U.S. Department of Justice
Bureau of Justice Statistics

COMPUTER CRIME

Electronic Fund Transfer Systems and Crime

Bureau of Justice Statistics
U. S. Department of Justice

Benjamin H. Renshaw, III
Acting Director

Carol G. Kaplan
Assistant Director,
Federal Statistics and Information Policy

U.S. Department of Justice
Bureau of Justice Statistics

Computer Crime

Electronic Fund Transfer Systems and Crime

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402

Prepared by:

Kent W. Colton, Ph.D.
James M. Tien, Ph.D.
Sherry Tvedt Davis, M.C.P
Bruce Dunn, M.P.A
Arnold I. Barnett, Ph.D.

July 1982

This document was prepared for the Bureau of Justice Statistics, U.S. Department of Justice by Public Systems Evaluation, Inc., and was supported by Grant Number 80-BJ-CX-0026. Points of view or opinions stated herein are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

NCJ-83736

PREFACE

The use of computers in the financial community has grown rapidly over the past decade at both the consumer and corporate levels. This report reviews the crime-related implications of this growth and tries to determine--to the extent possible--the nature and magnitude of EFT crimes. Some of the questions addressed in the report include: What is EFT? How has it grown and developed over the past decade, and what growth can be expected in the future? What sources are available, if any, to examine the nature and extent of EFT crimes? And, if available sources do not exist, what procedures could be used to effectively assess EFT crime in the future?

In addressing these questions the Bureau of Justice Statistics has tried to stimulate a range of research activities. An extensive literature search has been conducted to identify sources of relevant data, and site visits have been made to explore the potential use of these sources, and to confer with financial and EFT experts. Further, an advisory panel of EFT and criminal justice experts from business and government was established to review the work on the project and to recommend and identify further sources of information.

It is hoped that the recommendations and findings in this report will engender informed discussions in the criminal justice, financial, and computer communities about the relationships between EFT systems and crime. As our reliance on electronic payment systems increases, it is important that criminal justice professionals recognize and react to the potential for criminal abuse.

Benjamin H. Renshaw
Acting Director
Bureau of Justice Statistics

Public Systems Evaluation, Inc.
Cambridge, Massachusetts

EXECUTIVE SUMMARY

Over the past decade computers and computer-based technologies have come to play an increasingly dominant role in processing and carrying out financial transactions. Accompanying this growth has been a concern, expressed both within the law enforcement and financial communities, that increased reliance on electronic banking technologies--commonly referred to as "electronic funds transfers" or EFT--may create the potential or opportunity for new types of criminal activity, in particular computer-related white collar crimes. However, there has been very little systematic analysis of the relationship between EFT and crime. The purpose of this report, then, is to examine the nature and extent of EFT-related crime. Five issue areas are addressed:

- **What is EFT?** A functional definition of EFT is developed and specific technologies and applications are identified.
- **What is the state-of-the-art for EFT use? What can be expected in the future?** The current use of EFT is described and potential scenarios for the future are identified.
- **What is EFT crime? How can it be analyzed?** A definition of EFT crime is developed, and a classification framework for describing the nature and extent of such crimes is presented.
- **What sources of data on EFT crime exist?** The nature and problems of the primary existing data sources for EFT crimes are discussed.
- **How can the extent of EFT crime be estimated?** Several statistical approaches that could be used to make a statistically valid estimate of the occurrence of EFT crimes are considered.

What is EFT?

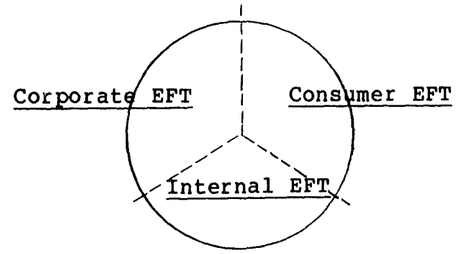
Five specific technologies are generally considered to fall under the rubric of EFT. Three provide financial services which are consumer-oriented. (Consumer-oriented services are often referred to as retail EFT.) Point-of-Sale (POS) systems are computer terminals located in retail stores that can be used to debit a customer's account and credit a merchant's account at the time a purchase is made, as well as

to authorize, verify, or guarantee a check. Automated teller machines (ATMs) are terminals that function much as a human teller and allow account holders to make a range of simple financial transactions such as deposits, cash withdrawals or advances, transfers and bill payments. Access to ATMs is acquired by inserting a magnetically-encoded plastic card and entering the companion personal identification number (PIN). In telephone banking, the customer uses a telephone to access a bank's computer, then presses the touch-tone buttons or instructs a bank employee to make a financial transaction. Its most common application is telephone bill paying (TBP) which allows a customer to enter an account number, PIN, and payment information to debit his or her account and credit a merchant's account.

Two other widely used EFT technologies provide primarily corporate-oriented EFT services. Automated clearing houses (ACHs) electronically gather--by the use of magnetic tapes--transactions from financial institutions, sort the transactions by receiving institution, and send the data on to the receiving institutions. A common application of ACH services is direct deposit of payrolls. Wire transfers are used to make interbank and intrabank money transfers into and out of individual, corporate, financial institution, and Federal Reserve accounts. A growing aspect of corporate EFT is cash management services in which financial institutions allow corporate customers to access account records and intitiate transactions electronically.

Although these five technologies are commonly identified with EFT if EFT is defined only in terms of specific technologies--as is too often the case--the full range of potential applications may be overlooked. More broadly, EFT systems can be thought of as payment systems that permit transactions--an "exchange of value"--where the value or money is represented by electronic messages. (As a contrast, in paper-based payment systems, value may be represented by such items as currency and coin, or checks). EFT systems also include the electronic exchange of information that facilitates financial transactions. Thus, a literal interpretation of the term "electronic funds transfer" would describe not only the technologies discussed above, but also applications such as the computerized processing of checks, electronic debits and credits to accounts made at teller terminals, and the internal processing of data at financial institutions.

From this perspective, the types of financial services provided by EFT systems may be thought of as falling into the three overlapping categories illustrated at the top of page v: 1) consumer-oriented EFT services (e.g., check



authorization, bill payments, purchases, deposits, withdrawals, etc.); 2) corporate-oriented EFT services (e.g., direct deposits of payroll, corporate interbank and intrabank transfers, wire transfers, etc.); and 3) internal EFT services (i.e., computerized processing of transactions within financial institutions etc.).

What is the State-of-the-Art for EFT Use? What Can Be Expected in the Future?

To understand the potential impact of EFT systems on crime, it is important to recognize the current status and anticipated growth of EFT technologies and services. This report presents transaction and dollar volumes for currency, check, and credit card payments. Several conclusions can be drawn from these baseline figures:

- ATMs are the most frequently used of the consumer EFT technologies. In 1980, for example, 102 million transactions were made each month from 17,000 terminals. The growth in ATM use and installations has been phenomenal. Two years earlier, in 1978, an estimated 39 million transactions were made each month from slightly less than 10,000 ATMs; by 1980 an estimated 25,000 ATMs had been installed. This substantial growth in ATM use is expected to continue for a number of years and throughout the century.

- POS systems have achieved only modest use. In 1978 an estimated 10 million POS transactions were made each month from 13,000 terminals. However, many terminals were used exclusively for check authorization and guarantee. POS growth is expected to occur on a regional rather than national basis.

- The use of TBP services has been somewhat limited. TBP services were offered by only 249 financial institutions in 1979 with a total of 425,000

accounts. However, growth is expected as the range of home banking services is expanded and many financial institutions are not conducting home banking experiments.

- ACHs are widely used. The 32 ACHs in the U.S. processed 18.9 million transactions each month in 1980 and 25.0 million each month in 1981. Continued growth in the use of ACHs is expected as more government agencies--and to a lesser extent private companies--turn to direct deposit of payrolls.

- Growth in the wire transfer area for interbank and intrabank transfers has been phenomenal. Data for two wire transfers services--Fed Wire and CHIPS--indicate that about 4.7 million wire transfers were completed each month in 1980.

- Although the volume of ACH transactions exceeds that of wire transfers, substantially more money is exchanged via the latter. In 1980 a total of $117 trillion was transferred on Fed Wire and CHIPS while the total for all ACHs was only $129 billion.

- Although the number of consumer EFT transactions exceeds the number for corporate EFT, the dollar values of corporate EFT transactions are substantially higher. For example, in 1980 the average ATM transaction was only $36, while the average Fed Wire transfer exceeded $1.8 million and the average CHIPS transaction exceeded $2.8 million. However, the number of ATM transactions in 1980--about 1.2 billion--is many times larger than the 56.4 million Fed Wire and CHIPS transfers.

- When compared to nonEFT transactions, consumer EFT transactions represent only a small portion of all financial activities. The number and value of corporate EFT transactions--particularly wire transfers--dominate the nation's payment system.

These baseline figures suggest that the EFT system is still evolving and that the rapid growth is expected to continue. Given this scenario, questions naturally arise--what is EFT crime? how can we examine its nature and extent?

What Is EFT Crime? How Can It Be Classified?

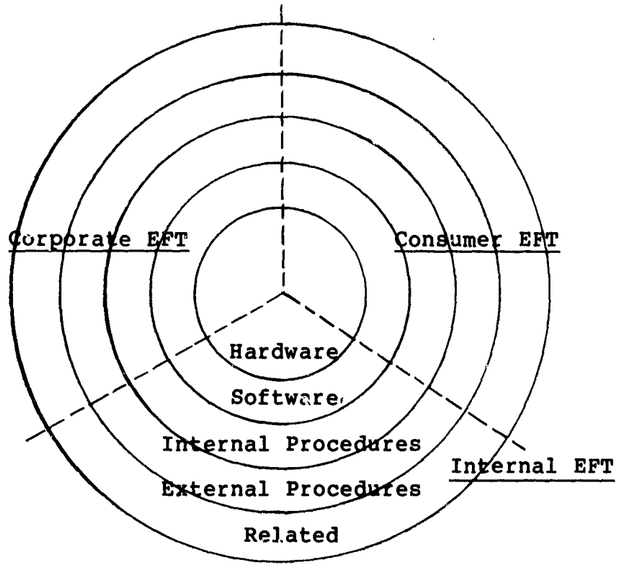
A range of alternatives can be developed to define EFT crime, each with its strengths and weaknesses. On the one

hand, traditional legal categories of crime (e.g., fraud or theft) can be used to describe EFT crime. But they reveal little about how the computer or EFT technology was involved in the crime. On the other hand, new classification systems could be developed based on the role of EFT technology in the commission of the crime, but there is little consensus as to how narrow or broad such classification approaches should be. From our perspective, a broad definition is probably the most useful and applicable, and the most likely to capture a full range of possible EFT crime incidents. Thus, any crime, whether prosecuted or not under traditional or special computer/EFT laws, that would not have occurred <u>but for</u> the presence of an EFT system is considered an "EFT crime."

Given this definition, a range of EFT crimes can be identified. The problem remains, though, as to how to categorize these crimes in a manner that will be most useful in understanding their nature and extent. Therefore, a "layered approach" is developed to classify EFT crimes according to the category of EFT and the component of the EFT system which is compromised by the crime. (It is recognized that the distinctions between these layers are somewhat artificial and that a particular crime may actually fit in more than one category. In the future, it may be useful to design a hierarchical classification scheme based on these categories.)

The three categories of EFT were identified earlier: consumer, corporate, and internal. In addition, five overlapping layers of EFT components can be envisioned. At the base of an EFT system is the hardware that allows transactions to be initiated, completed, and recorded. The next component is the software that "tells" the computer how to process transactions. The internal procedures followed by a financial institution in the day-to-day operation of the EFT system constitute the third component. The fourth is the external procedures followed by customers when they use EFT systems. And the final layer consists of any other behavior or action related to the presence of EFT. The diagram at the top of page viii illustrates the relationship between these layers of EFT components and the three categories of EFT technologies.

Additional dimensions can be used to further classify or explain EFT crime. Three identified and described in this report are system vulnerability, type of loss or "target asset," and the relationship of the perpetrator. Understanding these dimensions provides further insight on the type of information that might be collected in any system developed to examine the nature and extent of EFT crime.



What Sources of Data On EFT Crime Exist?

After defining EFT and reviewing possible classification approaches for EFT crime, the next question is--what sources of data exist? Unlike the general criminal justice field where the FBI Uniform Crime Reports serves as the primary source of reported crime, the EFT field does not have a comparable single source. Thus, a detailed literature search was conducted and a large number of experts thro ghout the country were interviewed in an attempt to identify sources of EFT crime data. Unfortunately, no adequate data sources were found, and very little is known concerning the nature and extent of EFT crime. A few impressions concerning the nature and incidence of EFT crime emerged from our discussions and the literature review, but it is important to carefully qualify these views as they are only impressions and are not based on rigorously acquired facts or data.

- Although we do not know the precise level of computer-related or EFT crime, EFT crime is still only a very small portion of all crimes at financial institutions

- The fraud associated with ATMs appears to be at least no worse than it might have been if the same transactions were conducted in a purely paper-based system.

- Although the number of consumer-related EFT crimes will probably grow over time as the technology expands and people become more aware of the possibilities for crime, the actual magnitude of any particular crime will generally be small because of the nature of the technology and the imposition of transaction limits.

- Customer frauds such as overdrafts or bad checks might be reduced by the use of consumer EFT technologies which provide for an electronic check of the assets held in any account. EFT also reduces the need to physically transfer financial assets, removing the opportunity for crimes such as personal and armed robbery.

- Although the actual level of corporate EFT crime to date is probably small, the potential for such crime is high because of the extremely large dollar volumes transferred each day.

- Although experts tend to agree that some EFT technologies may reduce the incidence of crimes such as burglary, larceny and fraud, the potential for loss is sufficiently great to cause dispute over the general impact of EFT on crime. For example, in the past, the magnitude of a few specific EFT crimes has been very high, particularly in the corporate EFT area, indicating a special vulnerability.

After a thorough search, four sources were identified as having the greatest potential to provide reliable information on the nature and extent of EFT crime: a file of computer abuse cases compiled at SRI International by Donn Parker and Susan Nycum; reports filed by financial institutions with their federal regulators; files on federal bank crimes kept by the Federal Bureau of Investigation (FBI); and a study on financial fraud conducted by the American Institute of Certified Public Accountants (AICPA). Each of these, along with a few surveys and miscellaneous materials, was examined in depth. A brief summary of the findings follows.

SRI Computer Abuse File. This file originated in the early 1970s as the focus of a National Science Foundation sponsored study on computer crime; later, funding support was provided by the Justice Department. Just as this project examines the criminal implications of EFT use, the SRI effort sought to identify computer crimes and to obtain some perception of their nature and extent. The file, an ongoing compilation of over 1000 computer abuse cases identified

through individual contacts and a newspaper clipping service is the most well-known record of computer crime--although it does not rely on any systematic or scientific data collection techniques.

The file focuses on computer abuse in general, rather than on EFT specifically, but a majority of the cases from financial institutions were identified as EFT-related. The file provides important information on the nature of computer crime, but is limited as a source of data to measure the extent of EFT crime as it includes only those cases which were selected by the media or the researchers. For example, large losses or unique crimes often bring a case to the attention of the researchers, but do not provide a random sample of information. Compounding the problem is the fact that EFT-specific crimes were not a primary focus of the SRI researchers, but a by-product of the collection effort. The file is a useful collection of cases, but it is not a statistically valid sample.

Federal Regulators. Until recently, all the federal regulatory agencies (i.e., Comptroller of the Currency, Federal Deposit Insurance Corporation, Federal Reserve Board, Federal Home Loan Bank Board) required financial institutions to report external (e.g., robbery, burglary) and internal (e.g., employee fraud, embezzlement) crimes. In general, the report consisted of a letter or standard form which identified the apparent irregularity and described the nature of the incident. These reports provided--and to some extent still provide--a potential source for EFT crime data.

Now, however, a bank must report only internal crimes and maintain an informal, in-house record of each external crime. Consequently, information on external crimes at financial institutions will no longer be available in a reasonably accessible form. Also, as the regulators use crime reports for specific and limited purposes, they are not collected or maintained in a manner which would easily identify or aggregate EFT crimes.

Although the federal regulators are a potential source of data on EFT crime, they could not provide information without major policy and procedural changes. Not only would the reports on external crimes need to be reinstated, but the reporting forms would have to be significantly altered to allow the retrieval of data on EFT or computer crimes.

Federal Bureau of Investigation Files. The FBI investigates most cases of bank fraud and embezzlement and maintains case records on federal offenses (financial crimes are considered federal offenses if the bank is federally-

chartered or if bank assets cross state lines in the course of a criminal act). Information on each case is recorded for historical and investigative purposes, and a variety of recordkeeping systems are maintained.

However, the FBI does not identify the use of a computer or EFT system in a case because it has no special bearing on broad law enforcement or prosecutorial efforts. In addition, although the FBI investigates the majority of financial crimes, records for many small bank crimes are usually maintained only at the local level. Thus, the national FBI records omit many EFT crimes, while emphasizing large losses and complex scenarios. Further, the FBI has a policy against providing case information on a regular basis, and numerous regulations emphasize extreme confidentiality.

The FBI is another potential source of data on EFT crime, but not without important modifications in their policies and procedures. A new federal law would have to be passed to make computer or EFT crimes a federal offense--and thus under the purview of the FBI--and new data collection procedures would have to be established to allow the retrieval of information on such crimes.

American Institute of Certified Public Accountants Study. In 1979 the AICPA decided to examine computer fraud in hopes of establishing appropriate accounting and auditing standards. It approached the task on an industry-by-industry basis, starting with banking. In cooperation with the Bank Administration Institute, 9,000 commercial banks were surveyed regarding computer fraud. The banks were selected to represent a geographic sample of the industry, and the sample was picked to assure that all of the major financial institutions were included.

However, the survey did not focus on the extent of computer fraud in banking. Rather, each institution was asked to describe only one case on the provided questionnaire. More than one-half of the sampled banks replied, although the vast majority indicated no computer fraud problems. Of the 5,000 responses, only 106 computer fraud cases were developed and only 85 were eventually classified as computer crimes. Unfortunately, although the study provides useful information on the nature of EFT crimes, it cannot be used to statistically estimate the extent of EFT crime as it asked for only one example of an EFT or computer crime, not the actual incidence of all such crimes.

After reviewing these and other possible sources of information on EFT crime our conclusion is that none provides

valid data for measuring and understanding the nature and extent of EFT crime. Each has only limited information, and all have problems from a statistical perspective. Further, although several offer a possible source of information, the potential exists only if major changes are made in the collection processes--changes which seem highly unlikely to occur without an explicit, concerted effort. These sources offer perceptions or clues about the actual incidence of EFT crime, but do not provide an adequate data base for statistical analysis.

How Can The Extent of EFT Crime Be Estimated?

From the outset of the study, we have tried to develop creative approaches to use existing, or new, data to estimate the occurrence of EFT crime. For example, we initially hoped to be able to compare two or more existing data sources to estimate the EFT crime problem by employing a modified version of the "capture-recapture" statistical technique. The concept is relatively simple: a sample of the population is captured, tagged in some suitable fashion, and then released. Subsequently, a second sample of the same population, now containing both tagged and untagged specimens, is obtained. The fraction of the second sample that had been tagged previously is used to estimate the total population size. The application of this technique to estimate the number of EFT crimes is straightforward if the capture-recapture series is considered as a set of independent and equivalent lists, files, or sources of information on EFT crimes. The lists can be compared to identify crimes contained in one or more lists and to estimate the missing or "hidden" population of all EFT crime. However, the available data sources do not yield lists of EFT crimes that are amenable to capture-recapture or other statistical analysis. More specifically, they are not detailed enough, not independently compiled, not based on a statistically valid sample, and not equivalent.

Given the dearth of existing EFT crime data, an alternative statistical technique that could be used to measure the nature and extent of the EFT crime was developed. We recommend that a national panel, or sample, of banks be established to provide an ongoing source of information on EFT crimes. In much the same manner that A.C. Nielsen Co. rates different television programs based on data collected from a national panel of some 1200 households, the EFT crime problem could be estimated based on data collected by an "EFT crime panel" of a limited number of financial institutions. A representative sample of financial institutions would be

selected to participate in the panel, and data would be gathered using special collection instruments for prescribed periods of time. Many issues need to be examined before such a panel is established. Three of these--panel stratification, the underlying model, and panel size--are addressed below.

Panel Stratification. The panel should be representative of the universe of U.S. financial institutions. In order to achieve this, the panel should be stratified to reflect at a minimum, the types, locations, and asset sizes of such institutions. However, if asset size is implicitly taken into consideration in the underlying model of the panel, then one possibility is to consider only the type and location dimensions. Realizing that the resources to collect such data are likely to be limited, it may be possible to group all financial institutions into two types (i.e., commercial banks and thrift institutions) and three locations (i.e., east, central and west). This results in a stratified EFT crime panel with six cells.

Panel Model. To determine the number and composition of banks in each of the six cells, it is necessary to develop a model which describes the underlying process. We therefore developed an initial model that could estimate the magnitude of the problem nationwide by extrapolating from the data provided by the panel of financial institutions. We stress the word "initial"; it is the very nature of statistical modeling that one must be careful that the results of our analysis do not contradict the assumptions used to obtain them. Further, statistical rigor should be accompanied with the flexibility to respond to unexpected events. The underlying model presented in the report is based on the following two assumptions: (1) the number of reported EFT crimes from a given bank over a fixed period follows a Poisson probability distribution; and (2) the Poisson parameter corresponding to a given bank is directly proportional to the asset level of that bank.

Panel Size. Based on some preliminary data collection efforts and the reported national distribution of banks by asset size and region, some sample calculations for panel size were made. Again, assuming limited resources, it might be feasible to have an initial size in the range of 50 banks. A panel of this size would provide reasonable accuracy levels for each of the cells, so that each could be a focus of interest, not only in terms of its contribution to the total panel size but also for itself. We also recommend that 20 percent of the national panel be systematically replaced each year.

The design of data collection instruments for the panel would ultimately be based on the three categories of EFT technologies (consumer, corporate, and internal) and would utilize the layered classification framework described earlier. Three major types of data would need to be collected. The first is an EFT transactions baseline that would summarize the extent of the institution's EFT services and record aggregate dollar and transaction volumes. The collection of the second type of data--EFT crimes--would be done on a case-by-case basis. The participating institutions would be asked to complete a special report describing each detected EFT crime. The third type of data would be a baseline of nonEFT transactions which would be used to examine EFT crime-based losses as compared to all financial transactions.

Financial institutions have traditionally been reluctant to release information on the type and extent of financial transactions. Information about the incidence of white collar crimes, including EFT crimes, has been viewed as particularly sensitive and thus it may be a problem to secure participation in such a panel. To encourage participation, the security of the requested information, as well as its value, would need to be demonstrated to bank officials. Bankers should be reminded that concrete data on the incidence of EFT crime may dispel fears about the safety of the systems. All participating institutions would be guaranteed anonymity, and data would only be reported in an aggregate form. Further, some form of cosponsorship with an established professional organization may be desirable.

A national EFT panel, as proposed in the report, is clearly an ambitious undertaking. Time and cost constraints may therefore make it appropriate to implement the panel with a phased approach. The first phase would focus on collecting data from only a subset of the panel--for example, one or two cells (perhaps one type of institution or one region and one asset size) could be chosen. The subpanel would still need to be large enough to be representative, but because the data from the chosen cells would not be used to make assertions about the others, the cost of beginning the panel would be lower. Data concerning a few cells of the panel could be gathered, analyzed and published; and at the same time the first phase could serve as a test of the panel concept and as an aid in deciding whether the panel should be implemented on a full scale basis.

The panel approach has several advantages. It would provide a "clean" source of data that could be confidently used to draw conclusions about the incidence of EFT crime. It would also allow the systematic review of EFT crimes

relative to total EFT and nonEFT transactions. In order to provide a greater understanding of the problems and potential for gathering information on EFT crimes, a preliminary effort was undertaken as a part of this study to collect at least some crime-related data from a small number of financial institutions. The results of this effort--especially as they provide insights concerning the potential of the panel approach--are discussed in the report.

The overall conclusion from the site visits and the preliminary data collection is that it is feasible to collect data on the incidence of EFT crimes from financial institutions especially in the area of consumer EFT crimes. Frauds and misuses stemming from EFT services are routinely investigated and recorded by financial institutions. In addition, baseline data for overall EFT transactions can be retrieved with relative ease. More importantly, at least some financial institutions would release this information, if appropriate safeguards for anonymity and confidentiality are implemented and the need and value of the data are established. However, although data on consumer and corporate EFT crimes are available and retrievable, it appears that it will be difficult to collect data on internal EFT crimes.

A final finding which emerged from the preliminary data collection effort does not relate to implementing the panel, but to the benefits of participating. The need to share information on preventing EFT losses as well as identifying EFT scams was mentioned several times in the interviews. A few informal arrangements exist between financial institutions to meet and discuss EFT security issues. But in most cases, one financial institution is usually unaware of the nature of EFT losses at another, even though both may be victims of the same or similar schemes. The proposed national panel would provide a formal mechanism to share such information among the members and to disseminate it to the entire financial community.

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

LIST OF EXHIBITS

1 INTRODUCTION

It is increasingly recognized that computer technology is a two-edged sword. It has the potential to create new opportunities and solve current issues; yet left unattended, it may create new problems. Electronic funds transfer (EFT), one application of computer technology, holds great potential for the future: it can process financial transactions rapidly and provide users with important data in a timely fashion. However, it may also lead to certain negative consequences, such as increasing the degree of integration and concentration within society, thereby creating the opportunity for abuse or control by a few and limiting the opportunity for participation by others. It is thus appropriate to monitor the implementation and evolution of such a technological innovation as it impacts society.

The purpose of this report is to address one of the potential problem areas surrounding EFT--namely, criminal abuse. What is the extent and nature of EFT-related crime? How can we improve our ability to monitor the impact of such problems in the future? At the outset of the study, five principal objectives for the research were identified:

- To analyze the nature of EFT, both to identify a functional definition and to examine the state-of-the-art and future scenarios.
- To analyze the nature of EFT crimes and to develop a functional definition and classification system for these crimes.
- To assess the probable trends regarding EFT criminal activity.
- To identify the major problems associated with current estimates of the extent and impact of such crimes.
- To identify future approaches to monitor the extent and impact that such EFT crimes will have on society.

This report deals with all five of these objectives; accordingly, five major chapters follow this introduction. Chapter 2 defines EFT systems. It sets forth a broad, functional definition of EFT and develops a framework that relates EFT services and technologies. Chapter 3 examines the "state-of-the-art" for EFT as well as projections for its future. Such information is important in relating the development of EFT technologies to potential criminal abuse.

Chapter 4 develops a framework for the analysis of EFT crime. It defines EFT crime, reviews types of EFT crimes, and outlines alternative classification systems from both a legal and a problem/solution perspective. Although it is not necessary to agree on one classification approach at this point (and in fact, it may be counterproductive to try to do so), developing a general framework for analysis is essential to identify the kinds of information that will be most useful in measuring the nature and extent of EFT crime. Chapter 5 examines existing sources of information related to EFT crime. A number of sources were identified and reviewed, but each--in its current form--has only a limited amount of information. Several have potential as a source of data but only if major changes are made in the collection process--changes which seem highly unlikely. Therefore the final chapter of the report outlines a possible new approach to measure the nature and extent of EFT crime. Although questions remain as to how to best monitor the level and impact of EFT crime and further research is required, answers for some of these questions are discussed in Chapter 6.

2 DEFINITION OF ELECTRONIC FUNDS TRANSFER SYSTEMS

To systematically examine the nature and extent of EFT crime it is essential that a common understanding of the underlying technology be established. Identifying EFT crimes is dependent on first recognizing the types of activities that constitute "electronic funds transfers." Defining and organizing EFT systems is reminiscent of the proverbial story of the blind men describing the elephant. Each author tends to highlight EFT from his or her unique perspective. We shall be like the rest, developing our definition and grouping EFT services and technologies so as to best relate EFT and criminal activity.

This chapter therefore begins with a definition of EFT, which is then used to describe the types of financial services offered through EFT as well as to identify the principal EFT technologies in use today. Later chapters in the report will relate these definitions and groupings to actual and potential EFT-related criminal activity.

2.1 DEFINING EFT

In defining EFT it is useful to have some idea of the varying nature of financial transactions. Financial transactions are exchanges of value, with no less than one side of the exchange having a specific monetary value. However, money can take at least four basic forms in our society: currency, checks, credit cards, and EFT transactions. Each form requires a support system of varying complexity to facilitate economic activity. To illustrate these forms of money and to examine their differences, we will review the simple example of a portable television purchased from a department store. (For the seasoned observer of financial transactions, the example will be elementary. It is included for those who may be new to the world of finance.)

Financial transactions using currency are relatively simple. In our example, the consumer hands the clerk the appropriate amount of currency, picks up her television set and goes home. The financial transaction is complete and direct. A national treasury is required to mint and manage the currency, but little direct financial institution support is required at the time of the transaction.

Payment by check increases the complexity of the process. In our example, the consumer writes a check for the amount needed, takes the television set and goes home. The

store has received value. However, although checks are legally negotiable, they are not socially negotiable. (By socially negotiable we mean accepted by common custom; for example, most of the store's employees would not want to be paid with endorsed checks.) Therefore, to transfer the check's value into usable form, the store needs to make another financial transaction. It deposits the check at its financial institution and the value is added to the balance of the store's checking account. This example illustrates two important points about checking transactions. First, checks are tied to financial institutions. A support structure is needed to arrange the transfers of checks and account balances. Second, the transfer process takes time. While a currency transaction takes place instantaneously, the checking cycle may take several days to complete.

Payment by credit card is even more complex because both purchase and loan functions are exercised. Using our example, the consumer hands the clerk her credit card so the clerk can prepare an invoice/receipt. The consumer signs the invoice, takes the copy and the television set and goes home. At month's end she receives a bill in the mail which she pays by check.

