the phenomenal growth in the use of EFT. A combination of forces, including deregulation, the siphoning-off of formerly profitable low-interest savings accounts, aggressive competition by nonbank financial institutions, and rapid advances in computer-based technologies, have established a volatile and competitive environment that is fostering large-scale EFT development. As bank profitability has become more uncertain,[3] banks have turned to EFT technologies as a primary means for reducing the costs of labor-intensive banking operations such as check processing and routine teller services. Nationwide, the overall volume of banking transactions is growing, but the type of transaction appears to be shifting from non-EFT to EFT. Figure 3 shows the type, value, and number of transactions in 1980 and 1982. The data indicate, for example, that the number of ATM transactions in 1980 was approaching that of bank credit cards and that wire transfers constituted the dominant—in terms of dollar volume—form of noncash transactions in the Nation. Assuming the 1980 combined assets of all commercial and thrift institutions to be somewhat less than $2.7 trillion (figure 4), the 1980 dollar volume of wire transfers is more than 40 times the combined asset value.

Figure 5 suggests that the use of ATMS, ACHs, and wire transfers has increased rapidly since the early 1970's. Other EFT technologies are less widespread. Despite the installation of some 10,000 POS terminals in the 1970's, most are limited to check and credit card authorization, although their use as an electronic payment mechanism for purchases has seldom gone beyond the experimental stage. However, wide consumer acceptance of ATMs and plastic cards suggests that POS systems may become more prevalent in the future.

Similarly, home banking promises to take the place of the more cumbersome TBP service as the former service moves beyond the experimental stage. Several banks are, in fact, planning to offer home banking services this year. One EFT authority predicts that home banking will account for the bulk of retail banking transactions by the year 2000. Cash management services are also rapidly becoming an integral part of corporate finance, although statistics on their use are not available.

The growth in EFT use to date will, however, pale in comparison to its expected future growth, especially as banking laws are changed to accommodate the information age and as computer and communications technology becomes more advanced. The Monetary Control Act of 1980 has, among other provisions, required the Federal Reserve Board to allow all depository institutions access to its wire

Fig. 3. Estimated number and value of financial transactions by type

	Number of transactions (billion)		Value of transactions (billion)	
	1980	1982	1980	1982
Nonelectronic				
Cash	*	*	$ 119	*
Checks	34.00	38.00	19,000	$ 21,000
Bank credit cards	1.30	*	49	66
Electronic				
ATMs	0.98	2.07	35	240
ACHs	0.22	0.31	153	*
Wire transfers	0.06	*	117,000	*

*Data not available
Sources:
1. Association of Reserve City Bankers. Report on the Payments System, 1982
2. Federal Reserve Bank of Atlanta. A Quantitative Description of the Check Collection System, 1981.
3. Zimmer, Linda F. "ATMs," Bank Administration, May 1983.
4. Keenan, Lee T. "ACH Product Management," Bank Administration, January 1983.
5. American Bankers Association. Testimony concerning credit card fraud, Subcommittee on Consumer Affairs and Coinage, House Committee on Banking, Finance and Urban Affairs, July 1983.

Fig. 4. Number and asset level of U.S. financial institutions by asset size

	1982				1981	
	Commercial banks		Mutual savings banks		Savings & loan associations	
	Number	Total assets (billions)	Number	Total assets (billions)	Number	Total assets (billions)
Uninsured	113	$ 2.1	71	$ 7.9	568	$ 12.8
Insured:						
Less than $50M	9,989	220.1	20	0.6	1,697	40.5
$50-$100M	2,401	165.0	77	5.6	820	59.0
$100M-$300M	1,436	228.3	111	19.5	740	115.6
$300M+	626	1,255.4	107	129.6	529	435.9
Total insured	14,452	$1,868.8	386	$ 163.2	3,786	$ 651.0

Sources:
1. Federal Deposit Insurance Corporation. 1982 Statistics on Banking, 1983.
2. U.S. League of Savings Associations. 1981 Savings and Loan Sourcebook, 1982.

[2]K. W. Colton, J. M. Tien, S. Tvedt, A. I. Barnett, (Public Systems Evaluation, Inc.) Electronic Fund Transfer Systems and Crime. Washington, D.C.: Bureau of Justice Statistics, 1982.

[3]Fortune magazine, September 1983, in an article by Orin Kramer, indicates

system (i.e. Fedwire); as a result, the number of institutions eligible to use Fedwire has increased from 5,500 Federal Reserve members to 19,200 commercial and thrift institutions. Further, retail EFT use is no longer limited to localized systems—shared ATM networks are proliferating. The first interstate ATM network became operational in January 1983.