Although the use of credit cards often involves checks, the actual number is uncertain. Several checks may be written for one purchase, or several monthly credit card purchases may be combined on one bill and paid by one check. However, it is clear that consumer credit card use has increased the dependency on checking accounts. The mechanics of using a credit card generally require a checking account, so "currency-only" consumers who want credit cards almost always acquire checking accounts. In addition, the emergence of credit cards has influenced the support system for transferring money. To encourage wide credit card acceptance, a linking mechanism has been developed between sellers, credit issuers and financial institutions. In essence that system has become an integral aspect of our economy.

Electronic funds transfers include a wide range of payment technologies and systems. If all these technologies were available to the consumer in our example she would have her choice of how to buy the television set. For example, she could use an automated teller machine to get currency from her account to pay for the television; have the clerk use an electronic check guarantee system to assure the store her check would be honored; or hand the clerk a debit card to insert into a point-of-sale terminal and immediately debit her checking account.

The institutions involved in the EFT support system are similar to those in the checking support system. Financial institutions provide deposit, checking, and loan services to consumers, businesses, and government. Clearing houses and the Federal Reserve facilitate transfers between financial institutions, and a range of federal regulators oversee the process. The primary difference in the transaction and support structure for EFT is the medium of communication. EFT involves money represented by electronic signals, not by paper such as currency, checks, or credit card invoices. This communication requires an electronic network to connect businesses with financial institutions, and computers are needed to manage this new high speed electronic network.

This discussion of financial transactions leads to an initial definition of EFT. In essence, EFT systems are payment systems in which the exchange of value or money is represented by electronic messages.* These systems also include the exchange of electronic information that facilitates a financial transaction (e.g., a check guarantee). Conventionally, such a definition focuses on specific technologies and applications; the wide range of technologies which support these exchanges of value and information are discussed later in this section.

2.2 ORGANIZING EFT SERVICES AND TECHNOLOGIES

The definition above provides a broad guide for our analysis, but further refinement is required in order to first relate EFT services with specific technologies and then to relate these technologies and services to criminal activity. We will therefore develop a framework to link EFT services with specific technologies.

EFT Financial Services

Financial transactions in the United States occur within a complex system of financial institutions (i.e., commercial

---

*Our definition is conceptually similar to the one used by the National Commission on Electronic Fund Transfers:

> EFT is a payments system in which the processing and communications necessary to effect economic exchange, and the processing and communications necessary for the production and distribution of services incidental or related to economic exchange, are dependent wholly or in large part on the use of electronics[NCEFT,1977a].

banks, savings and loan associations, mutual savings banks, and credit unions) and government regulatory agencies (i.e., Comptroller of the Currency, Federal Deposit Insurance Corporation, Federal Reserve Board, Federal Home Loan Bank Board, and National Credit Union Administration). Exhibit 2-1 lists the principal institutions involved with EFT. These institutions offer a wide range of financial services and as EFT becomes more prevalent many will be provided through EFT.

Exhibit 2-2 lists the kinds of financial services that are currently provided through the application of EFT technologies. These services are subdivided into three sometimes overlapping categories which will be used throughout this report when we talk about the link between EFT and crime. The first group is consumer-oriented EFT services and is divided in two parts: services which facilitate the transfer of information, and services which transfer money directly. Information transfer services include check authorization, check verification, check guarantee and file look-up. These generally give the consumer and the retailer direct access to financial information which assists in the transfer of money through authorization and guarantee. A number of EFT consumer-oriented services involve the direct transfer of funds. The range of financial transactions includes deposits, cash withdrawals, bill or loan payments, debit purchases, interaccount transfers, overdraft privileges, credit purchases, and cash advances. These are essentially the same services that a consumer would have using a standard checking or credit card account. The distinction is that with EFT, the services are provided through an electronic communications network.

The second group is corporate-oriented EFT services. These services use electronic communications to make institution-to-institution or institution-to-consumer money transfers. The most dominant of these services is wire transfers, generally used by corporations to make large payments to other firms and individuals. Occasionally wire transfer services are used to make individual-to-individual money transfers, but these constitute only a very small portion of the overall volume.* Another integral part of corporate EFT is cash management services in which financial institutions allow corporate customers to access account

*Although this study focuses on wire transfers made through financial institutions, it is recognized that insurance companies, brokerage houses, retail stores, and other businesses may employ internal wire systems.

Exhibit 2-1

Institutions Involved With EFT

Financial Institutions

Commercial Banks (over 14,000) - Banks are involved as providers of EFT by offering automated teller machine (ATM) and telephone bill paying (TBP) services. Banks also participate in automated clearing houses (ACH), point-of-sale (POS) systems, and wire transfers.

Saving and Loan Associations (over 4,000) - S&Ls were in the forefront of EFT development as they tried to use EFT services to gain a competitive advantage on banks. They implemented consumer EFT services such as ATM, POS, and TBP.

Mutual Savings Banks (almost 500) - Many MSBs were less involved with EFT at the outset since they were pioneering NOW Accounts. Today they are involved, like S&Ls, in consumer EFT services.

Credit Unions (over 24,000) - Some of the larger CUs were EFT innovators, like S&Ls, and concentrated on EFT consumer services.

Government Institutions

Federal Reserve - In addition to its regulatory role, the Federal Reserve was instrumental in organizing the first ACH. They have continued to provide leadership in developing standards for ACHs and protocols for interregional transfers.

U.S. Treasury - The Treasury has provided large transaction volumes to EFT by disbursing government funds with EFT. Treasury uses direct deposit of Social Security, military retirement, and SSI checks.

Regulators of Financial Institutions - Besides the Federal Reserve, there are four other major regulatory bodies: the Comptroller of the Currency, the Federal Deposit Insurance Corporation (FDIC), the Federal Home Loan Bank Board (FHLBB), and the National Credit Union Administration (NCUA). These regulators define the legal environment of EFT for federally-chartered institutions. State-chartered institutions often come under some federal control and are also regulated at the state level.

Business Institutions

Retail Stores - These stores are involved either by having ATMs on the premises or by installing POS terminals at check-out stands.

Employers - They participate in EFT by using direct deposit of payroll or by installing ATMs or POS terminals on premises as an employee benefit.

Exhibit 2-2

EFT Financial Services

Consumer-Oriented EFT Services

Services Which Facilitate the Transfer of Information

- Check and Credit Authorization
- Check Verification
- Check Guarantee
- File Look-up (Balance Inquiry)

EFT Services Which Involve Direct Money Transfer

- Deposit
- Cash Withdrawal
- Bill or Loan Payment
- Purchase
- Interaccount Transfer
- Debit with Overdraft Privileges
- Credit Purchase
- Cash Advance

Corporate-Oriented EFT Services

- Wire Transfers
- Direct Deposit of Payroll
- Preauthorized Debit Services
- Corporate Cash Management (including interbank and intrabank transfers)

Other Financial Transactions

- Transaction Records
- Account Transfers and Recording
- Check processing
- Credit Card or Loan Services

records or initiate transactions electronically. Another important service is provided by automated clearing houses. Two examples are direct deposit of payrolls and preauthorized debit services. Some may argue that these last two services are also consumer-oriented as depositing a payroll check in the bank is a service to the employee. However, the service originates from a centralized location, and is designed and marketed to large employers to save them the cost of writing innumerable payroll checks each pay period.

The third service group consists of those services used to electronically process other financial transactions. These may include recording counter transactions at teller terminals, account transfers, check processing and credit card or loan services. Although these transactions do not rely on the technologies generally considered as EFT (e.g., ATM, ACH), they do use electronic or computer technology and should not be overlooked in an analysis of EFT crime [Kutler, 2/4/81].

EFT Technologies

To develop a working framework for understanding EFT, it is essential to relate financial services to the principal EFT technologies used by financial institutions. The matrix in Exhibit 2-3 illustrates the links between the consumer and corporate categories of EFT-related financial services identified above and the five most prevalent EFT technologies: point-of-sale terminals (POS), automated teller machines (ATM), telephone banking systems, automated clearing houses (ACH), and wire transfer operations*. As these technologies have been described extensively in the literature this report provides a brief review of each along with a description of cash management services.

POS Technology

A POS system generally consists of four major components: computer terminals online to computerized customer information files, plastic transactions cards issued to all customers, a means to debit customers' accounts at the time of purchase, and a means to immediately credit merchants' accounts [Peat, Marwick, Mitchell & Co., 1977]. The three basic functions of POS are data capture, funds verification and payment authorization, and funds transfer [FDIC, 1976c]. Combining these functions allows a consumer

*Each of these technologies has major variations. By necessity we will describe generic types of EFT technologies, not specific variations.

Exhibit 2-3

EFT Financial Services Compared to EFT Technologies

Financial Services	EFT Technologies				
	POS	ATM	Telephone Banking	ACH	Wire Transfer Systems
Consumer-Oriented EFT Services					
EFT Services Which Facilitate the Transfer of Information					
• Check Authorization	X				
• Check Verification	X				
• Check Guarantee	X				
• File Look-up (Balance Inquiry)		X	X		
EFT Services Which Involve Direct Money Transfers					
• Deposit		X			
• Cash Withdrawal		X			
• Bill or Loan Payment			X		
• Purchase	X		X		
• Interaccount Transfer		X	X		
• Debit With Overdraft Privileges	X	X			
• Credit Purchase	X				
• Cash Advance		X			
Corporate-Oriented EFT Services					
• Wire Transfers					
• Direct Deposit of Payroll				X	
• Pre-authorized Debit Services				X	X
• Corporate Cash Management (Including interbank and intrabank wire transfers)				X	X
Other Financial Transactions					

to use a plastic magnetically-encoded card to make purchases. This is the idea of electronic banking or the cashless, checkless society that has been reflected in the literature.

As shown in Exhibit 2-3, POS is a consumer-oriented EFT technology. POS can provide all of the financial services under the consumer information category including check authorization, check verification, check guarantee, and file look-up. In addition, POS also provides services under the direct transfer category. In many places, however, POS terminals have been installed and transaction cards issued, but the system has not been used to actually make purchases. Rather, the use of POS systems has been limited to check authorizations and guarantees.* This is most often due to legal restrictions or the fear of nonacceptance by retailers and consumers. Because check authorizations and guarantees have advantages for both consumers and retailers, they are easily introduced POS applications. Later, once the check authorization and guarantee system has been up and running and acceptance is more widespread, it is possible to introduce debit transactions using POS technology.

One problem that has occurred with some POS systems is that the communications network between retail stores and a financial institution is limited. Often the system is limited to the computer records of one financial institution; that is, only customers who bank at the single participating institution can use the POS system installed in the store. This limits the attractiveness of POS systems to merchants. Now, many merchants are insisting before they enter into a POS agreement that the system must include as many financial institutions as possible. This requires financial institutions to work out an exchange system which switches transaction information to the appropriate financial institution. The specifics of operating switching systems are described in the literature [see for example, FDIC, 1976c]. The technology to do this has become available, but implementation has not occurred in many areas.

---

*VISA U.S.A is investing up to $10 million to install 130 IBM Series/I computers at its member locations for wide dissemination of POS check authorization and guarantee terminals. At no charge to the merchant, these processors (which can accomodate up to 130,000 terminals each) are envisioned as one answer to fraud and credit losses. They also provide a good incentive for merchants to try POS technology, in hope of more widespread acceptance [Trigaux, 7/8/81].

ATM Technology

ATMs are machines that permit customers to make a range of financial transactions, such as deposits, cash withdrawals, cash advances, account transfers, bill payments and account balance inquiries. ATMs can be either online or offline with the bank's main computer system. Access to the machine is regulated by the use of magnetically-encoded cards and a personal identification number (PIN).

ATMs may be either "free standing" or "through=-the-wall." Free-standing ATMs are placed away from the bank's physical plant. Common locations are retail stores, office complexes, and apartment buildings. Studies have shown that convenient access to ATMs from the home or office is more highly regarded by consumers than access near where they shop. Through-the-wall ATMs are physically part of the financial institution. However, they are situated where bank customers can use them after regular banking hours.

ATMs are the most popular form of consumer EFT. A survey of 35 financial institutions offering EFT services found that 70 percent of all EFT transactions were ATM transactions [Kutler, 11/18/80]. Part of the reason for this appeal can be seen in Exhibit 2-3. ATMs offer consumers a wide variety of banking services in a convenient way. Under the consumer information category, the technology provides file look-up--or balance inquiry--capabilities. In addition, under the direct money transfer category, ATMs can be programmed to allow consumers to make deposits, cash withdrawals, interaccount transfers, and cash advances, as well as to exercise overdraft privileges.

ATMs have had some problems in gaining acceptance. Frequent malfunctions decrease their usefulness to consumers and can hinder widespread acceptability. To counter this problem, and to reduce long lines at popular locations, some financial institutions have installed two or more ATMs at the same location. This response appears to be overcoming acceptance problems.

ATM systems need not be limited to a single financial institution. Many shared ATM networks have been organized in the last few years. This movement can be attributed in part to the high costs* of developing and marketing EFT

*The cost of an ATM varies significantly according to the type of system. Installation costs for a through-the-wall machine can be as high as $5,000, and as high as $15,000 for a more complicated free-standing unit. Other costs are

technologies such as ATMs that make it necessary for many financial institutions to share systems in order to reduce costs. Shared ATM networks are changing the nature of ATM use and will change the environment for ATM crimes. The growth and implications of this developing technology are discussed in Chapter 3.

Telephone Banking

Telephone banking technology basically requires a touch tone telephone and a bank computer. Information is entered by pushing the buttons on a telephone; the computer recognizes the different tones and thereby collects and processes the information. In less advanced systems, the consumer phones the financial institution and gives verbal instructions to an employee. Its most common application is telephone bill paying (TBP). This allows a customer to enter an account number, transaction information, and security codes to debit his account and credit a vendor's acccount. Not all TBP systems serve an unlimited number of vendors, however, so the customer may be required to list authorized vendors or accounts before making bill or loan payments.

TBP has been more readily accepted by consumers than merchants. There seems to be little appeal for merchants who must establish accounts at each bank offering the service and wait for notification by mail before they can draw against the deposits. Thus TBP and paper checks are equally rapid payment systems for the merchant--both are limited by the speed of mail. For customers, TBP seems to have been accepted by those who use it. It is more convenient than writing and mailing checks, and they are still able to retain information for tax and record purposes.

Other advancements in telephone banking are fast emerging. By adding two components to the system--a television set and an adapter--a customer can potentially perform many of the functions of an ATM at home. After connecting to a bank's computer, a customer can "dial-up" information for his account and display it on the television screen. Through signals entered with the telephone keys, the customer can make interaccount fund transfers, pay bills or loans, and verify account balances. An experimental version of this technology has recently been tested by a large Ohio

$15,000 for the software, and between $17,000 and $50,000 for the hardware (i.e., the ATM terminal). So, for example, if a bank installed two free-standing ATMs, the costs for installation, software and hardware would range from $79,000 to $149,000 [Peat, Marwick, Mitchell & Co., 1977].

bank [Bank One, 1981], and several other pilot projects have begun across the country. Another home banking service foreseen is online access to trust accounts that would provide an account snoypsis including the current value of holdings and information on dividend and interest payments [Tyson, 4/1/82].

Future telephone banking applications are envisioned that would allow merchants to advertise on cable television networks, and allow prospective customers to interactively make direct purchases through bank or coaxial cable television switches. One cable firm, Cox Cable Communication, Inc., is currently conducting a "shop at home" telephone banking experiment in San Diego. Five financial institutions and 500 households are participating. The number of users is expected to approach 1,000 by early 1982, while two additional systems are scheduled for startup in Omaha and New Orleans. Customer acceptance of the system has not yet been determined [Kutler, 3/2/81].

In anticipation of telephone banking advancements, American Telephone & Telegraph (AT&T) has announced technical standards for equipment using telephone lines that is marketed for home information systems. This is an attempt to standardize the emerging technology in hopes of creating widespread interoperability among products. The standards may inevitably be a setback for those systems which differ, but should ease consumer acceptance of the currently decentralized industry [Trigaux, 5/28/81]. The recent AT&T settlement allowing the divestiture of local telephone companies and expansion into new services is expected to result in its move towards home banking and teleshopping, possible in conjunction with nonbank financial firms such as American Express, Sears, and Prudential/Bache [American Banker, 6/15/82].

ACH Technology

An ACH performs services similar to those provided by a manual check processing system. That is, an ACH gathers transaction data from various institutions, sorts it by receiving institution, and then sends the information on to the receiving institutions. The ACH performs these functions electronically (i.e., on magnetic tape), rather than manually. This allows the clearing process to be done at computer, rather then human, speeds. ACHs process both debit and credit entries. As shown in Exhibit 2-3, ACHs usually provide services such as the direct deposit of payrolls and Social Security payments, and preauthorized debit and bill payments. These services are generally centralized

institution-oriented services, although consumers may often be recipients of ACH transactions.

Originally ACHs were regional entities belonging to a group of banks within an area such as Atlanta, San Francisco, or Detroit. Each system developed its own sets of procedure and computer software, making it very difficult to trade information between regional ACHs. Recent national efforts, however, are facilitating interregional exchange of ACH data. The National Automated Clearing House Association (NACHA) now serves as the parent organization for ACHs, and the Federal Reserve Communications Network links over 35 regional ACHs, providing a fast, nationwide clearing mechanism [Greguras, 1980].

Wire Transfers

The tape-based ACH procedures described above are elementary compared to the paperless funds transfer arrangements that are now technically possible, such as high-speed wire transfers between ACHs or between banks within an ACH [FDIC, 1976a]. Wire transfer networks in the U.S., especially Bank Wire II and Fed Wire, have been in operation for many decades. Their primary purpose is to transfer large value transactions between financial institutions and businesses. These networks are virtually unknown to the consumer and small retail customers of a bank. Billions of dollars are transferred each day, and the prominence of these systems is growing.

Four networks dominate wire transfer operations. Two are long established. Bank Wire II is a private, bank-owned system which provides a computerized money and message transfer system. Established in 1950 on leased telegraph circuits, Bank Wire II now has the capacity to support 400 members and 60,000 messages per day. It provides a complete system for debit and credit transfers between correspondent accounts [Baker, 1980]. Fed Wire, operated by the Federal Reserve System, is designed to electronically transfer funds, securities information, and administrative messages. The Fed has had some form of electronic or telegraphic message system since 1918, when it installed a private Morse code system. The present fully automated system has been in operation since 1973. Until recently, Fed Wire was limited to the 12 Federal Reserve Banks, their branches, and commercial banks which were members of the Federal Reserve. However, on January 1, 1981, Fed Wire was opened to all financial institutions on a fee basis. Parties to a transfer on Bank Wire II can no have same day settlement capability through Fed Wire.

Two other networks are gaining prominence. The Clearing House Interbank Payments System (CHIPS) began as a simple, automated replacement of the New York Clearing House Association's physical procedures for interbank checking account payments. Since 1970, when it connected nine New York banks, CHIPS has expanded to 80 members including domestic and foreign institutions outside the New York area. It is now the dominant system for international banking transactions. The Society for Worldwide Interbank Financial Telecommunications (SWIFT) began in 1973 as an international interbank payment system using dedicated communication lines leased from postal and telephone authorities. SWIFT has expanded its unique message standardization procedures to accommodate 900 members in 39 nations.

Cash Management Services

Cash management services are automated linkages between businesses, banks, and wire services. To initiate a wire transfer, a business may instruct the bank by telephone, written instruction, or electronic transmission. Banks similarly instruct the transfer networks. At present, the telex network is the predominant electronic linkage [Greguras, 1982]. However, with the proliferation of microcomputers, many large banks are offering computer-based access to account records. BankLink (a service of Chemical Bank), for example, is a dominant computer network for cash management and information systems, and consists of 50 member banks [American Banker, 4/21/82].

2.3 AN EXPANDED DEFINITION OF EFT

As defined earlier, EFT may be thought of as payment systems which permit transactions to be made where the exchange of value or money is represented by electronic messages. These systems may also include the exchange of information which facilitates the exchange of value. Conventionally, EFT has been identified in terms of specific technologies and applications. Automated teller machines, point-of-sale terminals, and telephone bill paying, are generally considered to comprise consumer EFT technologies; automated clearing houses, wire transfers, and cash management services are typically considered to comprise corporate EFT technologies.

This report, however, employs an expanded approach to identifying EFT that is less application specific. Computers are now firmly entrenched in the processing of virtually all financial transactions. For example, a check originates on paper, but its information is entered into a computer system

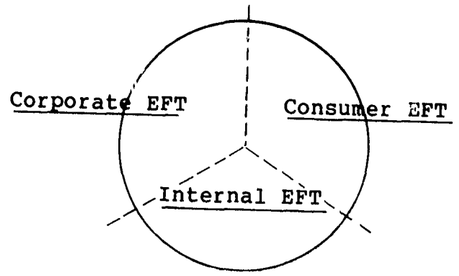
and the transfer of money to or from an account occurs electronically. Although to some, only those technologies that utilize electronic banking outside a financial institution's internal environment--such as the corporate and consumer EFT technologies listed above--are accepted as EFT, a literal interpretation of "electronic funds transfer" also describes the computerized processing of checks, credit card purchases, and almost all of the transactions that occur in a financial institution.

An expanded definition of EFT would therefore include all internal computer activities in financial institutions where the transfer of money or other financial instruments is accomplished electronically, regardless of the particular technology used to initiate the transaction. This approach is advantageous because specific banking technologies are evolving and changing rapidly, and it can accommodate future technologies that have not yet been conceptualized and are not included under the conventional definition.

Thus, to avoid overlooking possible crimes, EFT will be used to refer to any exchange of money or value, whether made internally by a bank employee or externally by a customer, that is initiated or completed electronically. As shown in Exhibit 2-4 below, EFT technologies can be thought of as

Exhibit 2-4

Categories of EFT Technologies



falling into one of three overlapping categories: consumer, corporate or internal EFT. Throughout this report, consumer EFT will refer to ATM, POS, TBP, home banking and other technologies that are used by individuals to make personal financial transactions. Corporate EFT will refer to ACH, wire transfer, cash management services and other computer communications technologies that are used by firms or other

organizations to carry out financial transactions and monitor financial information. Internal EFT will refer to the computerized processing of financial transactions within a financial institution.

3 THE STATE-OF-THE-ART FOR EFT TECHNOLOGIES AND SERVICES

To understand the potential relationships between EFT systems and criminal activity, it is important to recognize the current status and anticipated growth of EFT technologies and services. Obviously, as larger dollar volumes flow through EFT systems, they will become a more lucrative target for perpetrators. And, as the volume of transactions rises, and user knowledge increases, more opportunities for criminal abuse may occur. Thus, this chapter examines the state-of-the-art for consumer and corporate EFT. Looking first at the present in order to provide a baseline for future comparison, we review the number of EFT terminals and dollar and transaction volumes in the United States. We then try to identify future trends. Finally, this chapter concludes with a look at the crime-related implications of EFT use patterns.

The present baseline is drawn from a wide range of sources and on occasion some of the numbers may conflict. In considering the future, we have been able to find only one source, an unpublished report by Electronic Banking, Inc. (EBI). The data for both the baseline and future projections are summarized in Exhibits 3-1 through 3-5; Exhibit 3-1 reviews currency, check, and credit card transactions, and Exhibits 3-2 through 3-5 cover specific EFT technologies. (The sources for Exhibits 3-1 through 3-5 are listed together in Exhibit 3-6.)

3.1 THE BASELINE FOR CURRENCY, CHECKS, AND CREDIT CARDS

Exhibit 3-1 provides a baseline for currency, checks and credit cards, with the data varying in vintage from 1978 to 1980. Coin and currency are the nation's official money, and they remain a significant form of consumer payment for small transactions at the large majority of convenience retail stores (e.g., supermarkets, gas stations, and restaurants). The average level of cash in circulation in 1980 was $118.5 billion.

The bulk of the nation's money supply, though, is in the form of demand deposits--checking and NOW accounts--at commercial banks and a growing number of S&Ls and mutual savings banks. In 1978 it was estimated that over 90 percent of U.S. adults used the services of a financial institution, and about 90 percent of the users kept a checking account. Thus, about 80 percent of the U.S. population had checking accounts [Payments Systems, Inc., 1978]. In 1979, 15.1

Exhibit 3-1

Currency, Check, and Credit Card Transactions

	Year (Remarks)	Number Of Transactions	Yearly Dollar Volume
Currency	1980		$118.5 billion [14]
Checks	1979 (Fed Reserve clearing system only)	15.1 billion [16]	$ 8.5 trillion [14] *
	1980 (All checks)	34 billion [18]	$ 19 trillion [18]
Credit Cards	1977	**	$ 115 billion [14]
	1980 (Bank Cards Only)	1257 million [18]	$ 49 billion [18]

*The total number of dollars in checking accounts in 1979 was $265.4 billion [Federal Reserve Bulletin, February 1980]. The $8.5 trillion figure represents the total number of checks written during the year, or in other words, the $265.4 billion base times the number of times the base is turned over.

**Although we could find no estimates on the number of transactions, 62% of all U.S. adults hold at least one credit card, and the average household possesses 4.5 cards [A.J. Wood Research Corp., 1978].

billion checks worth $8.5 trillion were cleared through the Federal Reserve system. However, although it has been assumed that check volume was growing at a healthy annual increment of 7 percent,* a recent study by the Federal Reserve Bank of Atlanta estimated that the total number of checks processed in 1979 was 32 billion--20 percent less than many bankers assumed the volume to be. According to this estimate, the current rate of check growth is around 5 percent, and will drop to 4 percent in the early 1980's; to 2 percent by the mid-1980's; and by 1989 or 1990 the number of checks will level off. With the gradual leveling off of check volume, the study reasoned that the difference will be made up by electronic payment methods [Kutler, 2/6/81].

The remaining means for nonEFT payments is credit cards. A 1978 study estimated that 475 million credit cards were held by the U.S. adult population and that 62 percent of U.S. adults hold at least one credit card [Payment Systems, Inc., 1978]. Overall, credit card sales volume was estimated at $115 billion for 1977, and the figure has undoubtedly risen since then.

The implications of these numbers are important when considering the comparable potential for EFT consumer crime. Even though the 1978 numbers are out-of-date, they provide a useful comparison. When the dollar volumes for nonEFT transactions in 1979 ($118.5 billion in currency, $265 billion in demand deposits with $7.4 trillion in transactions and $115 billion in credit card sales**) are compared to the 1978 total for consumer EFT (ATMs, POS and TBP) of no more than $1 billion [Kevin, 1980a], it is easy to see that EFT has not yet become a major part of our economy on the consumer level. It undoubtedly will become increasingly important in the future, but for the time being it must be kept in perspective.

3.2 THE BASELINE FOR EFT TECHNOLOGIES

Although EFT financial transactions have not acquired the magnitude or dollar volumes of other financial transactions, they have become significant, especially in localized markets. Estimates of the present and projected use of POS, ATM, TBP, ACH, and wire transfer services are outlined in at Exhibits 3-2 through 3-5. The first column of

---

*This estimate is based on a 1970 study by Arthur D. Little, Inc. [Arthur D. Little, 1975].

**Credit card sales data are for 1977.

each exhibit provides the baseline for each of the technologies. When the numbers for a particular technology seemed to vary, we provided high and low estimates.

Estimates of point-of-sale use vary widely. As shown in Exhibit 3-2, one source estimated there were 13,000 POS terminals in 1977 with approximately 10 million transactions completed per month in the United States. However, this estimate included check guarantees and verifications as well as actual debit purchases. A lower estimate indicated 8,500 terminals and about 9 million transactions per month. A definitional problem is inherent in estimates of POS use however, because sources differ in how they count terminals. Some include check guarantee terminals along with POS debit terminals, while others do not--and, in essence count terminals by the function they perform instead of the technology. This also explains why it is difficult to get a dollar volume for POS terminals because much of the total is accounted for by check guarantees and authorizations, and not by actual electronic debits.

The data for automated teller machines is shown in Exhibit 3-3. The increase in installed ATMs in recent years has been almost exponential. In 1978 the number of ATMs was estimated at 9,750; by 1980 the estimate had risen to 17,000 machines, and to 25,000 in 1981. In 1979, 4,680 ATMs were shipped by manufacturers to financial institutions [Zimmer and Trotter, 11/19/80; ARCB, 1982]. The average number of transactions per ATM in 1978 was estimated to be between 3,760 and 4,000 monthly. This translates into between 36 million and 39 million monthly transactions nationwide, a much higher rate than that for other forms of EFT, consistent with consumer accepance of ATMs. Once again the almost exponential growth of ATM use is worth noting, with the number of monthly transactions between 1978 and 1980 rising from 39 million to 102 million.

However, the number of monthly ATM transactions includes balance inquiries as well as deposits and withdrawals. A recent study [Zimmer and Trotter, 1980] helps clear up some of the confusion. A survey of 109 banks found that 51.1 percent of all transactions were checking withdrawals, 20.4 percent balance inquiries, 11.9 percent checking deposits, 7.7 percent savings withdrawals, 2.8 percent account transfers, 2.3 percent credit card withdrawals, and 2.8 percent other transactions. Thus, four out of every five ATM transactions are financial transactions, while one out of five is a balance inquiry. Even if the 102 million transactions in 1980 are discounted for balance inquiries, the number of transactions per month would be over 80 million--making ATMs the most used form of consumer EFT.

Exhibit 3-2

Point-of-Sale (POS) Terminals

	Year		
	1977	1985	1995
High Estimates*			
Number of Terminals**	13,000 [5]	Available in 20% of SMSAs [8]	Available in 40% of SMSAs [8]
Number of Monthly Transactions	10 million [5]	35% of total transactions where available [8]	50% of total transactions where available [8]
Low Estimates*			
Number of Terminals**	8,500 [6]	Available in 10% of SMSAs [8]	Available in 15% of SMSAs [8]
Number of Monthly Transactions	9 million [6]	10% of total transactions where available [8]	25% of total transactions where available [8]

*EBI in their projections of future EFT growth made three projections: high, medium, and low, depending on the environmental factors that could occur. To provide the reader with a range of possible futures, this report focuses on the high and low projections.

**POS terminals are hard to number because some sources include check guarantee terminals while others do not. This makes comparison of numbers of different sources impossible.

Exhibit 3-3

Automated Teller Machines (ATMs)

	Year			
	1978	1980	1985	1995
High				
Number of ATMs	9,750[8]	17,000[11]	40,000[7]	50,000[7]
Average Number of Monthly Transactions Per Terminal*	4,000[8]	6,056[11]	10,000[7]	15,000[7]
Number of Monthly Transactions**	39 million	102 million	400 million	750 million
Low				
Number of ATMs			18,000[7]	25,000[7]
Average Number of Monthly Transactions Per Terminal*	3,760[9]		5,000[7]	8,000[7]
Number of Monthly Transactions**	36.7 million		90 million	200 million

*The average number of monthly transactions per terminal is confused by whether the total includes balance inquiries. In Zimmer's latest research she estimates 20.4% of all transactions are balance inquiries. [Zimmer and Trotter, November 19, 1980].

**Calculation based on the number of ATMs and the number of monthly transactions per terminal.

One aspect of ATM growth deserves special attention. Many shared ATM networks have been organized in the last few years. As discussed earlier, shared ATM networks allow financial institutions to lower the costs of providing ATM services. At a small scale, shared ATM networks allow small financial institutions to join the EFT movement. But much of the impetus for shared ATM networks comes from large financial institutions. Although recently proposed nationwide shared ATM networks such as Cirrus and the Regional Interchange Network, and Plus Systems offer the potential for increased economies of scale, they also set the stage for interstate banking [Triguax and Arvan, 2/11/82; Trigaux, 4/8/82]. Many of the trends and issues emerging from the shared ATM movement may be applicable to other EFT technologies as they grow in significance.

Discussion of this trend has been made more difficult by confusion over what to name the new sharing arrangements. At a conference on ATMs, Linda Fenner Zimmer, who has conducted numerous studies on ATM use, suggested a terminology for shared ATM networks which could be applied to all shared EFT systems [American Banker, 11/26/80]. Zimmer identified five forms of sharing arrangements:

- **Interchange** - two financial institutions, each owning an EFT system, permit the other's customers to access its machines;
- **Sharing** - EFT equipment is owned jointly by two or more financial institutions, in most cases an independent organization is formed to operate and coordinate the system;
- **Piggyback** - a financial institution with an EFT systems allows the customers of another without EFT to access its system;
- **Cooperative program** - any EFT program in which two or more financial institutions participate; and
- **Hybrid program** - any combination of interchange, sharing, and piggyback agreements.

Although the shared ATM movement is in a preliminary stage there were already more than 100 cooperative ATM or other EFT programs nationwide by 1980 ["A.O. Smith...," American Banker, 11/26/80]. Almost all of these existing cooperative programs are regionally organized, with nineteen large enough to require multiple data processing centers. Many of the regional systems are currently developing protocols for interregional switching of information, which

should assist in developing national EFT networks. More recently, several large banks have organized national ATM networks, although none is in operation at this time ["Technology Topics," American Banker, 2/3/82].

At least two factors could complicate continued expansion of shared ATM networks. One is the antitrust implications of cooperative ATM or other EFT programs. The other is interstate banking prohibitions. Even while legislatures try to resolve this issues, ATM and other shared EFT networks continue to grow. For example, the use of ATMs for withdrawals only, not deposits, across state lines is expected to occur based on the opinions of bank counsel that a withdrawal is the functional equivalent of cashing a check--which, of course, is not prohibited under banking laws [Greguras, 1982].

ATM networks are expanding not only in geographic size, but also in terms of the range of services offered to customers. With the aid of national credit and debit card corporations (who are working with financial institutions to permit combined access to ATMs in order to establish their own national EFT networks [Kutler, 4/6/81; Trigaux, 4/5/82]), consumers will soon be able to transfer funds, in either a preauthorized or on-demand manner, between financial, money fund and brokerage accounts in the cash management or "active asset" system traditionally reserved for corporations. Two systems which facilitate these intrabank and interbank transfers are now being tested, and major brokerage and money fund firms are committed to participate. These systems will be activated by a debit card which combines the logo of the participating financial institution and the national firm. Customers will be required to make an initial investment of $1,500 to $20,000 [Gross, 4/28/81, 9/2/81].

The baseline data for the most widely used form of telephone banking--telephone bill paying--are presented in Exhibit 3-4. TBP was offered by 249 financial institutions in 1979, and there were 425,000 active accounts with an actual monthly volume of $2.1 million. These baseline projections show that the scope of telephone bill paying is much smaller than that for other consumer EFT technologies. This promises to change, though, as additional home banking services (as described in Chapter 2) become available and accepted. By the end of 1981, for example, 17 home banking experiments had been conducted. A recent study by Trans Data Corp. predicted that the number of home banking projects could exceed 60 by the end of 1982.

Exhibit 3-5 presents the automated clearing house baseline summary. In 1980 there were 38 ACHs processing 18.9

Exhibit 3-4

Telephone Bill Paying (TBP)*

	Year		
	1979	1985	1995
High			
Number of Financial Institutions	249[13]	2,975[7]	8,000[7]
Number of Active Accounts	425,000[13]	8.9 million[7]	3.2 million[7]
Total Monthly Dollar Amount	$2.1 million[13]	$62.5 million[7]	$258.3 million[7]
Low			
Number of Financial Institutions		535[7]	1,625[7]
Number of Active Accounts		909,500[7]	4.9 million[7]
Total Monthly Dollar Amount		$5 million[7]	$31.3 million[7]

*As the primary service provided by Telephone Banking

Exhibit 3-5

Automated Clearing Houses (ACHs)/Wire Transfers

	Year		
	1980	1985	1995
High			
Number of Clearing Houses	32	70% of government payments to individuals[8]	90% of government payments to individuals[8]
Number of Monthly Transactions*	19.4 million[18] (232.8 million annually)	20% of payroll checks on direct deposit[8]	50% of payroll checks on direct deposit[8]
Monthly Dollar Volume (1977)	$3.3 billion[18] ($39.6 billion annually)		
Low			
Number of Clearing Houses		40% of government payments to individuals[8]	50% of government payments to individuals[8]
Number of Monthly Transactions*		2% of payroll checks on direct deposit[8]	5% of payroll checks on direct deposit[8]
Monthly Dollar Volume			
Fed Wire			
Number of Monthly Transactions**	3.6 million[17] (43.2 million annually)		
Monthly Dollar Volume	$6.6 trillion[17] ($78.6 trillion annually)		
Bank Wire			
Number of Monthly Transactions	.6 million[4] (7.2 million annually)		
Monthly Dollar Volume	$800 billion[4] ($9.6 trillion annually)		

*In 1979 the number of monthly transactions was reported at 14 million [Kevin, 1979].

**The annual rate of increase in Fed Wire volume was in the 18-20% range from 1972 to 1979, but in the last 7 months of 1979 to the end of 1980 it skyrocketed to 27% [American Banker, 17 December 1980].

Exhibit 3-6

Sources for Exhibits 3-1 through 3-5

1. Federal Reserve Board, "The Payment System in the United States," Washington, D.C., 1979, pp. 1, 9.

2. Federal Reserve Board, "1978 PACS Expense Report," Washington, D.C., 1979, pp. 138, 146.

3. A.J. Wood Research Corporation, data in Bank Card, Aug. 1978, p.3.

4. Daniel Kevin, "EFT-Description and Partial Evaluation," paper written for the Office of Technology Assessment, Washington, D.C., 1980, pp. 36, 47.

5. Rosemary Butkovic, Remote Financial Terminals and Participating Financial Institutions in the U.S. (Brookfield, Ill.: author, 1977), p. 25.

6. Allen Lipis, "Cost of the Current U.S. Payments System," Magazine of Bank Administration, October 1978, p. 30.

7. Electronic Banking, Inc., "EFT: The Next Fifteen Years," study with restricted use, source document not available, 1980.

8. Linda Fenner Zimmer, "ATM Boom Ahead," Magazine of Bank Administration, May 1979, p. 33.

9. American Bankers Association, Payment Systems Planning Division, "Results of ATM Security Survey," Washington, D.C., 1978.

10. American Bankers Association, "Results of the 1978 National Operations and Automation Survey," Washington, D.C., 1978.

11. Linda Fenner Zimmer and James Trotter, "ATMs: A Strategic Assessment," American Banker, 19 November 1980, p. 9.

12. Recent study by the Federal Reserve Bank of Atlanta, cited in Jeffrey Kutler, "Check Volume Fails to Rise as Expected, Fed Study Finds," American Banker, 6 February 1981, pp. 1, 6.

Exhibit 3-6
(continued)

13. Electronic Banking, Inc., "Directory of Telephone Bill Payment Services as of December 31, 1979," Atlanta, 1979, p. 3.

14. Federal Reserve Bulletin, February 1981, pp. 110-114.

15. Jeffrey Kutler, "Bank President Urging Total ACH Overhaul--System Termed Unable to Cope With New Technology," American Banker, 9 February 1981.

16. Jeffrey Kutler, "ATMs Are By Far the Most Popular of All EFT Services," American Banker, 18 November 1980.

17. Federal Reserve Board, Annual Report, 1980 (Washington, D.C.: author, 1980).

18. Association of Reserve City Bankers (ARCB), Report on the Payments System (Washington, D.C.: author, 1982).

million transactions each month worth $10.8 billion. Although in 1980 the number of monthly ACH transactions was less than that for ATM transactions, the monthly dollar volume for ACH transactions ($3.3 billion) was far larger than the total monthly dollar amount of all consumer EFT services combined. This can be easily understood when an average ACH transaction is compared to an average consumer EFT transaction. On the one hand, an ACH transaction such as a direct deposit of payroll may be one of hundreds of payments and involve thousands of dollars. On the other hand, a consumer EFT transaction such as a checking account withdrawal from an ATM may average less than $50 [Zimmer and Trotter, 11/19/80].

Exhibit 3-5 also includes data from Fed Wire and Bank Wire, two of the wire transfer services that facilitate interbank transfers. As can be seen in the 1980 baseline, Fed Wire accounted for $78.6 trillion and Bank Wire for $9.6 trillion worth of interbank transfers. In addition, almost $37 trillion in transfers were made through CHIPS in 1981; annual growth in volume is expected to exceed 20 percent per year [Arthur D. Little, Inc., 1982]. When these figures are compared to the ACHs' annual transfers of $129 billion in 1980, it is clear that the ACH system has not achieved the same order of magnitude or importance as Fed Wire, Bank Wire, or CHIPS.*

As discussed earlier, ACHs and wire transfer networks, along with cash management services, are generally grouped as corporate EFT. In a recent paper Fred Greguras made an important observation concerning comparisons between consumer and corporate EFT:

> Although the volume of business-to-business transfers is presently much lower than the number of consumer EFT transactions, the total value transferred on such systems is dramatically greater than the aggregated value of consumer EFT transactions. Corporate EFT constitutes less than one percent of the total volume of EFT transactions, yet amounts to about 85 percent of the dollar value of all transactions. On a daily basis, some commercial banks reportedly routinely

---

*It should be noted that initial work is now underway to upgrade and integrate the Fed Wire and ACH networks (operated by the Federal Reserve). The new system will be called Federal Reserve Communications System for the 1980s or FRCS 80. Implementation began on a pilot basis in mid 1981; the full system should be operational sometime in 1982 [Kutler, 12/17/80].

transfer funds amounting to almost two times the value of their assets through the existing wire networks [Greguras, 1980].*

What is the result of these baseline projections? Undoubtedly, significant dollar amounts are being transferred through EFT--$3.3 billion monthly in the ACHs or $25 million annually in telephone bill paying, for example. However, when compared to nonEFT financial transactions, they are still only a small part of our total economy. This consideration leads us to think about the future.

3.3 WHERE WILL EFT BE IN 1985 AND 1995?

At the present time, quantitative projections are available for only two of the four EFT technologies, ATMs and TBP. Exhibit 3-3 presented both high and low estimates for ATMs in 1985 and 1995. These projections were made by Electronic Banking, Inc.** EBI estimated that by 1985 the number of ATMs could range from 18,000 to 40,000 with the number of monthly transactions ranging from 90 million to 400 million. As recent data have shown that the number of ATMs in 1980 almost equals the low estimate for 1985, it is quite possible that the high estimate could be achieved by 1985. In essence, we are looking to at least double the number of ATMs in the next five years, with the number of transactions increased by five or ten times. In looking even further, to 1995, the projected number of ATMs ranges from 25,000 to 50,000 and the number of transactions from 200 million to 750 million.

Consumer surveys of ATM users demonstrate that an ATM is considered a convenient and useful innovation. This

*The data sources in this report do not allow a direct comparison to those noted by Greguras (his figures were provided by the consultant George White). However, the data certainly agree with the overall premise that although corporate-oriented EFT services constitute only a small portion of all EFT transactions, they represent the major portion of dollars transferred through EFT.

**As EBI states in their report, "Forecasting is not a Science." Estimates are made by EBI, but in many cases they are not based on specific quantitative formulas, rather they are reasoned judgements. The time periods covered in the EBI report are 1980, 1985 and 1995, with "high", "medium" and "low" estimates provided for 1985 and 1995. This report lists only the high and low projections.

acceptance by consumers who have tried ATMs holds well for their future. The number of ATMs will undoubtedly grow in the future, responding to the demand of the marketplace.

Exhibit 3-4 presented TBP projections. The number of financial institutions offering TBP services in 1985 may range from a high of 2,975 to a low of 535. This represents at least a doubling of the number of institutions offering TBP. In terms of the total number of active accounts, estimates range widely from 909,000 to 8,925,000, and estimates for total monthly dollar amounts range from $5 million to $62.5 million. Since these ranges are so wide, it is hard to get a real feel for where we will actually be in 1985. The projections for 1995 are also diverse. The projected number of financial institutions ranges from 1,625 to 8,000, with the total monthly dollar amount ranging from $31.3 million to $258 million. The acceptance of telephone bill paying will depend greatly on the availability of the touchtone telephone and the cost of TBP transactions. The true convenience of telephone bill paying is the ease of entering the data directly into the computer. Working through a human operator does not save the financial institution much money.

EBI also predicted the market penetration of POS and ACH systems. These projections are not as definite as those for TBP and ATM systems. The EBI projections shown in Exhibits 3-2 and 3-5 outlined the possible acceptance of POS and ACH in our economy. At the most optimistic, POS systems would be in place in 40 percent of the SMSAs and account for half of the transactions in 1995. The least optimistic 1995 projection has POS in 15 percent of the SMSAs and accounting for only a quarter of the financial transactions. These projections tell us that EBI estimates that POS will become an important regional financial system in some parts of the country, but may not become a national system. ACHs already cover all major sections of the country. 1995 projections show major ACH involvement in government disbursement programs. However, ACH penetration of the private business sector will depend on how well ACHs meet business needs, especially in an era of rising postal costs.

3.4 CRIME-RELATED IMPLICATIONS OF EFT GROWTH

EFT is becoming a significant part of the economy. At present the number of EFT transactions as a percentage of all financial transactions is still relatively small, but people are becoming more aware of the techology and how it can serve them. However, increased familiarity with EFT technologies

has also focused greater attention on the possibility of criminal abuse. And, although EFT systems are still evolving, each of the technologies has a different crime potential.

POS growth is regionally concentrated. In these areas the debit card will become more popular over the next decade. The primary crime problems with POS are likely to be related to card security. Experience with credit cards should help; and criminal problems concerning debit cards are not expected to be any worse than the problems we now face with credit cards.

ATMs already cover the nation and are expanding. Consequently, a number of crime problems with ATMs have already occurred. In New York City several highly publicized muggings have brought ATM security to the forefront [American Banker, 8/17/79]. In addition, the development and expansion of shared ATM networks adds to the potential for crimes of all types. Although the number of ATM transactions is high and growing rapidly, and the number of people using ATMs is large, the amount of money involved in any transaction is small. This reduces the potential for large losses through ATMs. Further, the EFT Act (Regulation E or "Reg E") has already made some provision for consumer liability with ATMs. (A discussion of the major liability provisions of Regulation E is presented in Appendix A.)

TBP will also grow, but the crime potential appears to be smaller than with the other technologies. Security procedures can be written into the software. However, as TBP develops into more extensive home banking, access to the computers owned and operated by financial institutions will grow, increasing the risk of false data entry.

A possible mitigating factor underlying the potential ipact of criminal activity, at least in the consumer EFT area, are the dollar, volume, and payee limits imposed on transactions. In TBP systems, for example, customers may make payments only to a predetermined set of merchants. Similarly, a customer may usually withdraw no more than a few hundred dollars each day from an ATM. These limits may lessen some of the incentive for widespread criminal activity.

ACHs and wire transfer systems, however, cover the nation and the potential for corporate EFT crime is worrisome. The number of transactions is relatively low, but the number of dollars transferred is extremely large. The potential for large scale embezzlement and fraud exists and this portends potentially serious security problems. The

proliferation of microcomputers in offices will probably increase corporate dependence on electronic transactions. While the criminal problems for consumer EFT are likely to be characterized by a large number of small dollar crimes related to the theft of a debit card or ATM access card, corporate EFT crime will probably be characterized by a few cases of much larger dollar amounts.

4 A FRAMEWORK FOR THE ANALYSIS OF EFT CRIME

This chapter discusses the conceptual issues underlying any analysis or measurement of the relationship between EFT technologies and criminal activity. It begins with a definition of the term "EFT crime." The following section uses the definition to identify the types of criminal activity that can be considered EFT crimes. In the third section, a conceptual framework--or layered approach--is proposed that can be used to describe major categories of EFT crime. The concluding section of this chapter examines alternative "classification schemes" for relating criminal activities to EFT.

4.1 DEFINING EFT CRIME

Over the centuries, western society has reached general agreement on useful definitions of criminal conduct--fraud, larceny, embezzlement, bribery, and vandalism are examples. Legal definitions of crime can be applied to specific actions by legislatures, law enforcement authorities, and courts to determine guilt or innocence. Being purposefully broad, however, these same definitions can hinder the examination of specific types of criminal activity because only general behavior is monitored. Further, new technologies such as EFT may create opportunities for criminal activity which fall outside traditional legal definitions. For example, it is often difficult to apply theft, larceny, or fraud statutes when a bank employee uses a computer to make unauthorized deposits to an account because there was no "physical taking" of money or property. Thus, applying definitions to activities related to computers and crime is problematic.

With the great increase in computer use in this country, the potential for computer involvement in criminal activity has grown. Many legislatures are responding by defining more clearly the types of actions, often overlooked in traditional criminal statutes, related to computer use that should be considered criminal. For example, Senate Bill 240, which was introduced to Congress in 1979 by Senator Abraham Ribicoff (Appendix B contains the text of the bill), proposes four categories of criminal actions concerning computer abuse:

- theft, through the use of computer technology, of money, financial instruments, property, services or valuable data;

- unauthorized use of computer-related facilities;

- introduction of fradulent records or data into a computer system; and

- alteration or destruction of information or files.

Although SB 240 has not been adopted, 17 states have enacted computer crime statutes. Similar to the proposed federal provisions, most serve two functions. First, they define computer data and information as property, thus making them the subject of theft, larceny, fraud, embezzlement, and other related statutes. Second, most of the enacted statutes make unauthorized access, use, modification, alteration, or obstruction of a computer system, computer program, or computer resources a crime if it is accompanied by criminal intent. Despite these efforts, EFT systems or related crimes are seldom explicitly identified in computer crime laws To date there have been few indictments, much less convictions, under any of the state computer crime laws. In the absence of judicial experience with the laws it is difficult to predict how the courts might interpret these statutes in reference to EFT crime. (See Appendix C for a detailed discussion by Susan Nycum of the criminal law aspects of EFT and computer crime.)

In addition, no commonly accepted definition of the term "EFT crime" has emerged in the literature. Nonetheless, the ability to differentiate crimes that can be attributed to the presence or operation of an EFT system from others that occur in financial institutions is a prerequisite for analyzing the nature and extent of EFT crime. Ideally, a definition of EFT crime should act like a sieve--catching and identifying certain activities as EFT crimes while letting others slip through.

As EFT crime is a form of computer crime, existing definitions of computer crime illustrate the difficulties of developing a specific definition. Several definitions of computer crime are listed in Exhibit 4-1. A scan across these definitions reveals great diversity. In particular, there are large disparities in how the role of the computer in the crime is viewed. Taber, for example, defines the role of the computer narrowly, such that the computer must have been "directly and significantly instrumental" in the commission of the crime.* Carroll is slightly less restrictive, defining computer crime as any threat

*Taber, in fact, reviewed 375 cases in the SRI Computer Abuse File (see Chapter 5 for a discussion of this data source) and considered only 8 of the cases to be genuine computer crimes [Taber, 1981].

Exhibit 4-1

Definitions of Computer Crime

Computer crime is a crime that, in fact, occurred and in which a computer was directly and significantly instrumental [Taber, 1980].

Computer crime consists of all threats directed against electronic data processing equipment (EDP) and its supporting facilities (hardware), programs and operating systems (software), supplies, information handled by the EDP system, negotiable instruments stored or created at the facility, and critical resources required by the EDP system to render service [Carroll, 1977].

Computer fraud and abuse is the use or attempted use of a computer with the intent to execute a scheme or artifice to defraud; or to obtain property by false of fraudulent pretenses, representations, or promises; or to embezzle, steal, or knowlingly convert the property of another to an individuals use. The intentional and unauthorized damage of a computer also constitutes computer abuse [SB 240, 1979].

Data processing crime is any act which involves and is designed to cause loss or damage or in any way defraud the company or its customers through the use or manipulation of the data processing system [DeGouw, 1978].

Computer fraud is (1) defalcation, whereby computer processing is used to assist in the unauthorized obtaining of assets belonging to the company, or (2) misrepresentation, whereby computer processing is used to assist in the production of financial information which is not derived from authorized transactions, or (3) physical action, whereby, as a result of breach of security, data or programs are stolen or the computer equipment is attacked [Jenckins and Pinkney, 1978].

Computer fraud is a shorthand way of referring to computer-assisted or related crimes. The people who commit these crimes may use the computer either directly or as a vehicle for deliberate misrepresentation of deception, usually to cover up the embezzlement or theft of money, goods, services, or information [Krauss and MacGahan, 1979].

Computer crime can be defined as a crime which either directly or indirectly involves a computer system as a means or as a target in the perpetration of the crime [Schabeck, 1979].

Computer abuse is any intentional act in which one or more victims suffered, or could have suffered a loss and one or more perpetrators, made or could have made, gain. The incident must be associated with computer technology or its use. [Parker, 1975].

directed against the components, both physical and human, of a computer system. Other definitions, such as those proposed in SB 240 and by DeGouw, are more general and include any incident in which the computer was used to assist in committing a crime as a computer crime. Finally, the most general definitions, such as those put forward by Parker and Schabeck, define computer crime as any crime associated with computer technology or its use.

A range of alternatives can be used to define EFT crimes; there is no consensus on how narrowly or broadly the role of the computer should be considered in the context of computer or EFT crime. Although each alternative has its own merits and weaknesses, a broad definition is probably the most useful and applicable, since it is most likely to capture a full range of EFT crime incidents. Thus, any crime whether or not prosecuted under special computer/EFT laws or traditional law, that would not have occurred but for the presence of an EFT system is considered in this report to be an "EFT crime." Only by adopting such an inclusive definition can the impact of EFT technology on the incidence of crime be fully assessed. In the context of the analogy of the sieve, this definition would identify a larger pool of incidents as EFT crimes.

4.2 TYPES OF EFT CRIME

Given this definition, it is useful to look at a few examples of incidents which are considered EFT crimes. Before reviewing plausible incidents, however, we recognize that each EFT technology has unique characteristics: some criminal scenarios are more readily associated with certain EFT services, and system-specific environments may lend themselves to unique vulnerabilities. Thus, it is useful at the outset to distinguish among the three categories of technologies: consumer EFT, corporate EFT, and internal EFT. The frequency and loss can be expected to differ among these groups. For example, consumer EFT crimes have been reported more frequently, but have tended to involve small dollar amounts in each criminal instance, corporate and internal EFT crimes, although not as frequently reported, involve larger potential dollar losses. Also, the methodology employed in the crime tends to differ.* Consumer EFT crimes appear to predominantly involve direct withdrawal of funds from a single checking or savings account by a

*The methodology behind a crime is particularly important when apprehension and prosecution are considered. The careful and consistent identification of criminal

perpetrator using lost, stolen, or "borrowed" ATM cards. Corporate and internal EFT schemes, on the other hand, generally have been accomplished through manipulation of both commercial and consumer accounts by perpetrators posing as authorized transactors with the aid of authorization codes.

Consumer EFT

The tremendous number of ATMs and the relative ease of access have focused attention on in ATM crimes. Many of the criminal scenarios discussed here are also applicable to POS and TBP. The most common ATM crime occurs when a transaction card and personal identification number (PIN) are stolen. Typically, ATM cards are obtained by stealing wallets or pocketbooks. As many customers keep a written copy of their PIN with the card, access to the account is unblocked. Perpetrators may also steal the card and PIN from the customer's mailbox and make withdrawals before the theft is discovered.* Another source of ATM cards occurs after cards and PINs are mailed. A small number will inevitably be returned due to address problems. When corrupt employees have obtained these returned cards, they have used them to make unauthorized withdrawals.

Customers may also purposely fraud the bank by withdrawing more money than was actually held in their account. One source suggests that overdrafts at offline terminals accounted for the largest part of consumer fraud perpetrated against ATMs in 1976 [Zimmer, 1976].** And, it is possible that withdrawls disputed by a customer were actually made by a relative or roommate without the customer's consent, or even the customer who may try to take

methodology within the law (e.g., defining a transaction card or making distinctions between legal and illegal intent in account transfers) could greatly enhance successful prosecution of fraudulent activity.

*Banks generally mail PINS and cards separately, and spaced a week or so apart. If the customer is away on vacation, or mail is kept in a common area, the opportunity to obtain both the PIN and card exists.

**Online terminals are not subject to overdraft when they operate properly because the terminal has access to information on the customer's account. Strategies to prevent overdrafts at offline terminals include bad account lists, magnetic coding devices which record the customer's balance on a magnetic strip of the access card, and withdrawal limits.

advantage of EFT consumer protection laws. Finally, Citibank was recently a victim of a new, sophisticated type of customer abuse: at least 14 customers sold their ATM cards and PINs to six perpetrators. As the customers agreed to wait several weeks to report their cards as lost or stolen, the ring was able to cash $375,000 in stolen checks at the ATMs over a 10-month period ["Six Indicted..., American Banker, 4/19/82].

Another ATM-related crime is counterfeit. Customers have reported that unauthorized withdrawals were made but that the card had never left their possession. When the banks deny that employees are responsible and the customers deny that they are making withdrawals, one could conclude that someone is gaining ATM access by counterfeit cards. The ability to produce such counterfeit cards with only limited resources is quite possible and has been demonstrated in credit card fraud cases.

At least one example of a confidence scam has involved ATMs. In this instance, again involving Citibank, the perpetrator watched a customer enter his PIN and complete his transactions. The perpetrator, posing as a Citibank employee, then approached the customer, explained that the bank was experiencing malfunctions with the ATM and asked the customer to activate the machine by inserting his card. The perpetrator then thanked the customer for his assistance and waited for the customer to leave. As the machine was still activated, the perpetrator then entered the PIN and withdrew cash. The U.S. Attorney General has brought a group lawsuit against Citibank on the behalf of 125 customers swindled in this manner. However, it is highly unlikely that this scheme could be repeated elsewhere as it relied on Citibank's unique ATM hardware and software--a system in which the customer "dips" his card to activate the machine, but retains possession of the card throughout the transaction [Trigaux, 4/9/82].

Finally, ATMs and users are subject to physical attack. Because they contain cash, ATMs are vulnerable to vandalism and burglary by both crude and sophisticated means. Similarly, personal robbery is also possible because of ATMs. Customers have been assaulted while making withdrawals at night, or in some cases forced to reveal personal identification numbers while releasing their access cards.

ATM losses tend to be small. ATMs usually have dollar limits which are small in terms of the size of transactions which regularly take place in corporate EFT. Zimmer indicates that losses associated with cash dispensers and ATMs have consistently been less than $100 per incident. It

is possible, however, to incur large ATM losses if multiple transactions are made without detection. However, Reg E has limited the liability of the consumer and this helps to negate the ATM fraud, although banks must still absorb losses.

Corporate EFT

To commit corporate EFT crimes a certain amount of specialized knowledge of the EFT system is required. In the typical scenario, the perpetrator learns the number of an account with a large bank and the specific code number needed to authorize the transfer. Then the perpetrator, either through false identification or with the help of an employee in the wire room, initiates a transfer to an account at a bank in another city. Because large sums of money are transferred through these technologies, losses from a given incident can be extremely high. It should be mentioned that the ability to fraudulently authorize a transfer is not unique to EFT systems, but the speed with which the money is transferred, allowing withdrawal prior to validation at the initiating bank, makes this type of crime worrisome.

One potential corporate EFT crime, however, does not require sophisticated knowledge. Occasionally, a bank will inadvertently credit the wrong account in a wire transfer, or credit the same account twice. In most cases the customer returns the funds. However, sometimes the recipient of the miscredit or double credit will abscond with the money, committing a crime in the process.

Internal EFT

Crimes committed with internal EFT technologies tend to involve a bank employee with computer access. The employee finds an account with a large balance and then transfers some funds to his or her own account and makes a withdrawal. In more complicated schemes, someone with substantial computer knowledge, typically a programmer with extensive applications knowledge, modifies an existing program. For example, small amounts are "shaved" from hundreds of accounts, deposited in a special account, and the books remain balanced. This is done automatically by the computer, so the programmer does not have to initiate any transfers himself. Unlike corporate and consumer EFT crimes that often involve only one transaction, internal EFT crimes often involve several transactions over a period of many months [Allen, 1981].