With regard to their proliferating ATM operations, bankers are especially sensitive about the recent fraud experiences of the credit card companies. Figure 6 shows how the fraud losses per $1,000 in transactions, as reported by major credit card organizations, have increased by almost 50% in the recent 4-year period; this increase in losses is even more dramatic on a transaction basis. It is generally believed that the increasing fraud losses, which have prompted new Federal legislation and a host of system changes, result largely from counterfeiting techniques used by syndicated criminal enterprises working with corrupt merchants. It is also believed that thus far, ATM losses from fraud are nowhere near that experienced by the credit card companies. Possibly, this is because of the added ATM safeguards (e.g., the use of a PIN in ATM and the lower daily ATM withdrawal limit, as compared with the credit ceiling of a card); or because ATMs are still not widespread and represent a relatively new payment method.

Bankers are also sensitive about the potential for loss in the corporate EFT area, where enormous sums of money are being transferred by wire. Although the average loss from a fraudulent wire transfer could be quite large, evidence to date suggests that the likelihood of such a fraudulent act is small indeed. On the other hand, although the average loss due to a fraudulent ATM transaction is quite small, the likelihood of such an act is not small. Unfortunately, there are at present no valid sources of data that could be analyzed to determine the level of retail, corporate, and internal EFT crime.

Fig. 5. Estimated number and value of electronic transactions by type and year

	Automated teller machines			Automated clearing houses		Wire transfers[a]	
	Installed terminals	Transactions (billions)	Value (billions)	Transactions (billions)	Value (billions)	Transactions (billions)	Value (billions)
1975	4,056	*	$ *	*	$ *	0.023	$ 42,400
1976	5,305	*	*	0.04	*	*	*
1977	7,749	*	*	0.09	*	0.033	59,400
1978	9,750	0.38	*	0.12	*	0.039	70,900
1979	13,800	*	*	0.15	*	0.046	91,000
1980	18,500	0.98	35	0.22	153	0.056	115,700
1981	25,790	*	*	0.30	*	0.070	137,700
1982	35,721	2.07	240	*	*	*	*

[a]Includes only Fedwire and CHIPS wire transfer services.
*Data not available.
Sources: See figure 3, notes 1, 3, and 4.

Fig. 6. Estimated credit card fraud loss by year, 1979-82

	Loss per transaction (dollars)	Loss per $1,000 volume (dollars)
1979	.042	1.126
1980	.053	1.321
1981	.065	1.499
1982	.079	1.673

Source: Major credit card organization data.

No valid sources of data on EFT crime

Given the potential for EFT crime, it is necessary to develop estimates of its incidence and knowledge about its characteristics. A number of factors, however, have contributed to the unavailability of valid data on EFT crime. These include the following:

- The proprietary nature of EFT systems and the corresponding concern over potential competitive disadvantages that might result from the release of operational data.
- The wide variations in definitions, procedures, and categories used by financial institutions to record transactions, fraud events, and charge-offs for sustained losses.
- Technical and practical difficulties in identifying the occurrence of an EFT crime either while in progress or after the event.
- The uncertainty about the legal status of specified actions that may (or may not) constitute crimes in a given jurisdiction.
- The likelihood that EFT violations will be handled through inhouse security or personnel procedures and not reported through the standard criminal justice system.
- The absence of any comprehensive or central source for EFT events reported through the criminal justice system.
- The nonexistence of standardized comparative data against which EFT losses can be measured on a current or trend-line basis.
- The relatively recent development of EFT techniques and ongoing changes that are continually being adapted into the system operations.

The dearth of existing EFT crime data has been recognized by banking industry associations, the Federal Government, and the Congress. A recent report by the Association of Reserve City Bankers (ARCB) stated that "there is a lack of empirical data on the nature and extent of crime in electronic payment systems... (and recommended further)...study of the nature and frequency of fraud in these systems."[4]

In response to the stated need, the Bureau of Justice Statistics (BJS) is supporting a study directed at collecting consistent, incident-level data that could be used to assess the nature and extent of EFT crime. Data will be collected from an ongoing national panel of selected financial institutions.

It is hoped that establishing an ongoing panel will tend to minimize the problems in data collection noted above and will afford an ongoing source of information on EFT crime that can be analyzed over time to provide pertinent trend information.

Further reading

Computer Crime: Electronic Fund Transfer Systems and Crime, 182 pp., NCJ-83736, 9/82.