Another type of crime, blackmail, is possible with internal EFT technologies but is highly unlikely in the corporate or consumer EFT categories. For example, detailed

information on customer transactions (e.g., transfers between customers' accounts) could provide a watchful user with the evidence, or the ability to create false evidence, required for acts of blackmail or bribery. Here again, the information is not unique to EFT systems, but the increased potential for remote and covert unauthorized access to account files that the computer provides makes the crime an EFT-related one.

4.3 A LAYERED APPROACH TO EFT CRIME

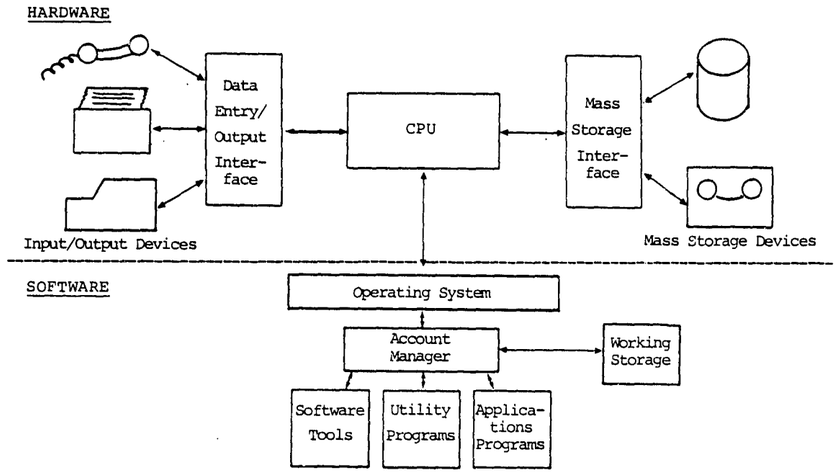
The wide variety of technologies and methodologies involved in the above examples illustrate the difficulty of trying to describe EFT crime: which attributes of EFT crimes should a definition or classification scheme emphasize? For example, a definition could be based upon the modus operandi used to commit a crime. Alternatively, EFT crimes could be categorized by traditional classes of crime such as robbery, embezzlement, or sabotage.

In understanding EFT crimes it is helpful to examine the manner in which the EFT system is structured. Exhibit 4-2 illustrates one approach to viewing the physical and human components of an EFT system. The core of any EFT system is the hardware that allows transactions to be initiated, completed, and recorded. It includes the computer itself (the CPU, or central processing unit) as well as interfaces with mass storage devices and input/output devices. The input/output devices include the terminals used by customers and employees to initiate EFT transactions, such as ATM and POS terminals, telephones, or terminals for entering wire transfer requests. The next component of the EFT system is the software that "tells" the computer how to process transactions. (Exhibits 4-3 and 4-4 are detailed lists of the devices and functions that constitute EFT hardware and software.) The third component is the internal procedures followed by a financial institution in the day to day operation of the EFT system. These internal procedures include both the use of internal EFT by employees (e.g., a teller enters an over-the-counter deposit into a terminal), as well as support activities for corporate EFT and consumer EFT. The final component of the EFT system is the external procedures followed by customers when they use EFT technologies such as ATM machines, POS terminals, and wire transfer telephone requests.

A natural progression of layers of EFT components from the hardware core outward to the use of EFT facilities by customers can be envisioned. These layers of EFT components

Exhibit 4-2

EFT Components



INTERNAL PROCEDURES

- Enter counter transactions
- Set EFT account requirements
- Authorize unusual EFT transactions
- Verify EFT transactions
- Authorize access to EFT records
- Prepare customer EFT statements
- Prepare internal EFT activity reports
- Train employees in EFT use
- Produce plastic cards
- Distribute plastic cards
- Generate PINs and passwords
- Limit access to computer facilities
- Enter wire transfer requests
- Design physical security for EFT facilities

EXTERNAL PROCEDURES

- Use EFT facilities
- Protect plastic cards from theft or loss
  Report loss or theft of plastic card
- Maintain secrecy of PIN/password
- Prohibit unauthorized use of EFT account/facilities

Exhibit 4-3

EFT Hardware Description

Mainframe

The heart of a computer system is the mainframe. It is comprised of one or more cabinets of electronics located in a computer center or computer room. The mainframe usually, but not always, includes these components:

- Central Processing Unit (CPU). Coordinates operation of entire computer system. The CPU runs programs, performs calculations, manipulates data.
- Peripheral Interfaces. These circuits allow the CPU to read and write information to and from data input/output devices.
- Mass Storage Device Interfaces. These circuits allow the CPU to communicate with high-volume storage units such as disk and magnetic tape drives.
- Working Storage. This category includes the high-speed random-access memory used by the computer to store programs which are currently being executed and data which is currently being manipulated. There are two important types:
  - —Core Memory: non-volatile electromagnetic circuits
  - —Semiconductor Memory: volatile electronic circuits

Data Input/Output Devices

This cateogry includes devices which facilitate communication between the computer hardware and programs and the computer users.

- Video Terminals
- Magnetic Card Readers
- Paper Tape Readers
- Printer Terminals
- Punched Card Readers
- Communication Lines
- Dedicated Terminals (e.g., ATMs)

Mass Storage Devices

Included in this category are devices used by the computer to store programs and data in machine-readable format.

- Hard-Disk Drives: high speed, random access
- Flexible-Disk Drives: medium speed, random access
- Magnetic Tape Drives: low speed, mainly sequential access

Mass Storage Media

Included here are the media which the computer uses to store information.

- Disk Packs
- Flexible Diskettes
- Magnetic Tape

Exhibit 4-4

EFT Software Description

Operating System

This is the most important program run by the computer. It instructs the CPU to allocate resources (processing time, memory space, etc.) according to demand. Other programs operate through the operating system to communicate with input/output and mass storage devices such as terminals, disks, printers, and so forth.

Account Manager

This program usually oversees all other jobs being run by the computer. It controls users' access to programs and data according to a defined priority scheme. It also maintains a record of the amount of CPU processing time, disk space, and other resources used.

Software Tools

This category includes programs which translate high-level job descriptions into machine-executable form. The final product of the software tools is a working program, such as an application or utility program (see description below). Examples are:

- Language Translators: FORTRAN, COBOL, RPG, etc.
- Debugging Tools

Applications Programs

These programs process data and generate reports. They communicate with input/output devices and mass storage files through the account manager and the operating system. Applications programs usually require the largest percentage of computer resources, and they are the most important as far as users are concerned. Examples are:

- Demand-Deposit Accounts Program
- Payroll Program
- Interest Calculating Program
- Communications Program

Utility Programs

These programs accomplish commonly needed "housekeeping" functions such as file copying, error correction, and so on. Once again, they operate through the account manager and the operating system to access terminals and files. Examples are:

- File Copy Utility
- Working-Storage Diagnostic
- File Repair Utility
- Disk Diagnostic

then constitute one dimension that can be used to classify EFT crimes on a "first cut" basis. Just as definitions of computer crime adopt different levels for the role of the computer, each layered EFT component adds a new level for the role of the EFT system in the crime. The definition of EFT crime, then, may be refined and conceptualized as a layered definition. Each successive layer of the definition broadens the range of incidents identified as EFT crime. The layers of the definition are the components which comprise the EFT environment within a financial institution. As described above, the EFT environment can be broken down into four interrelated components: hardware, software, internal procedures, and external procedures. (Of course, it is recognized that the distinctions between these layers are somewhat artificial and that a particular crime may actually fit in more than one category. Nonetheless, we feel this is a useful classification system for describing EFT crimes, at least on a broad level. In the future, it may be useful to design a hierarchical classification system based on these categories.)

Given this approach, the most restrictive category of EFT crime consists of those incidents which rely on the presence of EFT hardware. Hardware includes the physical components of the computer system that are necessary to make, verify, record, or report a financial transaction. Remote and dedicated terminals, communications links, input/output interfaces, central processing units (CPU), mass storage interfaces, mass storage devices, and stored data all comprise hardware. Potential EFT hardware crimes include the tapping of communications links to create, alter, or destroy data and transactions requests, or the use of EFT data and records to defraud a financial institution. A reported example of an EFT crime that may fall within the hardware category was a $900,000 wire transfer fraud involving two U.S. banks and two banks near the border of Italy and Switzerland. The perpetrators monitored wire transfers from the U.S. banks to one of the European banks. When a large amount had accumulated, the perpetrators inserted instructions, via the communications systems, to transfer the balance to an account in the second European bank. One U.S. bank discovered the wiretap in a routine inspection and notified the authorities [Krauss and MacGahan, 1979].

The second layer consists of crimes utilizing EFT or computer software. EFT software includes the applications programs required to make a financial transaction at a terminal or other communications device; to verify, record, or report a transaction; and to maintain an account. Operating systems instructions, utility programs, and software tools used for all applications programs are also

defined as software. Potential EFT software crimes include altering or creating an applications program to initiate or hide fraudulent transactions. One reported EFT software crime involved internal EFT. The head of computer operations for a bank set up a fake account which he controlled. He then changed the recording software so that it would automatically transfer money to the fake account. It was also reprogrammed to make up the differences and balance the daily accounts [SRI File Number 70311, 1977].

The third layer consists of EFT crimes that relied on or compromised the internal EFT procedures of a financial institution. EFT procedures are those activities carried out by a bank in support of its EFT hardware and software systems. Producing plastic cards for ATM and POS terminals, creating and entering punched tape to make wire transfer and ACH transations, preparing the EFT portions of a customer's monthly statment, and filing Regulation E reports are all examples of EFT procedures. Potential EFT internal procedures-based crimes include the theft, duplication, or unauthorized creation of plastic cards and PINS, verification of empty envelope deposits, entering fraudulent wire transfer requests, or stealing cash intended to replenish an ATM vault. As an example, a chief teller embezzled $1.5 million over three years by relying on his teller's terminal and access to cash. He applied various methods, including account transfers, adjustments, and failure to enter transactions [Krauss and MacGahan, 1979].

The fourth layer of EFT crimes are those committed through access as a user, whether authorized or unauthorized. These are external procedures-based crimes. EFT use is the process of gaining access to the EFT system--via a plastic card and PIN, online or telephone password, or signature (for wire transfer requests)--to make a transaction. Potential EFT external procedures-based crimes include using a stolen or black market plastic card and PIN to make transactions, making an intentional empty envelope deposit to withdraw money, or directing the bank to make an illegitimate wire transfer. In one reported example, the perpetrator opened at ATM account and gave his card to another who traveled frequently to the area. The second perpetrator then made a large empty envelope deposit to the first's ATM account. As the ATM immediately credited the account,the second was then able to drive to over 20 ATMs in the area and made the maximum withdrawal at each [SRI File Number 77329, 1977].

The final, and least restrictive, layer is EFT-related or environment-based crimes. These are crimes that would not have occurred without the presence of EFT technology but that cannot be readily attributed to EFT hardware, software,

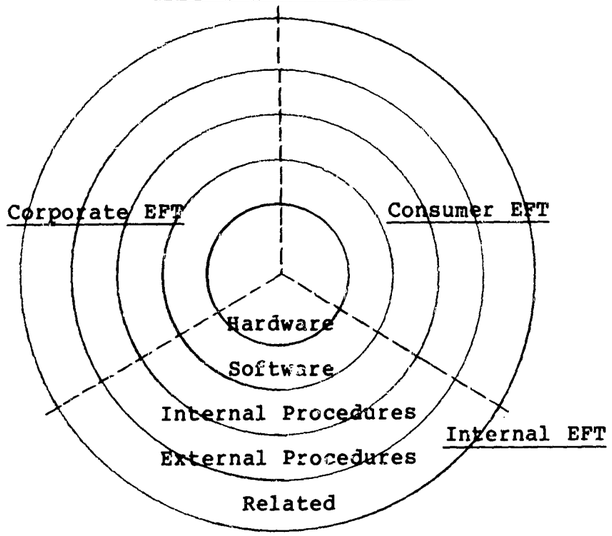
internal procedures, or use. Potential related crimes include mugging a user after an ATM withdrawal or selling POS cards on the black market. As an example, a Boston bank's ATM was torn from the wall and money stolen from its vault.

4.4 A CLASSIFICATION FRAMEWORK FOR EFT CRIME

The concept of a layered definition of EFT crime can be combined with the three categories of EFT technologies (i.e., consumer, corporate, and internal) discussed earlier to form the backbone of a classification framework for EFT crimes. Exhibit 4-5, below, illustrates the combination of EFT categories and components, and its relationship to a layered definition of EFT crime:

Exhibit 4-5

Layers of EFT Crime



Once the pool of EFT crimes has been identified by definition and categorized into the broad classes outlined in this conceptual framework, it is useful to consider additional dimensions that could be used to describe the nature and extent of EFT crime. In the realm of crime classification, two general types of schemes are commonly used: legal classifications and problem-solution

classifications. Unfortunately, only the former is in general use today. The application of both schemes to the study of EFT crime is discussed below.

Legal Classifications

Legal classifications are based on a traditional or legal definition of the crime such as burglary, embezzlement, or fraud. These definitions serve to identify suitable punishment or retribution for the commission of the crime. A change in the number of reported crimes within a given legal classification may also indicate a change in criminal activity or law enforcement, thus outlining needs for the criminal justice field. EFT crimes can be categorized by these legal defintions. Although it is difficult and somewhat awkward to force EFT crime into a classification system which was established long before the various methods of perpetration were conceived, such a classification scheme offers an important means of comparing the risks associated with EFT to the risks associated with a paper-based financial payments system.

The FBI Uniform Crime Reports is the central repository for reported crimes which are classified in terms of a legal, retribution-oriented definition. It records the type of behavior or activity that has taken place, but this method of classifying crime does not adequately describe the incident in a manner useful for analyzing the nature of a particular type of crime. For example, no information is reported on the methodology of the crime, or the relationship of the perpetrator to the victim.

Problem/Solution Classifications

It is often worthwhile to develop problem/solution schemes to classify crimes. These alternatives can be structured to provide information for reducing vulnerabilities for criminal attack. For example, the forceable entry into a private residence during a burglary or robbery could also be classified by the manner in which the entry was achieved (e.g., broken window, impersonation, picked lock). This would help identify appropriate methods to prevent similar forced entries in the future. Problem/solution classification schemes thus involve gathering data that help in juderstanding the nature of specific criminal incidents.

Many dimensions can be used to describe the incidence of EFT crimes; several are listed in Exhibit 4-6. To describe the nature of EFT crimes, useful information may include technical vulnerabilities, incidence of criminal attempts,

Exhibit 4-6

EFT Crime Classification Dimensions

Category of EFT Technology

- Consumer EFT: ATM, POS, TBP
- Corporate EFT: Wire Transfer, ACH
- Internal EFT

EFT Component

- Hardware
- Software
- Internal Procedures
- External Procedures

System Vulnerability

- Terminals
- Personnel
- Communications Links
- Computers

Type of Loss or Target Asset

- Money or Financial Instruments
- Unauthorized Use of Services
- Stolen Property
- Information Loss
- Physical Destruction

Identity of Perpetrator

- Bank Employee
- Bank Customer
- Related to Customer
- No Relationship

Modus Operandi

- Physical Attack
- Unauthorized Access
- Fraudulent Data or Records Introduced
- Programming Manipulation
- Communications Tap

Value of Loss

- Stolen Money, Property, Instruments
- Repairs to Damaged Property

Value of Recovery or Restitution

- None
- Partial
- Full

the frequency of specific environments associated with illegal actions, or the magnitude of losses. We feel that four dimensions are particularly useful for further describing the nature of EFT crimes. The initial classification would be made using the types and layers of EFT crime shown in Exhibit 4-5. Beyond that, detailed descriptions can be achieved by identifying the vulnerability of the computer or EFT system to criminal abuse, the type of loss or "target assest," and the relationship of the perpetrator to the customer or financial institution.

Classification by System Vulnerability

Various sources suggest that EFT crimes could be classified by specific functional or technical vulnerabilities. Parker and Nycum, for example, discuss how the operational characteristics of a computer system and perpetrator-unique methods of conduct (referred to as modi operandi) are related. Similarly, the National Commission on Electronic Fund Transfers suggested that the elements of a computer system deserved special focus. Four components of a computer system may be penetrated: terminals, communication links, computer, and personnel.

--Terminal Vulnerabilities

All EFT transactions, ranging from consumer-initiated ATMs to corporate-initiated wire transfers, rely on some kind of terminal to access the computer system. However, terminals that are accessible to the public (generally those associated with consumer EFT) are subject to a different set of risks than terminals which are normally accessible only to employees or authorized users. In general, terminals that are open to the public, such as ATMs and customer-operated POS systems are more susceptible to unauthorized access and physical destruction than the more secluded terminals used for ACHs and wire transfers. However, the potential magnitude of loss is much greater in the event of unauthorized access to terminals linked with corporate EFT. As discussed in Chapter 4 consumer EFT technologies have dollar limits that are very low compared to the transactions which regularly occur through corporate EFT.

The security of ATMs, and other EFT technologies relying on plastic cards to regulate access, lies with PINs (personal indentification numbers)--a simple, inexpensive practice. The customer first inserts his card and then keys in his PIN. If the PIN is correct, the customer is given access to his account. To maintain security, the customer must never write down or reveal his PIN. Because customers often do not heed

this warning, PINs are not always an effective means to block unauthorized access to an account.

Although financial institutions have reported security problems associated with unauthorized persons discovering PINS and stealing or duplicating the corresponding card, or with negligence on the part of customers in allowing their PINs to be discovered and their cards used, the limited information collected to date suggests that ATM providers experience less fraud than with similar paper-based systems. According to an American Bankers Association survey of 225 ATM providers, about 75 percent of the providers perceived losses to be less than they were prior to the advent of ATMs [ABA, 1978]. This explains why more secure identification techniques have not been implemented. At least some ATM providers view the current ATM identification system as an improvement in terms of security over what they have experienced in the past. Thus, they are reluctant to implement costly new strategies that may only marginally improve reliability.* Further, tighter security measures to protect against unauthorized use of terminals may inhibit authorized use, or at least make access more difficult.

Despite the apparent lack of incentives to move forward with costly new identification devices, with the growing awareness of the criminal vulnerabilities of PINs, several card protection technologies are being developed; three are receiving growing attention from bankers.** First,

---

*While many financial institutions would like to improve card security, none of the available methods has proved reliable enough to justify the costs. Under the standards in regulations and law, not only must a "reliable method" identify authorized users on a 99.5 plus percent basis in no more than three attempts, but also wrongful dishonors of authorized users by the authentication method must be infinitely small [Greguras & Sykes, 1980].

**Other methods to detect and prevent unauthorized access to purely customer-initiated terminals include: 1) anti-duplication devices such as radioactive isotopes, magnetic ink bars, heat and pressure sensitive materials, and personal characteristics links (i.e., finger or voice prints); 2) terminals designed to hide PIN entry; 3) requirements that customers report billing errors; 4) video recording of terminal transactions; 5) retention of the card when the PIN is repeatedly misentered; 6) transaction limits; and 7) customer liability in the event the customer is negligent and allows both his card and PIN to be used or is slow to report a lost or stolen card.

fingerprint identification by computer is being considered as a means to limit unauthorized access to ATMs. Equipment exists which can identify fingerprints ["Data Card...," American Banker, 1/7/81]. Second, voice identification by computer is being tested to limit unauthorized transfer of funds. This has relevance to corporate EFT and telephone banking as well [Matthews, 2/10/81]. Neither is reliable enough at this time to justify its costs. Third, smart memory chips or dual strips (one optical, one magnetic) on a card can fill two roles. Either can carry information to help limit unauthorized access, such as a password a person must remember, and either can act as an accounting record with the individual's personal computerized bank account carried on a plastic card. The memory chip provides more potential in this second role, but dual-strip technology may be more acceptable to established institutional networks [Kutler, 10/13/80, 1/20/81]. While these will not overcome PIN vulnerabilities, encoded account records may help reduces losses at offline terminals.

Following the unauthorized access problem, the ABA study suggests that customer-initiated fraud may be the second major security risk. Respondents attributed 22 percent of ATM loss to customer-initiated fraud. Without knowing more detail about the method of perpetration it is difficult to accurately speculate as to the vulnerabilities actually usurped. However, a large portion of that loss is probably attributable to customers withdrawing more money than was actually held in their account.

--Communication Link Vulnerabilities

The vulnerabilities of communication links connecting online terminals to computer systems and those connecting offline terminals differ significantly. Offline terminals produce data records in the form of tapes, cards, printouts, etc., which must be hand carried to computer input devices. A study performed on computer abuse (not specifically related to EFT) by functional vulnerabilities indicated that manual handling of input/output data accounted for 41 percent of all computer abuse cases reported in the study [Parker and Nycum, 1979]. Because offline terminal communication links required more manual handling of input/output data, they were more susceptible to manual alteration.

Online terminals input directly into computers through communication links such as wire cables, telephone lines, or microwave transmissions. Online terminals are subject to alterations of information in transmission or theft of information such as PINS and account balances. However, the methods of perpetration require sophisticated penetration of

the communication link. Online systems are primarily vulnerable to wiretapping devices such as imposters or spoofers. Spoofers generally are simple devices which insert deceptive instructions in the system, while imposters are more complex devices which simulate terminals [NCEFT, 1977a].

Another major communication link vulnerability is "appearances" or intercommunications between various branches of complex computer networks. Although very little documentation of the incidence or magnitude of EFT computer link penetration exists, the potential magnitude of loss warrants future analysis of such security risks. Most communication links are accomplished by wire (or cable) and microwave transmissions. At least among the wire or cable technologies there are many risk levels (e.g., telephone lines are quite easy to penetrate without detection, while coaxial cables are very difficult; coaxial cables, unlike other wire technolgies, incorporate testing, resistance testing, frequency testing, and alarms which are activated by changes in any of the above). But no method is completely effective, especially when the system includes numerous switches between capacities.

Because penetration cannot always be detected (and many EFT terminals are connected by telephone lines--the easiest technology to penetrate), many providers use encryption (i.e., coding of transmitted data) to further secure the system When transmissions are coded, it is more difficult for the criminal to use or alter the stolen information. Although no cost-benefit analysis has been performed to justify encryption or alternative methods to detect or prevent penetration, the potential magnitude of loss associated with a single penetration requires that greater effort be given to communication linK security.

--Computer Vulnerabilities

Several known methods of altering computer software are very difficult to detect, such as the trojan horse (i.e., computer instructions to perform unauthorized functions), salami techniques (i.e., transfer of small amounts from a number of accounts, such as rounding programs), logic bombs (i.e., programs which are activated upon the occurrence of some future event), asynchronous attacks (i.e., strategies which take advantage of the timing of various computer instructions), superzapping, browsing, and data leakage [Parker and Nycum, 1979]. Such techniques are hard to detect in advance of substantial loss because detection generally depends on the observation of inconsistencies in output generated after the fact. Also, they generally involve insiders with detailed knowledge of the comuter system.

Since great losses can occur in a short period of time, the risks are high.

The vulnerability of EFT computers to physical attack is another concern for which little information exists. As financial assets are increasingly stored in electronic form, physical vulnerabilities will present greater risks. For example, magnetic fields or rapid changes in temperature or moisture level can adversely impact electronic equipment and stored data. It is worth noting that physical destruction or the threat thereof does not require sophisticated knowledge or insider assistance as do other major vulnerabilities.

--Personnel

Because many EFT vulnerabilities require a high level of knowledge about computer systems, employees who possess such knowledge constitute a main point of vulnerability. They may be coerced by individuals or organizations into assisting in an EFT crime, or they may initiate it for their own purposes. In either case, the computer system is primarily vulnerable to the people who operate it. The more sophisticated the knowledge required or possessed by the employee, the greater the risk, both in terms of successful penetration and the magnitude of the assets which might be accessed.

Classification by Target Asset or Type of Loss

Parker and Nycum have compiled an extensive file at SRI International of reported computer crimes that have occurred in the last decade (see Chapter 5, pages 67 to 73 for a description). Based on these cases, they have suggested a classification scheme by types of losses, referred to as "target assets." The categories include physical destruction of equipment, intellectual property deception and taking, financial deception and taking, and unauthorized use of services.

Although the file they have collected is not a statistically-based sample of the universe of computer crimes that occur within financial institutions, and any conclusions should be made with caution, it does suggest the following about the vulnerability of financial institution's target assets:

> When computer abuse is perpetrated against financial institutions the vast majority of cases appear to involve financial deception or taking as opposed to other categories of target asset.

- Property deception or taking and the unauthorized use of services have not been a major target of computer crime, at least in the cases collected in the computer abuse file.

- Physical destruction of computers and their contents has occurred frequently enough to warrant significant concern. However, the average loss per incident has not been as great as that associated with deception or taking of either property or finances.

A classification system based on target assets warrants continued attention. Not only does it provide a basis to compare strictly paper-based systems to systems incorporating EFT technologies, but it also helps to focus on the primary targets of EFT crime. This identifies the problem and should help EFT providers consider an optimal allocation of prevention resources.

Building on Parker and Nycum's original classification, August Bequai developed five categories of target assets by breaking property deception or taking into two categories: theft of property, and theft of information [Bequai, 1978]. This further classification seems useful in that it may isolate purely privacy issues (under theft of information) from those issues which involve the loss of tangible assets. With this in mind, we recommend a five-part classification system related to target assets: physical destruction, theft of property, theft of information, financial deception and takihng, and and unauthorized use of services.

Classification by Relationship of the Perpetrator

EFT crimes usually require special knowledge about the EFT system and access procedures, and it is therefore likely that the pereptrator will be part of or known to the system. At least five categories of perpetrators can be identified. The first consists of the customers who use specific EFT applications. Consumers and merchants interact primarily through ATM, POS, and home banking technologies. Corporate customers interact primarily through wire transfer requests and direct deposit accounts. Because they are granted access, albeit limited, to the EFT system, unscrupulous individuals have the opportunity to commit EFT crimes. The second category consists of individuals related to bank customers, such as roommates, relatives, and employees. Employees of financial institutions constitute a third category of possible perpetrators. These insiders--such as tellers, accountants, auditors, and programmers--are often directly involved with the provision and use of EFT services and represent a distinct threat to security. For example,

Brandt Allen indicates that from the data collected in a study by the AICPA (described in Chapter 5, pages 78 to 80) a surprising number of insiders, and especially managers, were responsible for a large number of banking crimes [Allen, 1981]. The fourth category consists of the suppliers who provide financial institutions with EFT hardware and software. It includes individuals such as vendors and service representatives. The final category of possible perpetrators consists of individuals who neither operate nor interact with EFT services. Without an easy means of access to the system, they are likely to resort to tactics such as wiretapping, vandalism, burglary, and theft. Terrorists would also fall into this category.

Crimes classified by the relationship of the perpetrator may provide security designers with information regarding systematic vulnerabilities among security options. Internal auditing or operational safeguards may take precedence over physical or external security hardware. More complex customer transaction authorization procedures may appear to be demanded, or perhaps coding of electronic signals, an expensive but interesting modification at preent, may be deemed a high priority.

4.5 APPLYING THE FRAMEWORK

This chapter has developed a broad three-dimensional framework for classifying EFT crime. The first dimension is the category of EFT technologies (i.e., consumer, corporate, and internal EFT) used to commit the crime; the second is the layer of EFT component penetrated (i.e., hardware, software, internal procedures, external procedures, and related). Finally, the third dimension focuses on the legal and problem/solution classification schemes discussed above (i.e., legal definition, systems vulnerability, target asset, and perpetrator). By grouping all three of these dimensions together, we are not only able to relate traditional definitions of crime to EFT technologies but we can also link the level of the EFT system penetrated, the methodology of the crime, targeted assets, and perpetrators.

In turn, the dimensions of this classification framework can be used to describe the nature and extent of EFT crime. It helps in understanding, for example, which type of assets are most likely to be the target of criminal actions, the methods most likely to be employed for each type of EFT application, and the relationship of perpetrators according to the component of the EFT system penetrated. The classification system will therefore be used in the remainder of this report to identify the kinds of data needed to assess

the nature and extent of EFT crime. In Chapter 5 it will be be used to help evaluate potential data sources, and in Chapter 6 it will assist in developing a possible measurement approach.

5 SOURCES OF DATA ON EFT-RELATED CRIME

One of the primary objectives of this project has been to examine the full range of available data on EFT crimes in order--to the extent possible--to assess the nature, magnitude, and probable trends regarding EFT criminal activity. A number of references have appeared in newspapers and magazines, and occasionally in the professional literature, which speculate on the "growing problem" of computer or EFT crime; but when they are traced to their sources, only confusion seems to prevail. For example, a recent article on computer crime appearing in Time [2/16/81] suggested that only one percent of all computer crimes are ever detected. Upon investigation, it was discovered that the figures were taken from a book which referred to yet another article quoting a computer executive. After further examination, though, it appears that no one will actually claim ever making the remark; and needless to say, the widely published "statistic" has little foundation in fact.

Other statistics--such as only 1 of 22,000 computer crimes is ever prosecuted, or that 1800 computer crimes were reported in 1981--are mentioned periodically at conferences or by the media. During the course of this project we spent considerable time tracing the source of these and other possible factual analyses. To date, we have found no number or statistic which has any basis in published fact, that is, which originated through valid statistical derivation. Every figure appears to have come from personal estimates or a very limited number of case studies acquired by individuals in the computer community.

In a presentation on computer security, Brandt Allen further illustrated the confusion by citing three statements from peers in the computer security field:

- Despite the best efforts of management, accountants, auditors, and the courts, the general problem of embezzlement remains largely unsolved, and it is growing worse [and] computer-related frauds continue to increase [Allen, 1980].

- Available data does not generally support the contention that white-collar crime, particularly that involving computers, is growing [Courtney, 1980].

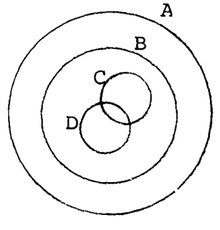
- Computer crime is a media creature, largely fed by computer security industry press releases [Taber, 1980].

CONTINUED

1 OF 3

Varying perspectives such as these are not unusual because no valid statistical data exist. Measuring EFT or commputer crimes presents a unique challenge in that often not only criminals, but also victims, desire that the incidents remain unpublicized. Thus, data must be discovered, not simply collected. This problem is especially relevant to EFT because the victims of the crimes (generally financial institutions) are sometimes reluctant to talk about violations for fear of reduced confidence among depositors.

The situation may be represented in the form of concentric circles, as shown below. The largest circle, in this case A, includes all EFT crimes that occur in a given



A--EFT crimes which occur

B--EFT crimes which are detected

C--EFT crimes which are reported formally

D--EFT crimes which are reported informally

time period. Circle B represents the portion of the crimes that are detected. However, not all of these crimes are reported: only a small portion of the detected crimes reach formal (circle C) or even informal reporting documents (circle D). Further, data recorded on these documents may vary by source because of differing reporting definitions and requirements.

The task of measurement, then, requires the analyst to first identify and classify reported crimes, and then to use the existing data (and any other relevant information) to estimate the actual magnitude of crimes occuring in a given period. Three questions arise when examining available sources of data: (1) Are there any specific numbers concerning the nature and extent of EFT crime? (2) Is the data source reliable, or in other words does it have any statistical validity? (3) Will any of the information provide an ongoing, accurate source for the future?

In order to address these questions a thorough literature search was conducted; dozens of industry, government, and law enforcement officials were interviewed; and site visits were made to review potential sources of data and to examine the records of financial institutions. This section of the report discusses the results of these efforts. First some of the perceptions about EFT crime trends that

have appeared in the literature are briefly reviewed. Second, the scope and reliability of potential sources of EFT crime data are evaluated. Finally, the prospects for measuring EFT crime using these sources are discussed.

5.1 PERCEPTIONS OF TRENDS

Before examining specific data sources for their measurement potential it is useful to identify some of the perceptions which emerge from the literature regarding the incidence of EFT crimes. In the absence of clear empirical data, a major consideration is whether crimes have actually increased or decreased with the advent of EFT. The dispute centers on two independent issues: the impact of EFT on the incidence of crime, and the impact of EFT on the magnitude of loss. Although the sources of information are sparse, Exhibit 5-1 identifies the impressions of contemporary research and professional opinion on these issues. The exhibit relates these findings to the traditional categories of crime and to the three primary categories of EFT technologies. Available evidence is sketchy, but a few tentative perceptions emerge:

- Although the precise level of computer or EFT crimes is unknown, it is probably true that EFT crime is still only a very small portion of all crimes at financial institutions

- Although experts tend to agree that the incidence of crimes such as burglary, larceny and fraud will be reduced by certain EFT technologies, the potential for loss is sufficiently great to cause dispute over the general impact of EFT on crime. The magnitudes of a few specific EFT crimes have been very high in the past, particularly in the corporate EFT area, indicating a special vulnerability.

- The incidence of crimes associated with ATMs is less, or at least no worse, than it might have been if the same transactions were conducted in a purely paper-based system.

- Customer crimes such as overdrafts and bad checks may actually be reduced by the use online ATM terminals, check guarantee and authorization mechanisms, direct debit POS terminals, and automatic bill paying. These new systems electronically check the assets held in an account to prevent improper withdrawals.

Exhibit 5-1

Impact of EFT on Traditional Crimes

	Consumer EFT						Corporate EFT				General Level w/o Regard To A Specific Technology	
	ATM		POS		TBP		ACH/ Direct Deposit		Wire Transfer			
	Incidence	Magnitude	Incidence	Magnitude	Incidence	Magnitude	Incidence	Magnitude	Incidence	Magnitude	Incidence	Magnitude
Theft												
Burglary			-									
Larceny					-		-		-			
Embezzlement											- [1]	+ [1]
Espionage												
Fraud	- [2]	- [2,4]	-		-					+ [3]	- [1,2]	+ [1]
Bribery											+	+
Blackmail											+	
Destruction												
Arson												
Sabotage	+		+								+	+
Vandalism	+		+									
Losses With No Relation to Particular Crimes	- [2]										In Dispute	

Legend: + indicates an increase in the incidence or magnitude of loss associated with the crime
- indicates a decrease in the incidence or magnitude of loss associated with the crime

References:
[1] Donn Parker, presentation February 20, 1978 to California Task Force on EFT
[2] ABA Survey of 225 banks offering ATM services, May 1978
[3] Potential may be there as in a few selected cases
[4] FDIC survey of EFT security in 1,260 federally-insured banks, 1977; cited in EFT in the United States: Policy Recommendations and the Public Interest, final report of the National Commission on Electronic Fund Transfers, October 28, 1977, Washington, D.C., pp. 183-185

- EFT reduces the need to physically transfer financial assets, a vulnerability to theft in the past. ACHs and direct deposit protect against mail theft, although they open up the possibility for EMS theft. ATMs reduce the need for persons to carry cash. Thus, EFT may reduce the incidence of high-frequency crimes such as fraud and armed robbery.

- Although the number of consumer-related EFT crimes will probably grow over time as the technology expands and people become more aware of the possibilities for crime, the actual magnitude of any particular crime will generally be small because of the nature of the technology.

- The advent of EFT may increase the potential magnitude of loss associated with crimes perpetrated or assisted by insiders or experts.

- Although the actual level of corporate EFT crime to date compared to the dollar volume is small, the potential for crime is high because such extremely large dollar volumes are transferred each day.

5.2 SOURCES OF DATA

Unlike the general criminal justice field for which the FBI Uniform Crime Reports serves as the primary source of data on reported crime, the EFT field does not have a comparable single source. Thus, to identify potential data sources, we conducted a detailed literature search and interviewed experts throughout the country. The initial literature search was run on the MIT Computerized Literature Search Service. As summarized in Exhibit 5-2, the literature on EFT is fairly extensive and the literature related to criminal activities is vast. However, when the two topics are combined, only 201 articles and books remain. Brief synopses were used to locate and review the most relevant documents (which provide the basis for many of the preliminary percepetions reported above). Unfortunately, very few of these documents actually contain specific information concerning the magnitude of EFT crimes. Most describe the operations of EFT systems; many explain the vulnerabilities of EFT and a small number discuss EFT crime as a potentially large or small problem. Only a very few provide any data related to the incidence of EFT crime.

After a thorough review, we identified four primary sources for information on EFT crime: a file of computer abuse cases compiled at SRI International by Donn Parker and

Exhibit 5-2

Summary of Computerized Literature Search: EFT and Criminal Activities

Type of Data Base	Time Period Covered (Inclusive)	Topic of Search and Number of Citations		
		EFT	Criminal Activities	EFT and Criminal Activities
Management, Administration and Finance	1971-1980[1]	945	10,055	168
Electronics, Computers and Control Technology	1969-1980	150	3,417	25
Social Science and Legal Resources	1972-1980[2]	20	8,976	7
Popular Magazines	1977-1980	43	2,321	1

[1] One data base covered the time period 1974-1980.

[2] One data base covered the year 1980 only.

Susan Nycum; reports filed by financial institutions with federal regulatory agencies; bank crime files maintained by the Federal Bureau of Investigation (FBI); and a study of computer crime in financial institutions conducted by the American Institute of Certified Public Accountants (AICPA). In addition, a few surveys and miscellaneous materials were found in the literature. Unfortunately, not one of these sources provides the data, or even the potential, necessary to measure and understand the nature and extent of EFT crime. Each has only limited information, and all have problems from a statistical perspective. Further, although several offer a possible source of information, the potential exists only if major changes are made in the collection process--changes which seem highly unlikely.

The SRI Computer Abuse File

The SRI Computer Abuse File, perhaps the most well-known record of computer crime, is a compilation of over 1000 computer abuse cases identified by Donn Parker, Susan Nycum, and others at SRI through individual contacts and a newspaper clipping service. The file originated in the early 1970s as the focus of a study on computer crime sponsored by the National Science Foundation. Similar to our present effort to identify and measure EFT crime, the project sought to identify computer crimes and to obtain some perception of the extent of such crime. The file was supported and maintained by NSF until very recently; it is now supported by the Department of Justice. The number of cases in the file by year and type are listed in Exhibit 5-3. Although the focus is computer abuse, of which EFT crime is only a subset, over 120 cases involve financial institutions and most are EFT-related. (See Appendix D for examples of these EFT crime cases).

The procedures for selecting cases and maintaining the computer abuse file are summarized in Exhibit 5-4. A variety of criteria are used to select cases for the file. Researchers review clippings, letters, and other documents from a case to determine its relevance. If approved, it is assigned a case book number which identifies the date of perpetration, the date discovered, the date prosecuted, and the type of crime. All pertinent data about the case are then recorded in detail in a central register to allow referencing of the case history without cumbersome review of the case file itself. Recorded cases are supplemented by new information as it appears in subsequent articles or documents. Information on source, loss, principals, disposition or description is often added.

Exhibit 5-3

SRI Computer Abuse File

Year	Number of Cases				
	Type 1 Physical Destruction	Type 2 Intellectual Property Deception and Taking	Type 3 Financial Deception and Taking	Type 4 Unauthorized Use of Services	Total
1958			1		1
59			1		1
60					-
61					-
62	2				2
63	1		1		2
64	1	2	3		6
65		1	4	3	8
66	1		2		3
67	2			2	4
68	1	3	6	2	12
69	5	9	4	4	22
70	8	8	14	11	41
71	7	20	25	8	60
72	17	20	19	18	74
73	10	26	28	11	75
74	7	22	34	12	75
75	5	21	49	9	84
76	5	21	36	5	67
77	14	19	50	14	97
78	12	22	28	14	76
79	8	27	28	18	81
80	3	12	17	10	42
81	1	1	8	6	16
TOTAL	110	234	358	147	849

Exhibit 5-4

Procedures For the SRI Computer Abuse Case File*

Sources

Case materials and potential case materials include:

- Clippings from Allen's PCB, a clipping service
- Clippings and photocopied articles collected by the staff and recieved from contributors
- Letters
- Handwritten memos from staff members regarding information received in conversation and telephone interviews.
- Staff reports of interviews with law enforcement agencies, participants, etc.
- Legal documents

Selection

The criteria for selecting new cases cannot be briefly stated. Dr. Donn Parker gives final approval to all new cases. Often, newspaper items do not give enough detail to make clear the role of a computer, and require decisions about follow-up. Therefore, any material Dr. Parker has not seen is sorted for his attention.

Cases--Place items describing what appear to be new cases in a NEW CASE ITEMS folder for Dr. Parker to examine and return with approval or other instructions.

Old Cases--When a new item is recognized as relating to a case already recorded, find the number and mark the item, and include them in the NEW CASE ITEMS folder.

Probable Cases--Clip together with a note indicating them as probable cases, and include in the NEW CASE ITEMS folder for Dr. Parker's decision.

Of Interest--Bring to Dr. Parker's attention, because they contain no cases but are relevant to our interests.

Non-Relevant--Place in the drawer of such limbo material, for any possible future use. Nothing is discarded.

Materials Selected

All approved materials, which include staff reports, correspondence, and other material received should be placed in a folder labeled TO BE ADDED. Materials in folder can be withdrawn for coding and recording.

---

*Information for this exhibit was obtained from Dr. Donn Parker at SRI. We appreciate his complete cooperation in sharing information concerning the file.

A computerized data base of brief case records is also maintained to allow information retrieval and flexible aggregation. These case records include a brief descriptive title and sources of additional information. They are codified by various elements of the case, such as perpetrators or defendants, victims, type of abuse, date and place of the abuse, and loss. Computer-produced indexes can be obtained by a user-oriented online retrieval system which uses keywords.

The SRI file is of greatest value for computer security and legal research. Cases provide practitioners and academics alike with feasible examples of the vulnerabilities of computer systems to abuse and the legal issues surrounding prosecution and sentencing. In some cases the file has sparked laboratory experiments in security technology or debate on public policy.

Another benefit of the file is the descriptive information it provides on the nature of computer, and some EFT, crimes. Based on the collected cases, some empirical results are available. Although not randomly collected, they provide useful insights regarding the number of cases in each category, known losses, and average loss per case. These data are presented in Exhibit 5-5. (See Chapter 4, pages 57 to 58 for further discussion of the applications of the SRI file.)

However, the SRI file is concerned primarily with computer crime, of which EFT crime is a small part. Thus, Parker attempted to isolate potential EFT crimes in the data base by identifying the subset which involved financial institutions [Parker, 1980]. Exhibit 5-6 summarizes these findings. Of the more than 800 computer abuse cases reported through 1980, 121 related to financial institutions. These cases are divided among the four types of target assets--physical destruction, financial deception and taking, intellectual property deception and taking, and unauthorized use of services--identified in Chapter 4.

The major limitation of the file as a source to measure the extent of EFT crime is that it includes only those cases which were reported by the media or uncovered by researchers. Large losses or unique crimes will often bring a case to the attention of the researchers, but this does not provide a random sample of information. Compounding the problem is the fact that EFT crimes are not a primary focus of the research, but only a by-product of the collection. Although the file is a useful collection of cases, it can not be considered a statistically valid sample. In a report on his work, Donn Parker emphasized that "the Computer Abuse Project is <u>not</u> a

Exhibit 5-5

SRI Computer Abuse Cases: Incidence and Loss

	Type 1 Physical Destruction			Type 2 Intellectual Property Deception and Taking			Type 3 Financial Deception and Taking			Type 4 Unauthorized Use of Services			All Types		
Year	No. of Cases:[1] % of Total	Known Losses[2] for Type 1	Av. Loss[3] Per Case, Type 1	No. of Cases:[1] % of Total	Known Losses[2] for Type 2	Av. Loss[3] Per Case, Type 2	No. of Cases:[1] % of Total	Known Losses[2] for Type 3	Av. Loss[3] Per Case, Type 3	No. of Cases:[1] % of Total	Known Losses[2] for Type 4	Av. Loss[3] Per Case, Type 4	Total Cases[1]	Total Known Losses[2]	Average Loss[3]
1958	- -	-	-	- -	-	-	1 0%	<1	<1	- -	-	-	1	-	-
1959	- -	-	-	- -	-	-	1 0	$ 278	$ 278	- -	-	-	1	$ 278	$ 278
1962	2 0%	-	-	- -	-	-	- -	-	-	- -	-	-	2	-	-
1963	1 50	$ 2,000	$2,000	- -	-	-	1 50	81	81	- -	-	-	2	2,081	1,040
1964	1 17	-	-	2 33%	$ 2,500	$2,500	3 50	100	100	- -	-	-	6	2,600	1,300
1965	- -	-	-	1 13	-	-	4 50	126	63	3 38%	-	-	8	126	63
1966	1 33	<1	<1	- -	-	-	2 67	28	14	- -	-	-	3	28	9
1967	2 50	<1	<1	- -	-	-	- -	-	-	2 50	$ 10	$ 10	4	10	10
1968	1 8	-	-	3 25	7,203	3,602	6 50	5,251	1,313	2 17	-	-	12	12,454	2,075
1969	4 20	2,000	2,000	8 40	1,003	334	4 20	6	2	4 20	2	2	20	3,011	376
1970	8 21	3,600	900	6 16	6,843	1,369	13 34	8,910	810	11 29	-	-	38	19,353	967
1971	7 12	-	-	20 34	9,844	1,641	24 41	5,943	540	8 14	351	175	59	16,137	849
1972	17 23	11,148	2,230	19 26	180	30	19 26	3,090	257	18 25	107	21	73	14,524	518
1973	10 13	4	2	26 35	26,782	2,435	28 37	206,274	11,460	11 15	7	1	75	233,066	6,474
1974	7 10	2,010	1,005	20 27	2,197	439	34 47	3,952	158	12 16	3	3	73	8,162	247
1975	5 6	115	58	21 25	91,670	13,096	49 58	6,513	176	9 11	14	5	84	98,312	2,006
1976	5 8	1,110	370	19 32	49,465	7,066	30 51	2,026	78	5 8	-	-	59	52,601	1,461
1977	14 16	2,252	322	16 18	17,946	3,991	44 51	47,501	1,319	13 15	154	77	87	67,853	1,330
1978	10 24	2,523	841	13 31	300	50	17 40	12,384	826	2 5	-	-	42	15,207	633
1979	2 10	-	-	11 55	-	-	4 20	200	200	3 15	-	-	20	200	200
TOTAL	97 14%	$26,761	$ 836	185 28%	$215,932	$3,322	284 42%	$302,661	$1,462	103 15%	$646	$ 32	669	$546,001	$1,685

1 Cases: Total known cases of this type in year, whether or not loss is known
2 Known Losses: Thousands of dollars
3 Av. Loss: Average for cases where loss is known

Source: Parker and Nycum, 1978, p. 7 (Data as of 4/13/79).

Exhibit 5-6

Financial Institution Cases in the SRI Computer Abuse File

Type of Target Assets	Financial Institution (FI) Cases		All Cases	
	Number	Percentage of 121 FI Cases	Number	Percentage of All 633 Cases
Physical Destruction of Computers or Their Contents	8	6	95	15
Financial Deception or Taking	110	91	274	43
Property Deception or Taking	2	2	164	26
Unauthorized Use of Services	1	1	100	16
TOTAL	121	100	633	100

Source: Modified from chart in Parker, 1980, p. 655.

rigorous, sociological, statistically-based crime study [Parker, 1980]." Thus, it is essentially impossible to use this file to make even general inferences regarding the incidence of computer, let alone EFT, crimes.

In addition, the majority of the EFT cases in the file are consumer frauds and thefts; only a few corporate or internal EFT crimes are included. Because information is so sparse in the latter two categories, it is even more unrealistic to expect to draw meaningful conclusions from the data. Finally, because much of the file claims media investigation as its source, a number of the cases at any one time are not verified. The consequences of this were explained in another SRI report:

> Applying the conclusions to all cases beyond those represented by the data base is subject to statistical uncertainty...Two instances have occurred where verified cases were subsequently found to be fictional, or at least not to contain sufficient basis in fact. Several unverified reported cases in the file are suspected of being without basis of fact, but remain in the file as real cases until proven otherwise [Parker, 1975].

Federal Regulators of Financial Institutions

A potential source of information on EFT crime are the reports filed by financial institutions with federal regulatory agencies. Until recently, most financial institutions were required to report internal crimes (e.g., embezzlement, employee frauds and larcenies) and external crimes (e.g., robberies, burglaries, nonemployee larcenies) to the appropriate federal regulatory agency: the Comptroller of the Currency for national banks, the Federal Reserve Board for state-chartered Fed members, the Federal Deposit Insurance Corporation for insured nonFed members, the Federal Home Loan Bank Board for savings and loans, and the National Credit Union Administration for credit unions. In addition, financial institutions are also required to report crimes to the law enforcement agency with jurisdiction over the crime--the U.S. Attorney, the FBI, or the local police department.

The requirement to report external crimes was adopted by the federal financial regulators pursuant to the Bank Protection Act of 1968; all the regulatory agencies required institutions to file a "Form P-2" or "Report of Crime" for each such external incident. (Copies of the FDIC and Federal Reserve "Report of Crime" forms are included in Appendix E.) However, in October 1981 the Federal Reserve, FDIC, FHLBB,

and the Comptroller eliminated this requirement to report external crimes. (A description of this decision is provided in Appendix F.) The NCUA agreed with the deleted regulation, but planned to publish its "nonrequirement" under a separate amendment. In its place, the agencies imposed a requirement that "the victimized institution maintain an informal, internal record of each external crime and file all such records in the main office of the institution." Consequently, Form P-2 is no longer used and consistent information on external crimes (which includes the categories of external procedures-based and environment-based EFT crimes identified in Chapter 4) at financial institutions will no longer be available in any aggregate--and therefore reasonably accessible--form.

Federal regulators still collect information on internal crimes and thus are likely to capture EFT crimes that are internal procedures-, software-, or hardware-based. However, there is no comprehensive regulation that all financial institutions report internal crimes to the appropriate regulatory agency. Although all the regulators collect reports of internal crimes, each follows unique procedures. The Comptroller, for example, requires through regulation that a national bank report by letter any incident in which it has substantial reason to believe a crime has been committed, or in which there is a substantial or unreasonable risk of loss, or in which unsafe or unsound banking practices are suspected (the Comptroller interprets this regulation broadly to include both internal and external crimes that meet this criteria). Similarly, the Federal Reserve Board requires state-chartered banks to report any felony, or any incident with a loss greater than $100. The FDIC, however, expects insured nonFed Banks to report any internal crime although this is based on long-standing policy, not law or regulation.

A brief look at the FDIC process helps to identify the kinds of information collected by federal regulators and to illustrate the purpose of the internal crime reports. The "Report of Criminal Irregularity" is a general form used to cover all types of exployee-related crimes. (A copy of the form is included in Appendix E.) It provides a place for the name of the participant, the nature of the apparent irregularity, a description of evidence, and general remarks. The form is filled out by bank examiners in regional offices after a bank reports a crime or after the examiner uncovers an unreported incident. This form is used to cover all types of employee-based irregularities. In completing the form, no special effort is made to assure the information collected is consistent, or to ascertain on a regular basis whether a computer or EFT technology was involved.

Once the information is received, the FDIC's Intelligence Section prepares an index card for each case and files it by the name of the offender. This file index is used to determine if people involved in the banking system have been involved in any reported irregularities in the past. If, for example, someone wanted to acquire a bank but his name was contained in the index of reported irregularities, a further investigation might be warranted.

Because information on internal crimes is collected by the FDIC for a very specific and limited purposes--to provide a cross-check of prospective members who may have been involved in previous criminal or supsect activities--the data are not aggregated or maintained in a manner which would facilitate measuring the nature and extent of EFT crimes. The reports are generally compiled by geographic occurrence, and classified by traditional legal definitions. The form contains no special place to denote a computer or EFT crime, and examiners are not expected to indicate whether a computer or EFT technology was involved. Information on the incidence of EFT crimes could therefore only be obtained by a case-by-case review--a nearly impossible task considering the nature and design of the form.

The letters filed with the Federal Reserve and the Comptroller are used for similar purposes. And, as with the FDIC, these reports are not aggregated or organized in a manner which would facilitate identifying or compiling EFT or computer crimes. The Federal Reserve, keeps an index card filed by bank for each reported internal crime. The letter and any accompanying documents are then filed with the other information kept by the Fed for that bank.

These letters and formal reports, or some new data collection effort organized by federal financial regulators, offer some hope as a potential source of data on EFT crimes. However, this could occur only if the reporting forms were modified to identify the specific relationships between EFT and crime. In reality, though, the design of a form and collection of data are only the first of many problems.

Each federal financial regulator deals only with a portion of the financial institutions in the country. For example, the Comptroller of the Currency, which still collects both internal and external crime data, possesses authority only over those commercial banks which are nationally-chartered. Although this group represents a large portion of U.S. financial institutions--and those that hold a majority of bank assets--it is only a portion nevertheless. Furthermore, many professionals maintain that smaller banks are more vulnerable to EFT crime than large banks with

sophisticated security systems. Thus a very important segment of the data base would be absent from the Comptroller's data. To get information on state-chartered banks, the reports filed with the FDIC and the Federal Reserve would also have to be included. But, as discussed above, the three regulators do not use identical reporting procedures, and the data collected is not likely to be consistent.

In addition, at present, only information on internal crimes are collected by all the regulators. Thus, information they could provide would in most cases exclude external procedures-based and environment-based EFT crimes. Further, it is unlikely that a regulatory agency would routinely release the information it collects, especially on a matter so sensitive as internal or external crimes. Such data have traditionally been difficult to obtain.

Finally, it must be remembered that the financial regulators are interested primarily in monitoring the health and security of the financial system. When it comes to crime, they want to protect their members from criminal abuse where possible and to learn how to best cope with it. However, they do not want to become law enforcement officials nor do they feel it is their job to measure or keep track of certain types of crime. One of the major arguments in favor of eliminating the requirement for the reporting of external crime was that information on such crimes is maintained by the FBI and is available to the other agencies. Thus, efforts to strengthen criminal data collection by regulators are unlikely to be supported by the regulators themselves. The potential exists for the collection of data on EFT-related crime by the financial regulators, but only if new reporting forms are designed and implemented, and only if major changes are made in the philosophy and approach of these agencies. Such changes seem highly unlikely.

Federal Bureau of Investigation

The FBI investigates most cases of bank fraud and embezzlement and maintains case records on federal offenses (financial crimes are considered federal offenses if the bank is federally-chartered or if bank assets cross state lines in the course of the criminal act). When a federal offense in involved, information on every aspect of the case is recorded for historical and investigative value and a variety of recordkeeping systems are maintained.

The primary source of national crime data maintained by the FBI, of course, is the Uniform Crime Reports. This document provides policy information and helps to keep track

of trends and priorities by monitoring total crimes reported within a given time period, classified by traditional legal definitions. These totals, indexes, averages, and trend analyses represent the combined reports of the FBI on federal offenses and state and local law enforcement agencies on state offenses. The FBI obviously does not keep case records concerning nonfederal crimes because they possess no jurisdiction over them; they merely collect and aggregate the reports submitted by states.

As discussed in Chapter 4, data classified according to traditional legal definitions are of limited value to our analysis unless some relationship between the crimes and EFT can be identified with reasonable ease. The ease of identification is also important because measurement must be somewhat continuous, or at least frequent, to be useful to decisionmakers. Since this relationship is not structurally identified at present, it is highly unlikely that EFT or computer crimes would ever be counted as a part of the Uniform Crime Reports; and even if it were achievable, only at an exorbitant cost.

In order to provide central information regarding the overall performance of the FBI, critical data regarding each case are recorded on a form known as the "accomplishment report" and forwarded by agents to FBI headquarters. (A copy of this form is provided in Appendix G.) At headquarters, the reports are entered into in a comuter data base. Data can be retrieved in various levels of detail provided the need for the information is of high enough priority. This information is not very specific, though, as its purpose is to meet program management rather than criminal investigation needs. Further, no information is maintained or collected at this level that identifies EFT or computer crimes.

A better source concerning the details of a particular case is the actual case file maintained at the branch level. Here again, though, no information is routinely collected that ascertains whether a computer or EFT technology was involved in a case. Because computer crimes are not federal offenses--and will not be unless new federal legislation (such as SB 240)is passed --there is no ongoing effort or "interest" by the FBI to maintain data in this area.

One option to provide better data on EFT crime would be to modify FBI recording documents to permit analysis of EFT crimes. For example, the "accomplishment report" and related computer file could be revised to allow monitoring of computer and EFT-related offenses. This could only happen, however, with the strong support of the FBI. Large EFT

crimes, for example, are usually investigated by the FBI, but as frauds, embezzlements, or other traditional crimes because no federal statutes identify them as EFT crimes. In short, the FBI does not identify EFT crimes because the relationship of the computer with the crime has no bearing on law enforcement or the prosecution efforts. Considering the numerous subgroupings of crime which compete with EFT for identification by the FBI, the uncertain benefit to the FBI of maintaining a separate statistic in this area, the fact that a computer crime is not a federal offense, and the problems involved in the definitions of EFT crime (e.g., state versus federal violations, at least from a legal perspective) resistance to this option seems formidable.

Two additional problems are inherent in the use of the FBI as a data source for EFT crimes. First, although the FBI investigates the majority of financial crimes, and surely the largest or most sophisticated, many small local bank crimes are not reviewed at the national level. Information of any detail is usually maintained only at the local level, and data is kept exclusively at that level if the crime is not considered to be a federal offense. In the case of EFT, this could include crimes such as vandalism, robbery of customers, and minor frauds. Thus, the FBI information by itself would purposely omit certain types of EFT crimes, while emphasizing large losses and complex scenarios.

Second, internal crime records and the Uniform Crime Reports are highly aggregated by design. This information is usually useful and adequate for FBI managers or the public. However, further detail is released with increasing difficulty. Neither law enforcement agencies nor victims are eager to provide information to the public on specific criminal activities since it may hamper the effectiveness of an investigation. Records for specific cases could be obtained through the Freedom of Information Act, but use of the FBI's crime files as a continuous or detailed source of information is doubtful at best. In fact, the FBI has a policy against providing case information on a regular basis, and numerous regulations emphasize extreme confidentiality. In conclusion, the FBI provides a potential source of data for EFT crime, but numerous problems exist, and it is highly unlikely that the problems can be, or will be overcome.

American Institute of Certified Public Accountants Study

In 1979 the AICPA set out to examine computer fraud in hopes of establishing appropriate accounting and auditing standards. They approached the task on an industry-by-industry basis, starting with banking. A task force was commissioned, and in cooperation with the Bank Administration

Institute 9,000 commercial banks were surveyed regarding computer crime.

When PSE first learned of this survey, it was hoped that it might provide a source of data on the nature and extent of EFT crime. The surveyed banks were selected to represent a geographic sample of the industry, and the sample was picked to assure that all major financial institutions were included. However, the survey did not focus on the extent of computer fraud in banking. Rather, each institution was asked to describe one case on the provided questionnaire. If an institution wanted to report more than one case it had to make an extra copy of the questionnaire. More than one-half of the sampled banks replied, although most indicated that no computer fraud problems had occurred. From the 5,000 responses only 106 cases on computer fraud were developed, and from these only 85 were classified as computer crimes. Information from these 85 cases was then examined in depth.

Annalysis of these cases provides a good description of the nature of at least some EFT crimes that occur within the banking industry. However, the data base does not provide any information on the extent of such crime, and unfortunately it is impossible to know whether these 85 cases are representative of incidents in all institutions. Specific information on each case includes the computer system involved, the methodology of the perpetrator, the relationship of the perpetrator to the institution, the target asset, and existing security precautions.