Bureau of Justice Statistics Special Reports are prepared principally by BJS staff and edited by Jeffrey L. Sedgwick, deputy director for data analysis. Marilyn Marbrook, head of the publications unit, administers their publication, assisted by Lorraine L. Poston and Joyce Stanford. This report was prepared by James M. Tien, George L. Fosque, Michael F. Cahn, and Kent W. Colton of Public Systems Evaluation, Inc., under the direction of Carol G. Kaplan, chief of the Federal statistics and information policy branch of BJS.

NCJ-92650, February 1984

[4]Association of Reserve City Bankers, Risks in the Electronic Payment Systems: Report of the Risk Task Force. Washington, D.C.: December 1983.

Bureau of Justice Statistics reports

(revised February 1984)

Single copies are available free from the National Criminal Justice Reference Service, Box 6000, Rockville, Md. 20850 (use NCJ number to order). Postage and handling are charged for multiple copies (301/251-5500).

Public-use tapes of BJS data sets and other criminal justice data are available from the Criminal Justice Archive and Information Network, P.O. Box 1248, Ann Arbor, Mich. 48106, (313/764-5199).

National Crime Survey

Criminal victimization in the U.S.:
1973-82 trends, NCJ-90541, 9/83
1981 (final report), NCJ-90208
1980 (final report), NCJ-84015, 4/83
1979 (final report), NCJ-76710 12/81

BJS bulletins:
Households touched by crime 1982, NCJ-86671, 6/83
Violent crime by strangers, NCJ-80829, 4/82
Crime and the elderly, NCJ-79614, 1/82
Measuring crime, NCJ-75710, 2/81

The National Crime Survey: Working papers, vol. I: Current and historical perspectives, NCJ-75374, 8/82
Crime against the elderly in 26 cities, NCJ-76706, 1/82
The Hispanic victim, NCJ-69261, 11/81
Issues in the measurement of crime, NCJ-74682, 10/81
Criminal victimization of California residents, 1974-77, NCJ-70944, 6/81
Restitution to victims of personal and household crimes, NCJ-72770, 5/81
Criminal victimization of New York State residents, 1974-77, NCJ-66481, 9/80
The cost of negligence: Losses from preventable household burglaries, NCJ-53527, 12/79
Rape victimization in 26 American cities, NCJ-55878, 8/79
Criminal victimization in urban schools, NCJ-56396, 8/79
Crime against persons in urban, suburban, and rural areas, NCJ-53551, 7/79
An introduction to the National Crime Survey, NCJ-43732, 4/78
Local victim surveys: A review of the issues, NCJ-39973, 8/77

National Prisoner Statistics

BJS bulletins:
Prisoners at midyear 1983, NCJ-91034, 10/83
Capital punishment 1982, NCJ-89395, 7/83
Prisoners in 1982, NCJ-87933, 4/83
Prisoners 1925-81, NCJ-85861, 12/82

Prisoners in State and Federal institutions on December 31, 1981 (final report), NCJ-86485, 7/83
Capital punishment 1981 (final report), NCJ-86484, 5/83

1979 survey of inmates of State correctional facilities and 1979 census of State correctional facilities:
Career patterns in crime (BJS special report), NCJ-88672, 6/83

BJS bulletins:
Prisoners and drugs, NCJ-87575, 3/83
Prisoners and alcohol, NCJ-86223, 1/83
Prisons and prisoners, NCJ-80697, 2/82
Veterans in prison, NCJ-79632, 11/81

Census of jails and survey of jail inmates:
Jail inmates 1982 (BJS bulletin), NCJ-87161, 2/83
Census of jails, 1978: Data for individual jails, vols. I-IV, Northeast, North Central, South, West, NCJ-72279-72282, 12/81
Profile of jail inmates, 1978, NCJ-65412, 2/81
Census of jails and survey of jail inmates, 1978, preliminary report, NCJ-55172, 5/79

Parole and probation

BJS bulletins:
Probation and parole 1982, NCJ-89874 9/83
Setting prison terms, NCJ-76218, 8/83
Characteristics of persons entering parole during 1978 and 1979, NCJ-87243, 5/83
Characteristics of the parole population, 1978, NCJ-66479, 4/81
Parole in the U.S., 1979, NCJ-69562, 3/81