A working paper by Brandt Allen [1981] outlined many of the major findings of the study. Allen reported that the introduction of fraudulent input was the most frequently mentioned criminal methodology. In most situations, perpetrators generated fraudulent transactions which were similar or identical to the type they were authorized to create. Of special interest was the large number of cases in which the entries were not financial transactions, but file maintenance entries, such as advancing due dates on loans.

The survey also included information regarding losses, although the report is quick to point out that the figures can be deceptive. For example, although the average loss per case was $125,000, there was one very large case of $5 million which accounted for a significant portion of the average loss per case. Of the 15 largest cases, the average loss is $657,000, well above the $125,000 average. If the extreme losses are removed, the average loss per case becomes much smaller than $125,000.

The most common types of fraud schemes were debits or charges to pending accounts. Perpetrators also often used their own personal accounts as conduits for the transfer of improperly-received funds. Manipulations in the checking and savings areas accounted for about half of the cases. In many cases a large number of transactions was involved in the fraud; for example, in 12 percent of the cases more than 100 transactions were completed before the crime was detected. Detection occurred primarily through complaints from customers or regular internal auditing controls.

Over half of the crimes were perpetrated by tellers, or data entry, operational and clerical personnel. This is to be expected since these personnel make up such a large portion of a bank's organization. A surprising finding, however, was the large number of bank managers involved--19 managers in 85 cases. Managers in the bank cases were likely to perpetrate loan frauds while clerical employees tended to go after savings and checking account systems. Only a relatively small number of computer specialists were identified as perpetrators--5 in 85 cases.

The AICPA study provides very useful descriptive information on computer crime in the banking industry, and a great deal of useful data has been compiled such as the type of crime, perpetrators, and modus operandi. However, it would be impossible to use this information as a source to predict or measure EFT crime in the United States, because the survey instrument was not designed to examine the level of EFT crime. Banks were requested to discuss only one computer crime even if they had experienced several. In addition, only general definitions of computer crime were provided; respondents were left to determine the significance of a computer crime. This may account for the great number of no "computer crime" responses.

Further, the survey is not statistically valid. This is a the critical flaw as a potential data source because it means the file cannot be used with any degree of certainty to measure EFT crime [Allen, 1981]. Perhaps most troubling from a statistical perspective are both the manner in which the profile of respondents was selected and the nature of the survey instrument. By focusing only on large banks, much of the target population was omitted. As with the FBI and federal regulators, the portion being ignored may be the segment with the highest criminal incidence. Further, responses were not always validated. Absent any rigorous survey follow-up, the respondents do not represent a valid sample of even the survey population.

Miscellaneous Surveys and Other Sources

In the literature review of EFT and criminal activites, we identified a number of specific surveys or statements related to EFT crime. However, very few provided information that was especially helpful in identifying the magnitude of EFT crime. In general they tended to talk about EFT technologies (for example, ATMs), and questions related to crime were asked only as incidental items to the general focus. Brief summaries of illustrative sources follow.

American Banker's Association ATM Survey, June 1978

In May 1978 the American Banker's Association sent questionnaires to approximately 225 banks which use ATMs in order to determine the level of security risk associated with ATMs. The study was done in hopes of warding off excessive Congressional action regarding ATM security issues. Over 60 percent of the 225 banks responded; this group operated about 20 percent of all ATMs as of June 1978. The sample, however, was geared primarily towards larger banks. The average respondent bank operated 14 ATMs, and two-thirds of these ATMs were online directly with computers.

When asked to compare losses associated with ATMs to losses from paper-based systems, most ATM providers indicated that ATM losses were less: 8.9 percent reported no ATM loss, 78.6 percent reported less loss, 7.1 percent reported equal loss, and 5.4 percent reported greater loss. Further, most ATM providers reported either no security problems or minor security problems associated with ATMs, but only 38 percent of the respondents characterized their ATM system as cost justified. 65.4 percent of the dollar losses of the ATMs resulted from unauthorized use of access devices, consumer fraud accounted for 22.3 percent, and 13.2 percent resulted from internal bank problems. The study also indicated that it was currently impossible to determine the cost effectiveness of additional security measures.

This kind of information is interesting and it provides some data regarding the magnitude of ATM crime as perceived by the banks. However, these statistics cannot be extrapolated from or validated as they are only perceptions of crime and are not based on an examination of actual crimes or a statistically-based sample of commercial banks.

National District Attorneys Association

A questionnaire was developed by SRI International in 1979 to determine the degree and nature of experience with computer crimes among attorneys associated with economic

crime programs [Parker, 1980]. SRI received 46 responses and found that 40 offices had received 244 reports of computer crime. Although the results are interesting, as acknowledged by SRI the reliability of the questionnaire was a major limitation. Even though examples of a computer crimes were included, only one respondent agreed that all the examples qualified as computer crimes. In addition, the questionnaire was not pretested, and follow-up sampling did not occur. The very small sample size also makes the data unusable for prescriptive purposes.

Prosecutors present a unique problem as a potential source of information in that definitions of computer crime become more important to the comparability of data. As discussed discussed indepth in Appendix C, laws regarding EFT crime vary among states. Thus, enforcement, prosecution and data analysis are unique to each jurisdiction.

Linda Fenner Zimmer, Surveys of ATM Facilities

Linda Fenner Zimmer has conducted numerous studies and case histories of ATM systems. Many have included a few questions related to security problems. For example, she found that one-third of the banks with ATMs that she surveyed in 1977 reported security problems with their system, although losses averaged less than $100 per incident and prevention was not difficult [Zimmer, 1977].

Federal Home Loan Bank Board Security Survey of Remote Service Units

The latest documented survey we could find by the Federal Home Loan Bank Board was conducted June 1976 and was reported on in the National Commission on Electronic Fund Transfers (NCEFT) final report. According to the writeup in the report, the Federal Home Loan Bank Board found "no known cases of robbery, successful fraud attempts, or loss to any account holders [NCEFT, 1977a]."

Survey Conducted by Payment Systems, Inc.

Payment Systems, Inc., a firm specializing in EFT, conducted a survey of 45 financial institutions with card-activated EFT systems. They found an average loss due to fraud of 10 cents per card for active cards, and a loss of 3 cents per card for the total card base [Kevin, 1980].

Bank Administration Institute

The Bank Administration Institute has described a number of computer-related crimes in its Fraud Bulletin. However,

this bulletin does not provide a measure of the overall impact of computer fraud on the banking industry, and is useful only on a case-by-case basis.

Estimates at an International Conference on Computer Security and Fraud Control, 1980

Robert Campbell, the President of Advanced Information Management, in preparation for the Conference noted above indicated that "authoritative estimates of the cost of computer crimes run the gamut from $100 million to $300 million a year. Some even say the problem is a $3 billion a year problem, and there is one estimate that says that computer crime, if proper precautions are not taken, will amount to $40 billion a year." Campbell also indicated that only 1 percent of all computer crimes are detected and only one in 22,000 crimes is successfully prosecuted owing to weak controls and accountability ["Computers...," Denver Post, 9/6/80].

When listed in the newspaper these figures sound informed. However, as we noted at the beginning of this section, to the extent that we have been able to track down and validate these types of numbers, we have discovered that they have no basis in fact, or at least they are based only on opinion and not on statistically-valid studies.

Chamber of Commerce of the United States Report on White Collar Crime

The Chamber of Commerce of the United States studied white collar crime and issued a report in 1974 [Chamber of Commerce of the United States, 1974]. According to this study $40 billion per year is the minimum total loss from white collar crime. This estimate includes losses of $100 million per year from computer crime (approximately 1/400 of all white collar crime).

In conclusion, the literature search regarding sources of EFT crime and contacts with people in the public and private sector around the country have shown that some data are available, but the data are very limited and do not provide either a one-time or an ongoing source to measure the extent and nature of EFT crime.

5.3 PROSPECTS FOR MEASUREMENT USING EXISTING SOURCES

At the beginning of this section three questions were outlined which arise in reviewing the available sources of data related to EFT crime: (1) Are there any specific

numbers concerning the nature and extent of EFT crime? (2) Is the data source reliable, or in other words, does it have any statistical validity? and (3) Will any of the information provide an ongoing, accurate source for the future?

Unfortunately, the answer to all three questions is essentially no. Several sources do provide specific numbers concerning the nature of EFT crime. Perhaps the two strongest are the SRI file on computer abuse and the study carried out by the American Institute of Certified Public Accountants (AICPA). However, as previously discussed, neither of these sources have gathered information using a statistically valid sampling procedure, neither provide data regarding the extent of EFT crime, and neither are collected on an ongoing basis nor could be utilized to examine EFT crime over time.

Data collected by regulators of financial institutions or by the FBI do have the potential to provide an ongoing source of information regarding the nature and extent of EFT crime. However, neither the financial regulators nor the FBI are gathering or maintaining any records of this type at present. Further, it would not only require new forms and procedures for data collection to do so, but also a revision in philosophy and approach. Designing a set of forms and procedures to collect such data is relatively straightforward, but changes in philosophy and approach are far more difficult to achieve.

Of all of the sources, the FBI probably has the greatest potential to eventually collect relatively good information concerning the nature and extent of computer crimes crime involving financial institutions. However, it is doubtful that such an effort will occur in the near future, especially without a law passed by Congress making computer crimes a federal offense. However, even if a new law was established, and if procedures were implemented to gather information on EFT or computer crimes, it is still very unlikely that the information would be available from the FBI on a widespread basis.

If information is to be gathered on the nature and extent of EFT crimes, new approaches will need to be developed. PSE has begun to develop several alternatives, and these are discussed in the following chapter.

6 ESTIMATING THE EXTENT OF EFT CRIME

While previous chapters of this report addressed the nature of EFT crime, this chapter considers its extent or level. However, before considering approaches to measure the extent of EFT crime, some critical issues affecting the extent of criminal activity in EFT should be considered. These issues--briefly discussed in the first section of the chapter--constitute an appropriate framework for viewing the relevance and potential of each approach. When the project began, PSE intended to explicitly derive an estimate of the EFT crime problem within the scope of the study. Unfortunately, as discussed in Chapter 5, the available data preclude us from making a statistically significant estimate at this time. In particular, in an initial working paper [Tien et. al., 1981], we proposed an approach which could have provided an estimate by comparing data from different sources. Despite the fact that this comparative approach was not applied due to data limitations, we discuss it in the second section of the chapter because it is a relatively inexpensive method which could potentially still be applied to the EFT area--provided the pertinent data become available--or to any other area where a quick estimate of, say, the crime problem is desired.

Given our inability to arrive at an estimate of the extent of EFT crime at this time, we propose a second, or alternative, measurement approach--the development of a panel or sample of U.S. banks which would provide a consistent set of data that could be employed to derive an estimate of the EFT crime problem. The "panel approach" is detailed in the third section, while the the concluding section discusses a preliminary test of the panel concept and its implications for implementing such a panel or naticnal sample.

Finally, it should be stated that although the statistical estimation approaches proposed in this chapter are in general quite involved and highly mathematical, they are presented herein with a minimum of technical jargon. It is our intent to familiarize both technical and nontechnical EFT experts with two potentially applicable approaches,* so that they may assist in any future application of either

---

*It should be noted that although these two approaches for estimating the extent of EFT crime are not the only possible methods (in fact, in the earlier working paper [Tien, et. al., 1981], we considered some parametric methods), they are potentially the most applicable, given our current state of knowledge about EFT crime.

approach. Technical details remain, of course, to be worked out in any specific application.

6.1 SOME CRITICAL ISSUES

In any determination of the extent of criminal activity in EFT, five critical issues must be considered: the first two--the developing technology and the proliferating demand--relate to the electronic or computer aspect of the problem, while the latter three--the evolving definition, the intricate detection, and the chronic underreporting--relate to the crime aspect.

Developing Technology

The underlying computer technology of EFT is developing at a tremendous pace, resulting in a decrease in computer costs and a simultaneous increase in computing capabilities. Efficient memory media, device miniaturization and distributed processing are three primary reasons for this amazing development. In terms of both cost and performance, the traditional magnetic storage media--tapes, disks and drums--are now challenged by two new solid-state technologies: charge-coupled silicon devices and magnetic bubble memories. These memory devices will, for example, have much faster access times than floppy disks--the current storage medium for microcomputers. In addition, the ability to handle 32 bits of data information--which is equal to the handling capacity of today's large mainframes but twice as much as today's most powerful microprocessor--will very soon change the microprocessor to a micromainframe.

The miniaturization of devices, begun less than a dozen years ago, was initially small-scale in scope: 10 devices were placed or integrated on a single semiconductor chip. This soon led to medium-scale integration with up to 100 devices per chip. Further advances in solid-state technology resulted in large-scale integration with up to 1,000 devices per chip, which heralded the age of microcomputers. Today, very large-scale integration is allowing 100,000 devices per chip--thus contributing to a new age in microcomputers, in which the micromainframe might be based on three semiconductor chips. In the future, it is anticipated that some 450,000 devices could be placed on a single chip.

Distributed processing and computer networking have allowed EFT activities to be decentralized and yet coordinated. In a distributed system, the data communication and data base management functions are performed by a number

of small computers that are physically connected by high speed transmission lines. The data base can also be organizationally and spatially distributed which has advantages for flexibility, management and privacy.

The developing computer technology of course affects and changes EFT use patterns,* thus making any estimate of the EFT crime problem unstable. An estimate of the size of today's crime problem can not be reliably updated to reflect future conditions without knowledge of these conditions and a model of their crime-related impacts. Unfortunately, the technology is changing so fast that "at least half of the applications that will exist in 5 or 10 years, we can't even imagine today" [Vadasz, 1981].

Proliferating Demand

A companion issue to the above developing technology concern is the anticipated proliferation and growth in the demand for EFT services; this latter issue would not only cause an instability in the estimate of the potential crime problem but also a difficulty in the identification of a valid estimation technique.

As reviewed in the following section, most available techniques for estimating hidden populations are based on the assumption of a "closed population." (A population whose size changes over time is referred to as "open," while a population whose size remains constant is said to be "closed.") Except for some special cases in reliability theory, most populations are not closed. In fact, as alluded to above, the extent of EFT criminal activity is likely to grow at least as fast as the EFT industry itself. Taking into consideration the non-constancy or openness of the underlying criminal activity or population growth results in an added realism that greatly complicates the estimation analysis. The complication cannot be easily dismissed: it fundamentally changes the character of the problem and must necessarily decrease our confidence in the resultant estimate.

---

*For example, although the magnetic stripe on the back of plastic credit cards was picked only a few years ago as the industry standard for storing the data identifying the account, the magnetic storage device is threatened with obsolescence. On the horizon are cards with integrated circuit chips embedded in them for storing information and updating cards each time they are used.

Evolving Definition

What constitutes a computer-based--or more specifically, an EFT--crime? As mentioned in Chapter 4, the manner in which one defines or classifies EFT crimes is dictated by the purpose or intended use of the resultant classification scheme. For example, if one were interested in crime prevention, then the most appropriate scheme would be based on characteristics of the modus operandi. On the other hand, if one were interested in criminal sanctions, then the classification scheme should be in legal terms. In this vein, the proposed Federal Computer Systems Protection Act of 1978 (i.e., Senate Bill 240) was introduced to make the use of a computer, under certain circumstances, a felony offense. Unfortunately, the Act focuses primarily on software-related abuses committed by individuals, while the stiff penalties specified in the Act were based in part on reports of large losses caused by management-related abuse and alleged organized crime [Campbell-Klein, 1980].

Although our layered definition of EFT crime--from hardware-based crime to related crime--presented in Chapter 4 is quite robust, it should be noted here that any definition or classification scheme must of necessity be flexible so that it takes into consideration the developing computer technology which, as stated earlier, would affect the EFT use pattern. This evolving definition of computer crime would obviously affect any estimation of its level.

Intricate Detection

While the computer can prevent, and in some cases provide a detailed audit trail for a simple fraud attempt, it can also be programmed to obstruct the detection of a sophisticated criminal act or to outrightly expunge the records of any illegal transaction. In theory, even the intricacies or difficulties in detecting a computer crime would not present a problem in estimation if the nature of the crime and the detection processes were adequately known. For example, if it can be assumed that the time x between crime incidence and expunging attempt is a random variable, then the probability distribution of x might be amenable to estimation. Similarly, one might be able to estimate the probability distribution of y, the time between crime incidence and crime detection. The chance, then, that a crime will remain undetected because of expunging is simply the probability that y exceeds x, an easy quantity to compute given the probability distributions for x and y.

Unfortunately, the underlying crime and detection processes are not known. Whatever its imperfections, this

estimate on crime detection has strong statistical implications. Suppose that because of a marginal improvement in surveillance, a computer swindler's chance of escaping detection drops slightly, from 99 in 100 to 97 in 100. Then, assuming the number of such offenses and the reporting rate for those detected remain constant, the reported rate will shoot up by a factor of three! In other words, we are at a stage at which all estimates about the size of the computer crime problem are subject to great instability.

Chronic Underreporting

In estimating the extent of crimes in general, the well publicized National Crime Panel surveys have served to highlight the fact that actual crime levels may be up to several times the reported levels. For example, although homocide is nearly always reported, larceny is typically very much underreported.

In the case of EFT crimes, we would also expect an underreporting phenomenon. In fact, we would expect an even more severe phenomenon since, as stated earlier, computer crimes are considered to be "white-collar" in nature. Financial institutions, for example, are concerned about their image and may be quite hesitant about reporting a fraudulent act, especially if the loss is below a certain figure. Again, if the degree of underreporting is known, then appropriate statistical techniques can be employed to correct for it. As a simple example, if 25 percent of confidentially-queried institutions indicate they would report a fraud of less than $5,000 and 50 percent indicate they would report a fraud of more than $5,000, it would be sensible to correct for underreporting by multiplying the number of known frauds of $5,000 or less by four and those greater than $5,000 by two.

6.2 A COMPARATIVE APPROACH

As mentioned earlier, at the outset of this study we were informed about the existence of several overlapping and presumably equivalent sources of data on EFT crime. We had hoped to compare two or more of these sources and--by employing a modified version of the "capture-recapture" statistical technique--to estimate the EFT crime problem. However, as discussed in Chapter 5, the available sources have serious problems as statistically valid and consistent information bases, rendering them inappropriate for a comparative estimation analysis. Nevertheless, it is still worthwhile to consider the capture-recapture technique and to discuss its potential application to EFT.

The notion of capture-recapture is central to many wildlife studies [Feller, 1968; Fienberg, 1972; Seber, 1973; Burnham and Overton, 1978]. The basic idea is simple: a sample of the population is captured, tagged in some suitable fashion, and then released. Subsequently, a second sample of the same population (now containing both tagged and untagged specimens) is obtained and tagged appropriately. The single capture-recapture step stops when the second sample is obtained, while the multiple-recapture series is based on obtaining three or more samples. The single and multiple capture-recapture methods are described in turn below, followed by a discussion of their potential application to measuring the extent of EFT crimes.

Capture-Recapture

In the case of a single capture-recapture step, the fraction of the second sample which has been previously tagged is used to estimate the total population size. Specifically, letting

n_1 = number of specimens in the first sample,

n_2 = number of specimens in the second sample,

T_2 = number of tagged specimens in the second sample,

$\hat{N}$ = estimate of the total population,

and if it can be assumed that in the second sample the tagged specimens are no more likely to be captured than untagged specimens, then the "best" estimate of the total population size is given by:

$$\frac{n_1}{\hat{N}} = \frac{T_2}{n_2} \text{ or } \hat{N} = \frac{n_1 n_2}{T_2}$$

The above estimate for N is quite reasonable under the assumptions we have made; we would "expect" that the fraction of tagged specimens in the second sample would be approximately equal to the fraction of tagged specimens in the entire population.

This example illustrated the basic idea behind capture-recapture methods with a simple model--technically, the univariate hypergeometric model. In most practical applications, however, a more complicated model is used along with a more elaborate sampling procedure. In the next section, we consider population estimates based on multiple-recapture.

Multiple-Recapture

Multiple-recapture is an estimation procedure that involves more than two samples of the population. In multiple-recapture, a specimen is given a unique tag each time it appears in a sample; so, for instance, if four samples were taken and a specimen were captured on the first and third then its label might be (1212), where "1" denotes captured and "2" denotes not captured. In this example, those elements in the hidden (i.e., noncaptured or missing) population would have the label (2222).

The underlying probability model most commonly used in conjunction with a multiple-recapture census is the multinomial distribution. In simple terms, the multinomial distribution assumes that the world is divided into k distinct cells and that the probability that a randomly chosen sample point falls into a cell j is p_j. When used with multiple-recapture, the unique "cell" into which a specimen is placed is identified by the tags on the specimen. Thus, under a multinomial model the above stated specimen would be placed in cell (1212).

Data gathered through a multiple-recapture census are most commonly presented in the form of a so-called contingency table. For example, in considering again the simple case of two data samples, let

x_{11} = number of elements appearing in both samples,

x_{12} = number of elements appearing in sample one but not in sample two,

x_{21} = number of elements appearing in sample two but not in sample one,

x_{22} = number of elements appearing in neither sample.

Schematically, the variables can be presented in tabular form as shown below. Here, x_{22} is the hidden population that we

	Second Sample	
First Sample	Present	Absent
Present	x_{11}	x_{12}
Absent	x_{21}	x_{22}

seek to estimate. Further, in keeping with our multinomial model, the probabilities P_{11}, P_{12}, P_{21}, and P_{22} can be assigned to the four cells, respectively. If we assume that

the two samples are independent, which is to say that, as before, a tagged specimen has the same chance of being captured as an untagged specimen, then the "best" estimate of the population size is given by

$$\hat{N} = \frac{(x_{11}+x_{21})(x_{11}+x_{12})}{x_{11}}$$

which can be shown to be equivalent to the $\hat{N}$ stated earlier. When more than two samples are employed or when samples are dependent, the details of the estimate become more complicated, but the basic concept described above remains unchanged.

In general, multinomial models require that $P_j = P_j(\theta)$; that is, each cell probability must be a function of a reduced set of parameters. For if there are no constraints on the P_j or N (the population), then all inferences about N which satisfy $N \geq n$ (where n is the size of the sample actually observed) are equally reasonable [Sanathanan, 1972]. This is obviously not an acceptable state of affairs when one is forced to choose a particular estimate N of N.

There are several ways of restricting the P_j to eliminate the above condition, and each carries an implicit set of assumptions about the mechanics of the multiple-recapture census. For instance, the independence assumption invoked in the previous sample has the following parametric representation. If θ_i = probability that a randomly chosen element is in sample i (i=1,2), then under the independence assumption,

$$P_{11} = \theta_1\theta_2 \qquad P_{12} = \theta_1(1-\theta_2)$$

$$P_{21} = (1-\theta_1)\theta_2 \qquad P_{22} = (1-\theta_1)(1-\theta_2)$$

Note that the original three parameters (P_{11}, P_{12}, P_{21})* have all been expressed in terms of two parameters (θ_1 and θ_2).

The parametric representation mentioned above is a special case of a log-linear model [Fienberg, 1972; Bishop, et. al., 1975], so called because the log of the cell probabilities is represented as a linear function of a set of suitably defined parameters. Log-linear models are flexible enough to provide estimates of N in situations where there is dependence between the various samples of the multiple-

*There are only three parameters since P_{11}, P_{12}, and P_{21} determine P_{22} since $P_{22} = 1 - (P_{11}+P_{12}+P_{21})$.

recapture census. Such dependence could arise in a criminal justice setting if, say, among equally active criminals those with long police records (i.e., previous captures) are more vulnerable to apprehension (i.e., recapture) than those who are unknown to the police.

Application Issues

How can a single capture-recapture or a multiple-recapture method be applied to determine the extent of criminal activity in the EFT area? The application is obvious if one considers the multiple-recapture series as a set of independent and equivalent lists, files or sources of information on EFT crimes. Thus, the lists are compared to cdentify crimes which are contained in one or more lists and to estimate the missing or hidden population of crimes.

There are, of course, several issues or problems to consider in such an application; that is, the underlying multiple-recapture assumptions place certain restrictions on the manner in which the lists are compiled. First, the lists must contain explicit and distinctive information about the crimes so that the matching of crimes across different lists can be accomplished. This may be a problem if one or more of the lists are confidential and the obvious crime identifiers have been deleted. In such a case, one might ask the agencies in question to undertake the actual matching task and then to provide a summary of the resultant matches.

Second, the lists must be compiled independent of each other. This is a very critical assumption, and it must be validated before a capture-recapture or multiple-recapture analysis can be undertaken. Should there be dependence among two lists (as, for example, in the case where one list has copied certain contents of another), it should be clearly identified and corrected, if possible. For example, if a national list of EFT crimes has assembled all the crimes occuring during a specific period of time from the contents of another list, then the two lists should not be compared, at least for the time period in question.

Third, although it has been stated that the lists should be equivalent (in the sense that they are focused on the same population), one could relax this requirement and use ad hoc procedures to compensate for the lack of equivalency, assuming, of course, that there is at least a certain degree of overlap among the lists. For example, crime statistics for New England (i.e., population one) may be available at one time, while at a later time we may be presented with crime data on northeastern cities (i.e., population two). When we have a good estimate of the overlap percentages (call

them P_1 and P_2), then the estimate $\hat{N}$ can be easily derived as follows. If we let

P_1 = percentage of population one contained in population two,

P_2 = percentage of population two contained in population one,

n_1 = number of elements in the first sample,

n_2 = number of elements in the second sample,

T_2 = number of tagged elements in the second sample,

$\hat{N}_i$ = estimate of the i^{th} population (i=1,2),

then

$$\hat{N}_2 = \frac{P_1 n_1 n_2}{T_2} \quad \text{and} \quad \hat{N}_1 = \frac{P_2 n_1 n_2}{T_2}$$

The success of this derivation is of course highly dependent on how well we know P_1 and P_2.

Fourth, one of the key assumptions underlying multiple-recapture is that the elements of the population are all equally likely to have the same capture history. In the case of the multinomial model this amounts to asserting that all elements in the population "experience" the same cell probabilities. This assumption is certainly open to question, and, in fact, in many instances it is a distortion of reality. One might anticipate, for example, that the capture history of crimes onto the various lists might be time dependent, with the most recent crimes being perhaps more likely to be captured and listed. The means available for correcting this flaw range from the exotic to the mundane. In the former category is the generalized jacknife estimator proposed by Burnham and Overton [1978]; since this method is highly specialized to wildlife studies, we will pass over it here. Another more attractive approach to resolving this issue is simply to partition the population into homogeneous subgroupings, estimate the size of each subgroup, and then aggregate the estimates. In the example above, this approach would involve estimating the size of the criminal population by time period and then adding up the number of criminals in the different time periods.

Fifth, a final potential issue concerns the fact that capture-recapture methods are based on a closed population. Interestingly, although, as stated in the first section, the

EFT crime population is certainly open and unstable over time, the identified crime lists are, for the most part, based on a closed population. That is, the lists are typically not compiled over time, but are compiled simultaneously and focus on the same crime population. Should the lists, however, be compiled at different points in time, there may be some instability questions (e.g., more recent crime detection methods may reveal more crimes, even past crimes); in such a case, we recommend partitioning the estimation problem and employing modeling techniques to describe and correct for the underlying instability.

In conclusion and once again, the available data sources do not provide lists of EFT crimes that are amenable to a capture-recapture analysis: more specifically, the available lists are--for the most part--not detailed enough, not independently compiled, and not equivalent. Specifically, we had hoped to be able to take the SRI and AICPA lists and compare them using capture-recapture techniques. However, these sources do not lend themselves to this type of analysis for the reasons discussed in Chapter 5. It is still possible, of course, that if in time two or more lists of EFT crimes are developed that can be compared, then the capture-recapture technique can be applied to yield a straightforward estimate of the underlying crime problem.

6.3 A PANEL APPROACH

After a thorough analysis of the available information concerning the nature and extent of EFT crime, and given the dearth of appropriate data, PSE proposes that a consistent set of relevant data be collected by a panel or sample of U.S. financial institutions. This is one of the primary recommendations of this report. In much the same manner that A.C. Nielsen Co. rates television programs based on data collected from a national panel of some 1200 households, it is possible to estimate the EFT crime problem based on data collected by the proposed EFT crime panel. A limited, but representative, sample of financial institutions would be selected to participate in the panel. Data would be gathered using special collection instruments on an ongoing basis, although analysis of the data would take place for a prescribed period, such as every year. The panel stratification, underlying model, and sample size are discussed in the following sections.

Panel Stratification

In establishing a panel, it is obvious that it should be representative of the universe of U.S. financial

institutions. To assure this representativeness, the panel should be stratified. Along how many dimensions should the stratification occur? It is our opinion that the panel should at a minimum be stratified to reflect the types of institutions, geographic distribution, and range of asset sizes.

However, if asset size is implicitly taken into consideration in the underlying model of the panel, then we need only consider the type and location dimensions. More specifically, in an attempt to minimize the number of distinct categories or cells in the stratified panel, we propose to group all institutions into two types (i.e., commercial banks and thrift institutions)* and three locations (i.e., east, central and west). Thus, as depicted in Exhibit 6-1, we propose a stratified EFT crime panel with six cells. It is recognized, however, that other dimensions could also be used to stratify the panel. Type and location were chosen because national statistics for these characteristics are readily attainable, while data for others such as the number of EFT transaction are not.

Panel Model

To determine the number and composition of institutions that should be selected for the panel from each one of the six cells, it is necessary that we develop a model which describes the underlying process. In this chapter, an initial model is developed for extrapolating an estimate of the magnitude of the problem nationwide from the data provided by the proposed panel institutions. We stress the word "initial"; it is the very nature of statistical modeling that one must forever be vigilant that the results of an analysis do not contradict the assumptions used to obtain them, and that one must accompany statistical rigor with the flexibility to respond to unexpected contingencies.

Our underlying model is based on the following two assumptions:

(1) The number of reported EFT crimes in a given institution over a fixed period follows a Poisson probability distribution.

Under this assumption, the probability of institution i having exactly x_i reported crimes in a fixed period (say, one year) is equal to

*The category of thrift institutions includes savings and loan associations and mutual savings banks.

Exhibit 6-1

A Stratified EFT Crime Panel with Six Cells

	EAST	CENTRAL	WEST	TOTAL
Commercial Banks [1]	Commercial East (CE)	Commercial Central (CC)	Commercial West (CW)	
Number	3,037	10,305	1,366	14,708
Assets ($Millions)	$575,984	$592,625	$255,196	$1,423,805
Average Assets ($Millions)	$189.7	$57.5	$186.8	$96.8
Thrift Institutions [2]	Thrift East (TE)	Thrift Central (TC)	Thrift West (TW)	
Number	2,214	2,380	461	5,055
Assets ($Millions)	$348,098	$255,759	$175,476	$779,333
Average Assets ($Millions)	$155.3	$107.5	$380.6	$154.2
Total				
Number	5,251	12,685	1,827	19,763
Assets ($Millions)	$924 082	$848,384	$430,672	$2,203,138
Average Assets ($ Millions)	$176.0	$66.9	$235 7	$111.4

[1] Source: [Federal Reserve Bank, 1979]
[2] Source: [National Association of Mutual Savings Banks, 1978; U.S. League of Savings Associations, 1980]

$$P(x_i) = \frac{\theta_i^{x_i} e^{-\theta_i}}{x_i!}, \quad x_i = 0,1,2... \qquad (6.1)$$

where θ_i can be easily shown to be the expected or average number of reported crimes for institution i in, say, a year. Of course, θ_i would not be known in advance; its estimation is a central part of the exercise. We would start with the Poisson distribution because it is the standard distribution for describing the fluctuating pattern of events that arise randomly and unpredictably and that can be thought of as independent.

(2) The Poisson parameter θ corresponding to institution i is directly proportional to A_i, the asset level of that institution.

That is,

$$\theta_i = (A_i/A_1)\theta_1 = K_i\theta_1, \qquad (6.2)$$

where $K_i = A_i/A_1$, $i = 1,2,...,N$.

In other words, we begin by assuming that the N institutions in the same location or region and of the same type experience roughly the same rate of EFT crime per million dollars in assets. While the data we gather might lead us to modify this assumption (and replace it with some empirically supported counterpart), it does not clash with one's intuition prior to developing expertise on the problem. Another reason for this assumption is that asset size is a more readily available data element than, say, number of EFT transactions. Exhibit 6-2 categorizes, for example, commercial banks by four asset sizes and three locations, in a manner that would be appropriate for establishing a panel to collect consumer EFT crime data.

Given the above two assumptions, the estimation of the level of EFT crime is straightforward. Suppose $(x_1,x_2,....,x_N)$ are the observed numbers of EFT crimes in, say, a year in the N institutions; for simplicity, assume that the A_i's are in ascending order (i.e., the first institution is smallest, etc.). The probability of achieving the observed result is:

$$P(x_1,..., x_N) = \frac{\theta_1^{x_1} e^{-\theta_1}}{x_1!} \cdot \frac{\theta_2^{x_2} e^{-\theta_2}}{x_2!} \cdots \frac{\theta_N^{x_N} e^{-\theta_N}}{x_N!}$$

Exhibit 6-2

Commercial Banks By Asset Size and By Location[1]

	EAST	CENTRAL	WEST	TOTAL
Under $50 Million				
Number	1,817	8,096	1,112	11,025
Assets ($Millions)	$41,804	$160,472	$19,214	$221,490
Average Assets ($Millions)	$23.0	$19.8	$17.3	$20.1
$50-300 Million				
Number	850	2,009	269	3,128
Assets ($Millions)	$91.478	$188,358	$29,134	$308,970
Average Assets ($Millions)	$107.6	$93.8	$108.3	$98.8
$300-1,000 Million				
Number	153	158	45	356
Assets ($Millions)	$80,414	$78,042	$25,433	$188,889
Average Assets ($Millions)	$525.6	$493.9	$565.2	$516.5
Over $1,000 Million				
Number	91	73	30	194
Assets ($Millions)	$617,963	$249,931	$268,968	$1,136,862
Average Assets ($Millions)	$6,790.8	$3,424.7	$8,965.6	$5,860.1
Total[2]				
Number	2,911	10,336	1,456	14,703
Assets ($Millions)	$831,659	$676,803	$342,749	$1,851,211
Average Assets ($Millions)	$285.7	$65.5	$235.2	$125.9

[1]Source: [FDIC, 1980].

[2]The "Total" row is slightly different than that in Exhibit 6-1 because of different sources--also, the source dates differ.

$$= B\theta_1^{\sum_{i=1}^{N} x_i} e^{-\theta_1 \sum_{i=1}^{N} K_i} \qquad (6.3)$$

where

$$B = \frac{K_1^{x_1} K_2^{x_2} \cdots K_N^{x_N}}{x_1! x_2! \cdots x_N!} \qquad (6.4)$$

is a numerical constant that is not a function of θ_1.

From (6.2), one can obtain the maximum-likelihood estimate of θ_1 (i.e., the numerical value for θ_1 under which the observed result would have the highest probability of arising). The equation for the estimate θ_1 is:

$$\hat{\theta}_1 = \sum_{i=1}^{N} x_i / \sum_{i=1}^{N} K_i \qquad (6.5)$$

Once θ_1 is estimated, the parameters for the other banks follow from (6.2):

$$\hat{\theta}_i = K_i \hat{\theta}_1, \quad i=1,2,\ldots,N \qquad (6.6)$$

As anticipated, the expected or average value of $\hat{\theta}_1$ is equal to the true value θ_1; that is,

$$E(\hat{\theta}_1) = \theta_1 \qquad (6.7)$$

Furthermore, the estimate of the variance of $\hat{\theta}_1$ around the true value θ_1 is given by

$$\hat{V}(\hat{\theta}_1) = \hat{\theta}_1 / \sum_{i=1}^{N} K_i \qquad (6.8)$$

and the estimate of the standard deviation is given by

$$\hat{S}(\hat{\theta}_1) = (\hat{\theta}_1 / \sum_{i=1}^{N} K_i)^{1/2} \qquad (6.9)$$

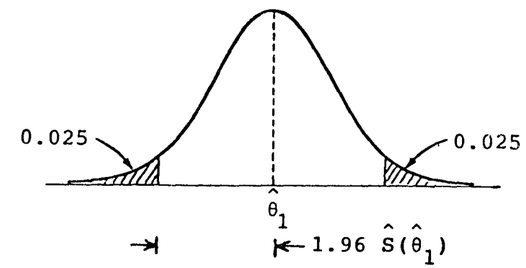
In order to apply a 0.95 confidence interval to the estimation of θ_1 (i.e., range centered at θ_1 that should contain the true value θ_1 with a probability of 0.95), it is necessary to develop a probability density function for θ_1. Combining (6.5) with (6.1), we can see that θ_1 is a Poisson random variable scaled by the

$$\sum_{i=1}^{N} K_i$$

constant. In most instances, especially if the mean of the Poisson distribution is greater than 20 or N is large, θ_1 can be approximated by a normal distribution, in which case, as illustrated in Exhibit 6-3 below,

Exhibit 6-3

Normal Approximation for $\hat{\theta}_1$



the 0.95 confidence interval for θ_1 can be stated as:

$$\hat{\theta}_1 \pm 1.96\ \hat{S}(\hat{\theta}_1) = \hat{\theta}_1 \pm 1.96(\hat{\theta}_1 / \sum_{i=1}^{N} K_i) \qquad (6.10)$$

Furthermore, if the total assets of all N banks in cell c is A_c, then the 0.95 confidence interval for θ_c, the number of EFT crimes for all N banks in cell c, is:

$$(A_c/A_1)\hat{\theta}_1 \pm (A_c/A_1)1.96(\hat{\theta}_1 / \sum_{i=1}^{N} K_i) \qquad (6.11)$$

In reviewing (6.11), two important facts should be borne in mind. First, the quantity

$$\sum_{i=1}^{N} K_i$$

affects the precision or accuracy of the estimate: either a large N and/or large values for K_i would improve the accuracy. In fact, assuming θ_1 remains unchanged, a sample of one institution of a very large asset size would yield just as accurate a result as a sample of N, N>1,

institutions of smaller asset sizes; however, we would strongly recommend that, at least initially, a sample or panel of several institutions with different asset levels be constituted so that the two basic assumptions (i.e., (6.1) and (6.2)) can be validated. If the assumptions prove untenable, then, as mentioned earlier, the underlying statistical model for the EFT crime panel would have to be modified.

Second, the estimate $\hat{\theta}_1$ refers to the number of reported EFT crimes, which as discussed earlier is presumably only a subset of the total. One could try to incorporate the phenomenon of underreporting by introducing the parameter P, the probability a given EFT crime will actually be detected and reported by a panel bank. Because a binomial process (i.e., a crime either is detected and reported or it is not) is superimposed on a Poisson process, certain theorems about probability tell us that the final process (i.e., reported crimes) is still Poisson and all the above results would prevail with the exception that θ_1 is replaced by θ_1/P. For example, (6.11) would become:

$$\theta_C = (A_C/A_1)\hat{\theta}_1/P \pm (A_C/A_1)1.96(\hat{\theta}_1/P\sum_{i=1}^{N} K_i)^{1/2} \qquad (6.12)$$

In sum, since P is typically much less than one, our estimate of the crime level would increase by a (1/P) factor while our accuracy would decrease by a $(P^{1/2})$ factor.

Panel Size

In order to determine the "best" size of the proposed EFT crime panel from the previous modeling effort, it is necessary that we have an estimate of the average number of EFT crimes per $1 million of assets per year for each of the six cells identified in Exhibit 6-1. Based on the preliminary data collection effort we found a rate of reported ATM crimes of 0.09 per $1 million of assets per year at a central (i.e., midwestern) commercial bank, and a rate of 0.06 per $1 million of assets at a western commercial bank. Using the 0.09 figure and the information contained in Exhibit 6-2 for the "commercial central" cell, we have undertaken some sample calculations of (6.11) in Exhibit 6-4. The results in Exhibit 6-4 clearly show that by increasing the cell size from 4 to 8 banks we are able to improve our accuracy by a factor of 10.1/7.2 = 1.4. Once again, although our accuracy is not tremendously improved, we would recommend a larger cell size, at least initially, in order to validate the basic assumptions of the model.

Exhibit 6-4

Sample Calculation for "Commercial Central" Cell

Asset Category i	A_i, Average Asset Size ($Million)	$K_i' = A_i/A_1$	Number of Banks	Total Asset Size ($Million)	Assuming N=4 Banks in Cell: N_i, Number of Banks in Cell	Assuming N=4: $K_i = K_i' N_i$	Assuming N=4: x_i	Assuming N=8 Banks in Cell: N_i, Number of Banks in Cell	Assuming N=8: $K_i = K_i' N_i$	Assuming N=8: x_i
1	$ 19.8	1.00	8,096	$160,472	1	1.00	1.78	2	2.00	3.56
2	$ 93.8	4.74	2,009	$188,358	1	4.74	8.44	2	9.48	16.88
3	$ 493.9	24.94	158	$ 78,042	1	24.94	44.45	2	49.88	88.90
4	$3,424.7	172.96	73	$249,931	1	172.96	308.22	2	345.92	616.44
	Total	—	10,336	$676,803	4	203.64	362.89	8	407.28	725.78
	Estimated Number of Reported ATM Crimes in Cell				60,912 ± (6,153 or 10.1%)			60,912 ± (4,444 or 7.2%)		

[1] x_i is the expected or average number of EFT crimes occurring in all panel banks in asset category i. Using a rate of reported automatic teller machine (ATM) crimes of 0.09 per $1 Million of assets per year, x_i = 0.09(Average Asset Size)(Number of Banks in Cell).

The method just illustrated could be used separately in each of the six disjoint cells of the proposed EFT crime panel. One would simply add the various estimates together to estimate the national level of reported EFT crimes. Because the random errors associated with the six individual cells tend, to some extent, to cancel one another (e.g,. it is highly unlikely that fluctuations lead to overestimates in all 6 cells), an estimate of the national total is expected to be more, not less, accurate than the individual numbers added to achieve them. If, for example, each of the six cells yields estimates with uncertainty levels of 10.1 percent, then, if the various estimates are of roughly the same order-of-magnitude, the uncertainty level of the national estimate is only $(10.1/6^{1/2})$ or 4.1 percent.

Since we have shown in Exhibit 6-4 that we are able to achieve an uncertainly level of 10.1 percent in the "commercial central" cell with only 4 banks in that cell, it seems reasonable, at least from an accuracy perspective, to have a national panel of 24 (i.e, 4 times 6) institutions yielding an overall uncertainty level of 4.1 percent. However, because of the assumption validation reason stated earlier we suggest a much larger panel size of perhaps 50 institutions. A panel of this size would also provide reasonable accuracy levels for each one of the six cells, which may each be a focus of interest not only in terms of its contribution to the total picture but also for itself.

Although we cannot overemphasize the importance of validating the model assumptions, it should be noted that the panel approach would remain valid even if our current model of the underlying process is problematic, in which case we could easily modify the model to take into consideration the more realistic conditions. We would simply reiterate that the panel data would allow testing the key assumptions of the model and, should the assumptions prove demonstratably false, indicate those modifications of the model that would be necessary. Exploratory data analysis of the kind we are discussing is not circular reasoning or an ad hoc approach, but rather an accepted and highly-developed branch of modern statistics. We are confident that the panel data would yield a statistically defensible estimate of the level of EFT crime; given the fact that the technology itself is still evolving and even exact figures would quickly obsolesce, we doubt that one should even strive for more at this time.

Finally, we would also recommend that 20 percent of the national panel be systematically replaced each year. This would allow for the changing EFT environment to be better reflected in the panel, as well as to sensitize more financial institutions to the EFT crime problem. In fact, if

the institutions which are rotated out of the formal panel continue to collect and share their crime data, then the panel would in effect be enlarged and the larger data set would yield even more accurate estimates of the EFT crime problem.

6.4 A PRELIMINARY TEST OF THE PANEL APPROACH

The preceding discussion has provided the statistical basis for one approach to measure the nature and extent of EFT crime--a national panel of financial institutions. However, given this analytical framework, a question remains: Can such an approach be implemented in the "real world?" More specifically, one must ask: Are data on EFT crimes compiled by financial institutions? Will financial institutions participate in such a national panel? Can such data provide meaningful insights about the nature and extent of EFT crime?

To explore these questions, a preliminary data collection effort was undertaken, as part of this study, to test the feasibility of the panel approach. Although we originally set out to contact only 2 to 3 institutions, in an effort to include both small and large institutions from the a variety of geographic regions in the United States, site visits were ultimately made to six financial institutions.* Working with the managers of various EFT services, we discussed the type of information available on EFT use and crimes. The operation of each bank's EFT system was reviewed and, where possible, the forms and procedures used to investigate EFT crimes were discussed. The three categories of EFT crimes and operations--consumer, corporate, and internal--were used to direct the focus of the interviews and information gathering.

As a result of these site visits, we decided to try to collect data from three institutions. Preliminary consumer EFT crime data--in the form of ATM disputes and complaints--

---

*In order to protect the confidentiality of the institutions and the information gathered by PSE, the names of the six institutions are not mentioned in this report. However, they did represent a range in terms of geographic distribution and asset size (although all of them tended to be larger institutions.) The amount of information obtained in the site visits varied, with some of the institutions being very open and cooperative and others somewhat more guarded in their response.

were collected at two institutions, and preliminary corporate EFT crime data--in the form of wire transfer losses--were collected at one institution. As part of the negotiations allowing us to collect and analyze the data, PSE agreed that the identity of the three participating institutions would remain confidential. Nonetheless, their participation in the study is acknowledged and appreciated.

The overall conclusion from the site visits and data collection is that it is feasible to collect data on the incidence of EFT crimes from financial institutions, especially in the area of consumer EFT crimes. Frauds and misuses stemming from EFT services are routinely investigated and recorded by financial institutions. In addition, baseline data for overall EFT transactions can be retrieved with relative ease. More importantly, at least some financial institutions would release this information, if appropriate safeguards for anonymity and confidentiality are implemented and the need and value of the data are established. However, although data on consumer and corporate EFT crimes are available and retrievable, it appears that it will be difficult to collect data on internal EFT crimes. None of the institutions we visited reported that it had experienced any incidents of internal EFT crime. Most also indicated that even if they had experienced such incidents, they would not readily release the files.

In the discussion that follows four topics will be covered related to the preliminary test of the panel approach. First, the collection procedures for both consumer and corporate EFT crime data are reviewed, and second, issues raised during the limited data effort are identified. Third, some hypotheses about the nature and extent of ATM and wire transfer crimes are noted based on the data collection effort, although the information gathered is not included at this time because of its preliminary nature. Finally, the section concludes by examining the implications this experience holds for implementing a national project to measure EFT crime through the panel or survey approach.

Data Collection Procedures

The data for EFT crimes were collected during site visits (generally a week in duration) to each institution. An initial meeting was held with the managers of the ATM or wire transfer departments to review the extent of EFT operations, outline the procedures followed when a suspected fraud or misuse case was reported, and identify the key personnel who could provide case-by-case and baseline data.

Incident-Specific Data for ATM Crimes

The first step in the data collection process (at the two sites visited) for ATM crimes was an incident-by-incident review of reported incidents. A form was designed to abstract information from the existing files that described the nature of each reported ATM crime or misuse incident. These incident-based data fell into four general categories: 1) how the incident was reported; 2) a description of the crime and loss; 3) disposition of the crime; and 4) supplementary narrative description. Exhibit 6-5 lists the specific variables collected for each category.

At one bank (Site 1) a 10 percent sample of all reported ATM crimes over a 22-month period was drawn; at the other (Site 2) all the files for the most recent 12-month period were reviewed. Three factors led to these choices: the number of years the ATM network had been in operation, the number of cases reported, and the filing system for cases.* A total of 287 cases were reviewed at the two banks. It was determined that no crime had been involved in 34 of the cases (e.g., the customer forgot he had made a transaction, the ATM did not dispense money properly, etc.), leaving a total sample of 253 ATM crime or misuse cases.

Baseline Data for Consumer EFT Crimes

As a second step in the collection process for the ATM crime data, three types of baseline data were collected from each institution: system description, overall transaction

---

*Site 1 had started its ATM operations within the last few years and was still expanding its network. Thus it was experiencing large increases in ATM use and crime reports. Because the bank had a very large number of reported ATM crimes, a 10 percent sample was used to keep the data collection manageable. As cases were filed alphabetically without regard to date, the sample was drawn from the full period ATMs had been in operation. This had the added benefit of accounting for changes due to increases in the size of the ATM network.

Site 2 had offered ATM services for several years and its patterns of ATM use and losses were fairly steady. Thus, a one-year sample would not be biased by growth. In addition, cases were filed alphabetically by year so that a single year's cases could be easily abstracted. Finally, the number of cases was not so large that a 100 percent sample would be unwieldy.

Exhibit 6-5

Incident-Specific Data for Consumer EFT Crimes: ATMs

How Incident was Reported to Financial Institution

- Type of Complaint
- Date Incident Occurred
- Date Reported to Bank
- Customer Sex

Description of Incident and Reported Value

- Modus Operandi/Reason for Complaint
- If Card Stolen, where
- Reported Value of Incident
- Number and Type of Transactions
- Type of Account
- Identity of Perpetrator: Known
  Suspected
  Unknown
- Relationship, if any, of Perpetrator to Customer or to Bank
- Was PIN revealed to Perpetrator?
- Was PIN written with or near card?
- Status of Complaint: Crime Involved
  Crime Suspected
  No Crime Involved
- Victim of Complaint: Customer
  Financial Institution
  Unknown

Disposition of the Complaint

- How Complaint was Resolved:
  Customer Credited for $____
  Customer Not Credited
  Restitution Made for $____
  Customer Dropped Complaint
  Pending
- Amount of Reg E Liability Assessed: $____
- If Not Credited, Did Customer "Appeal"?
- Legal Action: Criminal
  Small Claims
- Date of Disposition

Narrative

- Any additional information that adds to the understanding of the incident.

figures, and noncrime losses.* The background data, or system description, included the number of ATM machines, total and active card bases, the range of transactions permitted through ATMs, and the proportion of time ATMs operated offline. The transactions data included the monthly number and value of ATM withdrawals and deposits by account type, the number of balance inquiries, and the number and value of cash advances and bill or loan payments. Noncrime losses are those associated with ATM operations which were not considered fraudulent such as cash differences when an ATM is balanced or "bounced" ATM withdrawals. These baselines are an important part of the data collection process because they allow the incident-specific data to be analyzed from the perspective of all ATM transactions.

Incident-Specific and Baseline Data for Wire Transfer Crimes

Because of the extremely low incidence of wire transfer crimes reported by the participating financial institutions, we collected aggregate data for wire transfer losses and operations at one institution. These aggregate figures were for each year of a three-year period and included the number and value of losses, as well as a description of the cause (i.e., miscredited or double-credited account, unauthorized transaction) and the relationship of the suspected perpetrator (e.g., corporate customer, individual customer, not a customer). Comparable data on the number and value of all money transfers were also collected. This information is useful in identifying the criminal vulnerabilities of wire transfer operations, the nature of the loss investigations process, and the types of information available in the corporate EFT area.

Issues Raised During Data Collection

During the site visits, PSE discovered that although data on ATM and wire transfer transactions and crimes are often kept in retrievable form at financial institutions, a number of issues surrounding the mechanics of data collection will need to be addressed in establishing a national panel for data collection. These issues are identified and detailed below.

---

*In addition, aggregate figures for all ATM crimes reported over the sampled time period were collected at Site 1, to compare with the 10 percent sample. These aggregate data indicate that the 10 percent sample presented a reasonable estimate of the total number and value of ATM crimes.

Defining ATM and Wire Transfer Crimes

To precisely define an EFT crime, two questions must be answered: Was EFT involved? Was a crime committed? In Chapter 4, we defined an EFT crime as "any crime . . . that would not have occurred but for the presence of an EFT system." During the site visits we learned that financial institutions could easily determine whether a customer's complaint (the financial institutions' term for a crime) was related to EFT by identifying that the transactions in question were made at an ATM or involved wire transfers. However, it was often difficult for the investigators to determine whether a crime was involved in a reported complaint or dispute. As a consistent set of data is desired for a national survey, the definition of what constitutes an EFT crime for each type of EFT service or technology will need to be clearly stated at the outset.

In ATMs, it is often difficult for the bank to ascertain whether the disputed transactions were unauthorized. Consider, for example, the potential explanations for a customer's complaint that he did not make the $100 ATM withdrawal shown on his statement, although his transaction card is still in his possession.

- Assume the customer is truthful: someone could have obtained his code and made the withdrawal using a counterfeit card, or the transaction could have been "manufactured" internally by someone modifying the software that records ATM transactions. A more likely explanation is that a friend or relative who knew the PIN (e.g., the PIN was written down with the card, the customer told him the PIN at an earlier date) "borrowed" his card, withdrew the cash and returned the card. In the first two cases, the customer is clearly the victim of a criminal act. In the last case, it is not certain that a crime had been committed, as the customer allowed access to his account by writing or revealing his PIN. Further, the customer may know or suspect who made the withdrawal, but reported it to recover from the financial institution rather than the perpetrator. In this instance, it is uncertain whether the institution or the customer is the victim.

- Assume the customer is lying: he made the withdrawal but hopes to collect from the financial institution by misusing consumer protection laws such as Regulation E. Clearly, a different crime has been committed, and the institution is the victim.

- Assume the customer forgot he made the withdrawal: no crime was committed.

In many cases, the financial institution cannot determine whether the customer is truthful, mendacious, or forgetful, and is uncertain whether to label the complaint as a crime.

Just as it is difficult for financial institutions to determine whether a crime is actually involved in an ATM complaint, the criminal aspects of wire transfers misuses are also ambigious. In particular, financial institutions appear to be reluctant to identify a wire transfer loss as a crime unless a perpetrator intentionally sets out to fraud the institution by compromising or circumventing its safeguards for preventing unauthorized wire transfers. However, occasionally, an error may create the opportunity for misuse. For example, a wire transfer may be credited to the wrong account, or an account may be inadvertently credited twice for the same payment. In most cases, the recipient of the miscredit or double credit would notify the financial institution. But a few individuals withdraw, rather than return, the money. Clearly, the wire transfer system has been misused, but not all financial institutions may identify these cases as crimes.

Identifying EFT Crimes

Data for this study were collected on a retrieval, rather than on-going basis. Thus, the incidents reviewed at each institution were those it identified as EFT complaints or potential crimes. We discovered that the incidents recorded as EFT crimes at a given institution are not necessarily drawn from an identical "pool" of possible EFT crimes as those recorded at another. As a consistent set of data is desired for the national panel, the scope of EFT crimes should be identified at the outset of the data collection.

The data collection suggested two types of possible ATM and wire transfer crimes that might not always be recorded as complaints crimes by all financial instituitions: those in which there is no loss, and those in which a mistake by the financial institution was involved. While EFT crimes resulting in a loss to the institution or customer will generally be recorded and investigated as a crime or suspected crime, if there is no loss involved or a crime is only attempted the incident may not be routinely recorded depending on the policy--usually informal--of the financial institution. For example, one institution included reports of stolen ATM cards that did not result in a loss in its fraud case files and monthly and annual tallies of ATM-

related frauds. Another handled stolen card reports with no loss as part of its customer services, not loss investigations. Similarly, wire transfer requests that are rejected because they do not meet administrative criteria may actually be unsuccessful unauthorized transfers, but few institutions record them accordingly.

Bank errors may create the opportunity for misuse that is not recorded as an EFT crime. For example, at one of the institutions we visited, customer reports that an ATM had not dispensed the full amount of the withdrawal were investigated with other complaints; at the other institutions they were not routinely investigated. There are at least three explanations for such a complaint: 1) the customer did not receive the full withdrawal and the ATM was over by the difference when balanced; 2) the customer did not receive his withdrawal but his account was not debited; or 3) the customer reports he did not receive the full withdrawal for which his account was debited but the cash drum of the ATM was balanced. The first two cases are obviously not crimes, the third always leaves a lingering suspicion at the financial institution. Similarly, as discussed above, wire transfer losses stemming from unrecovered miscredits or double credits are clearly crimes, although few institutions classify them as such.

Organizational Aspects of Data Collection

Just as no two financial institutions define and identify EFT crimes in the same manner, the data collection effort revealed that no two are likely to investigate losses or complaints in the exact same manner. For example, one financial institution combined ATM loss investigations with credit card loss investigations so that the investigators are completely outside the chain of command of the manager of ATM operations. The other placed ATM operations and loss investigations within a single department, but each was managed independently. Other institutions may handle ATM complaints as they arise in an ad hoc fashion. Further, the security department may be advised of a particular incident if it is of a serious nature, but formal channels between the security officer and ATM investigators do not always exist.

In all three arrangements, it is unlikely that a single individual will be directly responsible for loss investigations as well as all other facets of an institution's ATM system. However, our site visits and interviews seem to indicate that the responsibilities for managing wire transfer operations and maintaining case records for crimes are likely to be vested in a single individual. Because both crime and transactions data would be

desired in any EFT crime data collection effort, it is likely that more than one manager would be responsible for both sets of data in the ATM area, while a single individual might be responsible for both in the wire transfer area. In most instances, however, any division of responsibility can be easily overcome if the project has the support of a senior officer from the financial institution.

Recordkeeping for ATM and Wire Transfer Crimes

The fact that many large institutions have formal procedures for investigating ATM crimes should make it a relatively straightforward task to compile data on ATM crimes for the national panel. This is due in part to Reg E which requires financial institutions to investigate and resolve within 10 business days any complaint originating from the use of customer-initiated consumer EFT terminals (ATMs comprise most of these at present). Given the stiff penalties contained in Reg E, financial institutions tend to keep fairly comprehensive, formal records of ATM disputes. Our discussions and site visits indicate that the incident-based information which the panel would collect for ATM disputes--such as the value of the dispute, identity of the perpetrator, and modus operandi--is routinely recorded. The introduction of a new data collection instrument for the panel is not likely to be cumbersome.

Recordkeeping for wire transfer crimes appears to be much more informal than that for ATMs and other consumer EFT technologies. Although, as discussed in Chapter 5, financial institutions are required in many instances to report crimes or suspected crimes to law enforcement authorities and federal financial regulators, this report may often take the form of a letter or phone call. If the financial institution considers an incident to be a misuse, rather than a fraud or other crime, there may be no requirement to record it. The records or files that the institution maintains are likely to be those that chronicle the incident and the efforts it undertakes to have the disputed funds returned. Further, the investigation process is likely to be somewhat ad hoc and informal, resulting in data elements that vary from case to case. The data collection instruments used to collect data for a national survey may introduce a new element of formality into the wire transfer loss investigations process.

Nature of ATM and Wire Transfer Crimes

The efforts to collect preliminary data on ATM and wire transfer crimes demonstrated that the nature of the crimes vary depending on the technology, and, as a consequence, the procedures for data collection may also need to vary. For

ATMs, we feel that there are two ATM crime characteristics which will influence the implementation of the any national effort to collect data on EFT crimes. First, the data in our sample suggest that ATM crimes occur quite frequently, so that large financial institutions with 50, 100, or more ATMs may receive 225, 450, or more reported ATM crimes each year. Second, the types of crime associated with ATMs tend to be the same. For example, a stolen transaction card is often used to make withdrawals, and customers' cards are sometimes used without authorization by a family member. The large number and repetitive nature of ATM crimes lend them to a data collection scheme that can be highly structured, with specified choices for each item to be recorded. These collected data, in turn, can be easily aggregated.

In contrast, wire transfer crimes tend to be infrequent and unique. The incidence of wire transfer crimes appears to be so low that even the largest financial institutions may experience at most a handful each year. Thus, the total number of wire transfer crimes reported by a national panel of financial institutions may be measured in the hundreds. Given this small number of crimes, a larger sample of institutions may be required for wire transfer crimes. However, the panel may be able to indulge in the luxuries of reporting the wire transfer crimes less often and more in the format of a case study. Although several common data elements could be reported for each incident, the report could rely heavily on a narrative description which could emphasize its unique aspects.