Courts

State court caseload statistics: 1977 and 1981 (BJS special report), NCJ-87587, 2/83
State court organization 1980, NCJ-76711, 7/82
State court model statistical dictionary, NCJ-62320, 9/80
A cross-city comparison of felony case processing, NCJ-55171, 7/79
Federal criminal sentencing: Perspectives of analysis and a design for research, NCJ-33683, 10/78
Variations in Federal criminal sentences, NCJ-33684, 10/78
Federal sentencing patterns: A study of geographical variations, NCJ-33685, 10/78
Predicting sentences in Federal courts: The feasibility of a national sentencing policy, NCJ-33686, 10/78
State and local prosecution and civil attorney systems, NCJ-41334, 7/78

Expenditure and employment

Justice expenditure and employment in the U.S., 1979 (final report), NCJ-87242, 12/83
Justice expenditure and employment in the U.S., 1979: Preliminary report, NCJ-73288, 1/81
Expenditure and employment data for the criminal justice system, 1978, NCJ-66482, 7/81
Trends in expenditure and employment data for the criminal justice system, 1971-77, NCJ-57463, 1/80

Privacy and security

Computer crime:
Electronic fund transfer and crime, NCJ-92650, 2/84
Computer security techniques, NCJ-84049, 9/82
Electronic fund transfer systems and crime, NCJ-83736, 9/82
Legislative resource manual, NCJ-78890, 9/81
Expert witness manual, NCJ-77927, 9/81
Criminal justice, NCJ-61550, 12/79

Privacy and security of criminal history information:
A guide to research and statistical use, NCJ-69790, 5/81
A guide to dissemination, NCJ-40000, 1/79
Compendium of State legislation: NCJ-48981, 7/78
1981 supplement, NCJ-79652, 3/82

Criminal justice information policy:
Research access to criminal justice data, NCJ-84154, 2/83
Privacy and juvenile justice records, NCJ-84152, 1/83
Survey of State laws (BJS bulletin), NCJ-80836, 6/82
Privacy and the private employer, NCJ-79651, 11/81

General

BJS bulletins:
Federal drug law violators, NCJ-92692 2/84
The severity of crime, NCJ-92326, 1/84
The American response to crime: An overview of criminal justice systems, NCJ-91936, 12/83
Tracking offenders, NCJ-91572, 11/83
Victim and witness assistance: New State laws and the system's response, NCJ-87934, 5/83
Federal justice statistics, NCJ-80814, 3/82
Report to the nation on crime and justice: The data, NCJ-87068, 10/83
1983 directory of automated criminal justice information systems, NCJ-89425, 10/83
Sourcebook of criminal justice statistics, 1982, NCJ-86483, 8/83
BJS five-year program plan, FY 1982-86, 7/82
Violent crime in the U.S. (White House briefing book), NCJ-79741, 6/82
Dictionary of criminal justice data terminology: Terms and definitions proposed for interstate and national data collection and exchange, 2nd ed., NCJ-76939, 2/82
Correctional data analysis systems, NCJ-76940, 8/81
Technical standards for machine-readable data supplied to BJS, NCJ-75318, 6/81
Justice agencies in the U.S., 1980, NCJ-65560, 1/81
Indicators of crime and criminal justice: Quantitative studies, NCJ-62349, 1/81
A style manual for machine-readable data, NCJ-62766, 9/80
Myths and realities about crime, NCJ-46249, 10/78

To be added to any BJS mailing list, copy or cut out this page, fill it in and mail it to:

National Criminal Justice Reference Service
User Services Dept. 2
Box 6000
Rockville, MD 20850

If the name and address on the mailing label below are correct, check here ☐ and don't bother to fill them in again. If your address does not show your organizational affiliation (or interest in criminal justice) please put it here:

If your name and address are different from the label, please fill them in:

Name:

Title:

Organization:

Street or box:

City, State, Zip:

Telephone: ( )

Interest in criminal justice:

Please put me on the mailing list(s) for:

☐ **All BJS reports**—30 to 40 reports a year, including 12 bulletins and many special reports

☐ **BJS Bulletins**—timely reports of the most current justice data

☐ **Courts reports**—State court caseload surveys, model annual State court reports, State court organization surveys

☐ **Corrections reports**—results of sample surveys and censuses of jails, prisons, parole, probation, and other corrections data

☐ **National Crime Survey reports**—the Nation's only regular national survey of crime victims

☐ **Sourcebook of Criminal Justice Statistics** (annual)—a broad spectrum of data from 153 sources in an easy-to-use, comprehensive format (433 tables, 103 figures, index)

U.S. Department of Justice
Bureau of Justice Statistics

Official Business
Penalty for Private Use $300

Postage and Fees Paid
U.S. Department of Justice
Jus 436

THIRD CLASS
BULK RATE

Washington, D.C. 20531

Special Report

END