Some Hypotheses About ATM and Wire Transfer Crimes

Before discussing the implications that the preliminary data collection effort holds for the implementation of a national project to measure EFT crime, it is useful to briefly explore some hypotheses about ATM and wire transfer crimes that have emerged from the data collection effort. These hypotheses are useful, not only for the preliminary insight they shed on the nature of these crimes, but also because they demonstrate the kinds of questions and issues that can be addressed with consistent data on EFT crimes.*

The preliminary figures presented in the ATM area are based on a sample of 253 ATM crimes from the two

*The actual data collected from the three financial institutions are not included in this document. The information is still preliminary and obviously represents data from a statistically insignificant number of institutions (i.e., two for the ATM area, and one for the

institutions. The preliminary figures presented in the wire transfer area are based on a review of the 16 incidents of wire transfer loss that occurred at one institution over a three-year period.

Hypotheses Concerning ATMs

- Recalling the five categories for EFT crimes identified in Chapter 5--hardware, software, internal procedures, internal procedures, external procedures, and environment --the sample suggests that the vast majority of ATM crimes are external crimes.

- Only a very small percentage of ATM transactions appear to be involved in ATM disputes (less than 1/2 of 1 percent) with an average of 4 transactions per dispute. Further, the average loss associated with ATM crimes is probably quite low--only a few hundred dollars per reported crime. However, given the large number and high usage of ATMs, the total national loss from ATM crimes probably runs into several million dollars per year.

- Despite the low average loss associated with a reported ATM crimes, it is possible for a perpetrator to obtain over a thousand dollars from an ATM account if multiple withdrawals are made over a time period of a few days.

- It appears that most ATM crimes tend to fall into one of two categories: those involving lost or stolen cards and PINs, and those involving customer complaints that unauthorized withdrawals were made against an account. In our sample, almost two-thirds of the cases involved lost or stolen cards, and slightly more than one-third involved unauthorized transactions.

wire transfer area.) If the information were released at this point, it might be misunderstood or misrepresented, no matter how carefully it was qualified--especially give the current lack of available data and the attention such information might receive. The data do provide the basis, though, for outlining the hypotheses listed in the text, and they do demonstrate the feasilibity of collecting statistically valid and consistent information on the nature and extent of EFT crime. Further, at a later time, when viewed in conjunction with other data which may be collected, this information can, and should, provide an interesting base for comparison and analysis.

- The preponderance of lost or stolen cards and disputed transactions suggest that ATMs are most vulnerable to crime when the user and the ATM interact. Thus the security of the account rests on maintaining the secrecy of PINs and safekeeping cards. In fact, our sample suggests that more than half of the customer's tend to write their PINs with or near their cards, creating the opportunity for unauthorized use of their cards. (Both banks in our sample relied on bank-generated PINs.)

- One problem in preventing ATM crime losses is customer delays in reporting incidents. Although slightly less than one-fourth of the cases were reported within 1 day of the incident, more than one-third were not reported until at least 2 weeks had passed. Some delays occur when customers are not aware of unauthorized transactions until a statement is received, while others occur when customers fail to promptly report lost or stolen cards, or suspicious withdrawals.

- It appears that the perpetrators of an ATM crime often have some relationship to the customer or bank. In the subset of cases in which the identity of the perpetrator was known or suspected, a household member, a friend, a bank employee or a customer was implicated in almost all the incidents.

- Financial institutions appear to absorb most of the loss associated with ATM crimes with the banks absorbing about two-thirds of the total loss, and the customers about one-third. Reg E liability assessed against customers appears to account for only a few percentage points of the total loss.

- The sampled cases suggest that ATM crimes are very unlikely to result in arrest or other legal actions. None of the sampled cases resulted in an arrest. In three cases, the customer took the bank to small claims court because it had refused to credit his account; only one of the three customers won his case.

Hypotheses Concerning Wire Transfers

- There appears to be a consensus that the security of wire transfer systems are generally under control, but that the potential for large losses from criminal actions exists and should be treated seriously. To the extent that unauthorized wire transfers occur,

they tend to be characterized by a high level of loss. At least one private supplier of EFT security estimates that the average wire fraud loss is in the vicinity of $400,000 [Atalla, 3/22/82].

- It is likely that the actual number of incidents is quite low. For example, the bank included in our sample--a large commercial bank heavily involved in wire transfers--had experienced no losses due to unauthorized or otherwise fraudulent wire transfers in the last decade.

- Wire transfer crimes are generally thought of as unauthorized wire transfers in which the perptrator manipulates a bank's wire transfer system to have funds improperly credited to his account. However, our very preliminary data collection indicates that there may be another source of loss: customer's who fail to return money that is miscredited or double-credited accounts to their accounts. Once the customer fail's to return the money. a wire transfer crime has been committed as per our definition in Chapter 4. (An interesting point is that while agreeing to the fact that the customer who absconded with the miscredited or double-credited money is commiting a crime, some bank officials view the act in a less severe light because, as one official puts it, "we gave him the opportunity to become a criminal.")

- The data suggest that the incidence of losses due to miscredites or double credits is also extremely low, and only occurs every few hundred thousand transactions. Although the average loss might range in the thousands of dollars, this is much less than 1 percent of the value of an average wire transfer.

- One interesting aspect of such wire transfer losses is that they tend to involve individuals rather than corporations. Although wire transfers to individuals represent a very small proportion of the total volume of wire transfers, the vast majority of the losses involved transfers to individuals.

Implications for the National Panel

In addition to providing insights into the nature of ATM and wire transfer crimes, the preliminary data collection is also of great benefit as a source for developing guidelines for the design of data collection instruments and procedures for a national panel or sample of financial institutions. As

discussed above, a number of issues were uncovered during the site visits to collect data for ATMs and wire transfers. Based on both the lessons learned from of the data collection process and a review of the results by a group of EFT experts at a workshop held in Washington, D.C. on June 18, 1982, the implications these issues hold for implementing the panel are summarized below.

Structure of a National Panel

The national EFT crime panel would consist of a statisically-drawn sample of financial institutions which would provide data on EFT crimes. However, as part of a project to estimate the extent of EFT crime, it would also be desirable to establish an Advisory Group in support of the panel.

Such an Advisory Group would consist of technical consultants, users, vendors, regulators, auditors, and a subset of institutions from the panel of financial institutions. It would meet on an as needed basis to provide support to the panel in the areas of technical issues (e.g., the vulnerabilities of EFT systems to crime, use and value of collected information), data collection form design and implementation issues (e.g., the characteristics of incidents to be recorded as crimes), and statistical issues regarding the underlying model for constructing the panel (e.g., appropriate sample size). As some members from the national panel would also serve on the Advisory Group, they could assist in "selling" the approach and survey instruments to the sampled institutions.

Some additional considerations for the panel structure include:

- Given the differences in the numbers of institutions that provide consumer and corporate EFT services, and the varied nature, extent, and value of related crimes, separate samples and procedures should be used to collect data on consumer and corporate EFT crimes.

- Earlier in this report, we identifed the need to collect data on internal EFT crimes. It will probably be difficult to obtain this information. Financial institutions tend to be hesitant to release information on internal crimes or may classify them as "errors." However, the extent of internal EFT crimes could be explored within the consumer EFT panel of financial institutions to suggest a data collection approach for the future.

- It may be desirable to select a few institutions from the national panel which could serve as a "control group." In-depth data collection at these control institutions through site visits and interviews could be used to determine the extent to which EFT crimes are not formally reported, and to provide a check against the data provided by the full panel.

Data Collection Design and Procedures

The design of data collection instruments and procedures for the panel would ultimately be based upon the recommendations of the Advisory Group and review by the sample of financial institutions. However, at this stage it is possible to identify three major types of data which need to be collected for each EFT technology: (1) EFT "crime" incidents; (2) a baseline for EFT transactions; and (3) a baseline for nonEFT transactions. The discussion of the preliminary data collection effort on pages 106 to 109 illustrates the specific kinds of data in the ATM area that would be sought for each category.

Based on the preliminary effort, three steps in the data collection process can be envisioned:

- First, a site visit would be made to each participating financial institution. A basic description of the institution's EFT system would be recorded and initial contacts with the employees who would serve as liasons during the study would be established.

- Second, data for EFT crimes would be recorded on an incident-by-incident basis. The instrument would be introduced during the site visit so that questions about its implementation could be answered.

- Third, aggregate figures for all EFT transactions would be recorded on a monthly or quarterly basis. Again, a simple form would be provided for this task. These data would serve as a baseline for evaluating the incident-specific data.

Defining and Indentifying EFT Crimes

As discussed earlier, the definition, identification, and investigation of EFT crimes varies across institutions. Thus, the data collection instruments used in any effort to measure EFT crime should be carefully designed to allow participants to provide data in a meaningful and consistent manner. Implementation issues should be discussed with the

participating financial institutions to develop a common definition of EFT crime, a common understanding of the type of incidents to be recorded as EFT crimes, and consistent procedures for data collection. More specifically:

- To ensure that a consistent set of data is recorded, "EFT crime" should be clearly defined from the outset. A broad definition such as that presented in Chapter 4 would capture the fullest array of incidents. The definition should indicate that an attempted crime is also a crime as in the case of traditional crimes.

- Because the term "crime" has many connotations, words such as "dispute," "complaint," or "misuse" should be used to describe the type of incidents to be reported. For example, each panel member would be asked to record any known or suspected misuse of funds, equipment, or access related to its EFT system. All incidents reported to the financial institution would be recorded without regard to loss, as would attempted frauds.

- Most EFT crimes are investigated and formally recorded. However, some crimes may only be refelcted in aggregate "sensitivity measures" for the EFT system (e.g., captured ATM cards could be damaged--and thus not involved in a criminal act--or altered--and represent an attempted crime. Thus, to assure uniform data across institutions, specific examples of the types of incidents considered EFT crimes should be provided. Incidents to be reported as known or possible ATM crimes could include, but not be limited to, reports of lost or stolen cards, customer complaints of disputed transactions, suspicious empty envelope deposits followed by withdrawals, branch reports of unbalanced cash drums, and altered or counterfeit transaction cards captured at the ATM. Wire transfer crimes could include, but not be limited to, unauthorized transfers, attempted unauthorized transfers, and unrecovered miscredited transfers, or administratively rejected transfer requests.

Organizational Aspects and Recordkeeping

The apparent division of responsibility for EFT investigations and operations indicates that EFT fraud losses as a group may not yet be a focus of interest for managers--who have been more accustomed to thinking of checking losses,

ATM losses, or credit card losses as the "costs of doing business" for that function. Thus, the proposed effort to collect data on EFT crimes may require intraorganizational coordination. For example, complaint records for each EFT technology may be maintained in independent departments, and data on overall EFT transactions may be kept in yet others. The participation of a senior officer in an oversight position would be very helpful in ensuring successful data collection.

Other organizational issues affecting implementation of a national panel of financial institutions include:

- Data for this study were collected from existing files by PSE employees during site visits to minimize the staff time required of the participating institutions. The proposed panel approach, however, would involve the member's employees in recording EFT crime data on an ongoing basis. Thus, the design for the data collection instruments should take into account limits on the institutions' personnel resources. Ideally, the forms would also be used by the institutions for their investigation purposes.

- Reporting procedures for consumer and corporate EFT crimes appear to differ. At the institutions visited, ATM investigations were formally structured, while complaints tended to be numerous and repetitive in nature. Wire transfer investigations, however, tended to be less formal, and complaints were infrequent and dissimilar in nature. These differences lend support to the concept of designing separate data collection procedures and forms for consumer and corporate EFT services.

Nature of EFT Crimes

The characteristics of crimes within different categories of EFT technologies (such as frequency, value, and modi operandi) will influence the format of data collection. For example, Given the apparent frequent incidence of reported consumer EFT crimes, it would be appropriate to use structured data collection instruments which specified choices for the items to be recorded. Choices can be easily developed because consumer EFT disptues tend to repeat similar scenarios. In contrast, because the expected number of corporate EFT disputes is small, the data collection instruments can be longer and more open-ended. This structure is desirable given the unique and more complicated characteristics of these disputes.

Other implications stemming from the differing nature of EFT crimes include:

- If a participating financial institution has an extensive consumer EFT system, and thus a very high number of complaints, it may be desirable to report only a sample of such incidents to the panel. This would require less employee time to complete the data collection instruments, but would still provide data sufficient for the panel's needs.

- The magnitude of consumer EFT crimes is much greater than that of corporate EFT crimes. It would probably be feasible to limit the size of the national sample for consumer EFT to the 50 institutions identified earlier. However, given the apparent low incidence of corporate EFT crimes, a much larger sample of institutions may have to be selected for this category although each institution would provide data for fewer cases than in the consumer category.

Securing Participation of Financial Institutions

To ensure the success of the panel approach, it is important to secure the participation of randomly selected financial institutions. However, the release of information about the incidence of white collar crimes--including EFT crimes--has been viewed as particularly sensitive. Fortunately, during the site visits we learned that bank officials are also concerned that the nature and extent of EFT crime have been misunderstood, especially by the press. As they are aware that little data now exist to support or refute many assertions about the potential for EFT crimes, they realize there may be utility--both in terms of public opinion and their own internal evaluations and decisions regarding EFT--in obtaining better information so that EFT crimes can be viewed in a realistic manner. Some approaches for encouraging participation in a national panel include:

- Protecting the confidentiality of the participating financial institutions through anonymity. Just as the identity of the banks participating in our preliminary data collection effort were not revealed, all members of the EFT panel could be assured that the data collected from their institution would never be directly identified with them.

- All findings and data released should be reported in an aggregated or merged fashion across all the participating banks in, say, a cell of the panel. Thus, although one might know which banks are

participating in the overall panel, it would not be possible to single out any member of the cell from the published statistics.

- The resultant panel findings could be expressed in relative, rather than absolute, terms. That is, the results could be expressed as proportions (e.g., proportion of EFT transactions resulting in a crime, proportion of crime-related losses to total EFT volume) rather than absolute values; thereby further reducing the chance that the results could be used to identify the participating institutions.

- In order to increase the likelihood that a randomly selected bank would participate in a national panel, it is clear from our experience of approaching banks to participate in our preliminary study that some form of cosponsorship with an established professional organization would be helpful. For example, the Association of Reserve City Bankers or the American Bankers Association could serve this purpose. These organizations are becoming increasingly aware that there is a lack of concrete data on the occurrence of crime in EFT systems. This lack has become a source of concern, at least to some, and it may help improve the response to a formal panel-based data collection effort.

A Phased Approach

The national EFT panel, as outlined in this chapter, is clearly an ambitious undertaking. However, it is likely the resultant data and analysis would justify such an undertaking. If such information were gathered, both criminal justice professionals and financial experts would be able to speak with authority regarding the nature and extent of EFT-related crime in both commercial banks and thrift institutions and for the three regions of the country. Nevertheless, because of resource--time and cost--constraints, it may be appropriate to begin this undertaking with a first phase which would focus on a subset of the panel. To derive the maximum benefit from the resources available for data collection, it may be best to begin by exploring only a few cells of the panel. These cells could be chosen because of their potential as a rich source of EFT crime data. For example, one type of financial institution, probably commercial banks, in perhaps one geographic area could be sampled from. This one-cell subpanel would still need to be large enough--perhaps about 7 or 8 banks (or 14 banks if two cells were included)--so as to allow the data to accurately represent the population in that cell. But

because the data from this cell would not be used to make assertions about the others, the cost of beginning the panel effort would be substantially lower. Alternatively, only one EFT service under each category of EFT technology could be included, such as ATMs in the consumer area, and wire transfers in the corporate area. Approaches such as these would allow for data to be gathered, analyzed, and published, and would provide information on both the nature and extent of EFT crime for the one or two cells or services selected. Further, the first phase effort could serve as a test of the panel concept and as an aid in deciding whether the panel should be implemented on a full-scale basis.

Concluding Thoughts

A final finding which emerged from the preliminary data collection effort does not relate to implementing the panel, but to the benefits of participating. The need to share information on preventing EFT losses as well as identifying EFT scams was mentioned several times in the interviews. A few informal arrangements exist between financial institutions to meet and discuss EFT security issues. But in most cases, one financial institution is usually unaware of the nature of EFT losses at another, even though both may be victims of the same or similar schemes. The proposed national panel would provide a formal mechanism to share such information among the members and to disseminate it to the entire financial community. Additionally, as one of the ATM loss managers indicated to us during the feedback of the collected data, not only is there no mechanism to share information on ATM losses and crimes among institutions (and thus determine whether losses were excessive, normal, or small), individual banks do not fully understand the nature of their own losses. Analysis of data collected through the panel approach would meet both types of information needs.

REFERENCES

Abell, Bruce. "A Technology Assessment: The Social Consequences of Far Less Cash and Checks." Computers and People 26(February 1977):7-10,21.

A.J. Wood Research Corporation. Data cited in Bank Card, August 1978, p. 3.

Allen, Brandt. "Computer Fraud: New Findings, New Insights." Paper presented at the 8th Annual Computer Security Conference, New York, N.Y., November 9-12, 1981.

Allen, Brandt. "Threat Teams: A Technique for the Detection and Prevention of Fraud in Automated and Manual Systems." Computer Security Journal 1(Spring 1981):1-13; The Darden School Reprint Series, University of Virginia, Reprint No. DSR-81-04.

American Bankers Association. "Results of the 1978 National Operations and Automation Survey." Washington, D.C., 1978. (Mimeographed.)

American Bankers Association, Payment Systems Planning Division. "Results of ATM Security Survey." Washington, D.C., 1978. (Mimeographed.)

"AMEXCO to Test ATM Plan Nationally." American Banker, 30 April 1981.

"A.O. Smith's Schmelzer Sees More Sharing." American Banker, 26 November 1980.

Arthur D. Little, Inc. The Consequences of Electronic Funds Transfer. Cambridge, Mass.: author, 1975.

Association of Reserve City Bankers. Report on the Payments System. Washington, D.C.: author, 1982.

"AT&T and IBM: Shaping Home Information Services." American Banker, 15 June 1982.

Awad, Elias M. "The Issue of Electronic Funds Transfer: An Overview and Perspective." Computers and People 26(June 1977):7-9,22.

Baker, Donald I. and Penney, Norman. The Law of Electronic Fund Transfer Systems. Boston: Warren, Gorham, and Lamont, 1980.

Bank One. Channel 2000. Columbus, Ohio: author, 1981.

"Bank-at-Home Priority Stressed; United Amer. Hails Response." American Banker, 20 November 1980.

"BankLink Gets 50th Member." American Banker, 21 April 1982.

Battey, Phil. "Committee Hopes to Include EFT in New Uniform Commercial Code." American Banker, 19 January 1981.

Becker, J. Quoted in Time, 16 February 1981.

Benton, John B. "Electronic Funds Transfer: Pitfalls and Payoffs." Harvard Business Review 55(April 1980).

Benton, John B. "Electronic Funds Transfer: Pitfalls and Payoffs." Harvard Business Review 52(July-August 1977):16-17,20-21,28-29,32,164-66.

Bequai, August. Computer Crime. Lexington, Mass.: Lexington Books, 1978.

Bishop. Y.M.; Fieberg, S.E.; and Holland, P.W. Discrete Multivariate Analysis. Cambridge, Mass.: MIT Press, 1975.

Brouillette, Geoff. "BofA Offers Small Businesses Telephone Payroll Service." American Banker, 3 November 1980.

Blumenthal, Ralph. "Electronic Fraud Accompanies Move Toward Tellerless Banking." New York Times, 26 March 1978.

Burke, Jack. "EFT: More Security, Not Less." Banking, January 1977, pp. 37, 84, 86, 89.

Burnham, K.P. and Overton, W.S. "Estimation of the Size of a Closed Population When Capture Probabilities Vary Among Animals." Biometrika 65(1978):625-33.

Butkovic, Rosemary. Remote Financial Terminals and Participating Financial Institutions in the U.S. Brookfield, Ill.: author, 1977.

Campbell-Klein, Cecelia E. "An Historical and Analytical Study of the Federal Computer Systems Protection Act of 1978 (Senate Bill 240)." Master's thesis, University of California, Irvine, 1980.

Carroll, John M. Computer Security. Los Angeles: Security World Publishing, 1977.

Chamber of Commerce of the United States. A Handbook on White Collar Crime: Everyone's Problem, Everyone's Loss. Washington, D.C.: Government Printing Office, 1974.

Chase Manhattan Bank. "Advertising Insert." American Banker, 26 November 1980.

"Chicago EFT Group Makes Plans to Solicit Banks for Shared Networks." American Banker, 8 January 1981.

Colton, Kent W. and Kraemer, Kenneth L. Computers and Banking. New York: Plenum Press, 1980.

Colvin, Bill D. "Computer Crime Investigators--A New Training Field." FBI Law Enforcement Bulletin, July 1979.

"Computers Spur Sophisticated Crime Wave." The Denver Post, 6 September 1980.

"Corporate Fraud Checklist." Computer Fraud and Security Bulletin, Supplement.

Coughran, Edward H. Crime by Computer. San Diego: UC San Diego Computer Center, 1976. Cited by Daniel Kevin, "EFT System Integrity." Paper prepared for Office of Technology Assessment, Washington, DC, 1980, p. 213

Courtney, Robert H., Jr. "The Democratization of White Collar Crime." Computer Security Journal 1(Spring 1980).

Craddock, Candace U. "The Status of EFTS in Canadian Banking." The Canadian Banker & ICB Review 87(June 1980):28-31.

"Credit Card Probers Warning Banks of 'White Plastic Scheme.'" American Banker, 16 December 1980.

"Data Card Corp. Purchases Rights to Fingerprint-Identification System." American Banker, 7 January 1981.

Deutsch, Barry L. "Personal Productivity and the ATM." American Banker, 25 November 1980.

DeGouw, Chris. "Data Processing Crimes." EDPACS 5(January 1978):1. Cited in James R. Dudine, "Computer Fraud in Banking," Thesis, Rutgers University, 1980.

Dooley, Ann. "ABA Finds Banks Curtailing Lossess with ATMs." ComputerWorld.

Dudine, James R. "Computer Fraud in Banking: Perspective for the 1980s." Thesis, Rutgers University, 1980.

Duffy, Helene, and Duffy, Robert J. Electronic Money in Perspective. Boston: Datavision Associates Inc., 1974.

"Earnings Rise Lags Sales Gain During Docutel Corp.'s 3d Qtr." American Banker, 5 November 1980.

"EFT and Privacy." Federal Reserve Bulletin 64(April 1978): 279-84.

"EFTS Decisions Will Have Lasting Impact." Infosystems, March 1976, p. 33.

"EFTS Ushers in a Major Revolution in Banking." Infosystems, March 1976, pp. 33-34.

"Electronic Banking: A Retreat from the Cashless Society." Business Week, 18 April 1977, pp. 80-90.

Electronic Banking, Inc. "Directory of Telephone Bill Payment Services as of December 31, 1979." Atlanta, 1980.

Electronic Banking, Inc. "EFT: The Next Fifteen Years." Atlanta, 1980. Distribution of source document restricted by author.

"Farmers Bank Del. and Girard Bank Arrange Interstate George Card Use." American Banker, 7 January 1981.

"Favorite of Institutions and Users." American Banker, 18 November 1980.

Federal Deposit Insurance Corporation. 1980 Annual Report. Washington, DC: author, 1981.

Federal Deposit Insurance Corporation. Division of Management Systems and Financial Statistics. Electronic Funds Transfer System Glossary. Washington, DC: author, 1978.

Federal Deposit Insurance Corporation. Division of Management Systems and Economic Analysis. A Guide to EDP and EFT Security Based on Occupations. Washington, DC: author, 1975a.

Federal Deposit Insurance Corporation. Division of Management Systems and Economic Analysis. Introduction to the Automated Clearing House. Washington, DC: author, 1976a.

Federal Deposit Insurance Corporation. Office of Management Systems. Introduction to Automated Tellers. Washington, DC: author, 1975b.

Federal Deposit Insurance Corporation. Division of Management Systems and Economic Analysis. Introduction to EFT Security. Washington, DC: author, 1976b.

Federal Deposit Insurance Corporation. Office of Management Systems. Introduction to Point of Sale Systems. Washington, DC: author, 1976c.

Federal Reserve Board. Annual Report, 1980. Washington, DC: author, 1980.

Federal Reserve Board. Annual Statistical Digest 1970-1979. Washington, DC: author, 1981.

Federal Reserve Board. "1978 PACS Expense Report." Washington, D.C.: author, 1979b.

Federal Reserve Board. "The Payment System in the United States." Washington, DC, 1979a.

Feller, W. H. An Introduction to Probability Theory and Its Applications Vol. 1, 3d ed. New York: John Wiley and Sons, 1968.

Fienberg, E. "The Multiple-Recapture Census for Closed Populations and Incomplete 2^k Contingency Tables." Biometrika 59(1972):591-603.

"From the Telephone Company: A Massive PBX Net in NY and Consulting Expertise." American Banker, 31 December 1980.

Geary, Anne. "Bank Compliance With the Electronic Fund Transfer Act." Banking Law Journal 97(August 1980):596-620.

Gore, Newton. "Tumultuous Financial..." American Banker, 17 November 1980.

Greguras, Fred M. Corporate EFT: Vulnerabilities and Other Audit Considerations. Kutak Rock & Huie, 10 December 1980.

Greguras, Fred M., and Sykes, David J. "Authentication in EFT: The Legal Standardd and the Operational Reality." Computer/Law Journal 2(Winter 1980):67-86.

Greguras, Fred M. Letter To Kent W. Colton, Public Systems Evaluation, dated 18 May 1982.

Gross, Laura. "Consumers Flock to Banks Promoting No-Fee Cards." American Banker, 9 February 1981.

Gross, Laura. "Fidelity 'Money Line' Uses ACM Nets to Ease Bank-Money Fund Transfers." American Banker, 3 September 1981.

Gross, Laura. "Master Card to Start 'Money Manager' Plan." American Banker, 2 September 1981.

Gross, Laura. "State Street Brokerage Firm Plans Money Fund Debit Card." American Banker, 28 April 1981.

Holmes, Edith. "Commission Gives Nod to Treasury EFT, Bars Bell." ComputerWorld, 3 October 1977, pp. 1-2.

"An Inside Look at Card Standards." ABA Banking Journal 27(September 1980):97-98.

Jenkins, Brian, and Pinkney, Anthony. An Audit Approach to Computers. London: The Institute of Chartered Accountants in England and Wales, 1978.

Jurgen, Ronald K. and Ernst, Martin L. "Electronic Funds Transfer: Too Much, Too Soon?" IEEE Spectrum 14(1977):51-7.

Kevin, Daniel. "EFT-Description and Partial Evaluation." Paper prepared for the Office of Technology Assessment, Washington, DC, 1980a.

Kevin, Daniel. "EFT System Integrity." Paper prepared for the Office of Technology Assessment, Washington, DC, 1980b.

Kirchner, Jake. "EFT Providers Bewail Cost of Privacy Legislation." ComputerWorld, 9 April 1979.

Kirchner, Jake. "Privacy Emphasis Expected in 96th Congress." ComputerWorld, 25 December 1978, p. 5.

Kraemer, Kenneth L., and Colton, Kent W. "Policy, Values and EFT Research: Anatomy of a Research Agenda." Communications of the ACM 22(December 1979):660-70.

Kranzley & Co. "The Analysis of Certain Potential Threats to EFT System Sanctity." A study conducted for the Electronic Industries Foundation, 1976.

"Kranzley Switch Bought by Metroteller." American Banker, 26 November 1980.

Krauss, Leonard I., and MacGahan, Aileen. Computer Fraud and Countermeasures. Englewood Cliffs, New Jersey: Prentice Hall, 1979.

Kutler, Jeffrey. "ATMs are by Far the Most Popular of All EFT..." American Banker, 18 November 1980.

Kutler, Jeffrey. "BAI Guide to Streamline Cash Management Delivery." American Banker, 29 October 1980.

Kutler, Jeffrey. "Bank Wire President Urges Total ACH Overhaul; System Termed Unable to Cope With New Technology." American Banker, 9 February 1981.

Kutler, Jeffrey. "Cable Firm Plans Home Banking System in Omaha, New Orleans." American Banker, 2 March 1981.

Kutler, Jeffrey. "Can ATMs Be Profitable? The Ayes Grow." American Banker, 26 November 1980.

Kutler, Jeffrey. "Carter Administration Plans Liberal EFT Deployment Push, If Re-elected." American Banker, 30 October 1980.

Kutler, Jeffrey. "Check Volume Fails to Rise as Expected, Fed Study Finds." American Banker, 6 February 1981.

Kutler, Jeffrey. "Citi Adds ATM Consultant to Thrift Resources Unit." American Banker, 6 November 1980.

Kutler, Jeffrey. "Citi ATM Net Signs Banks in Six States: INCA Marketing Push is Picking Up Steam." American Banker, 9 February 1981.

Kutler, Jeffrey. "Funds Transfer Terminology Task Force, Data Security Committee Report Gains." American Banker, 17 December 1980.

Kutler, Jeffrey. "'Intelligent' Memory Card Studied." American Banker, 20 January 1981.

Kutler, Jeffrey. "National EFT Push Takes on New Urgency." American Banker, 11 February 1981.

Kutler, Jeffrey. "Tiny Chip-in Card May Emerge the Ultimate Payment Vehicle." American Banker, 13 October 1980.

Kutler, Jeffrey. "Visa Exec Calls for Electronic Validation to Lessen Fraud." American Banker, 4 February 1981.

Kutler, Jeffrey. "VISA Plans Upscale Card, ATM Network." American Banker, 6 April, 1981.

Larson, Robert E. "Cost of EFT Services..." American Banker, 17 November 1980.

"Legal Maneuvering Shows Weaving of Electronic Funds Net." Infosystems, March 1976, pp. 34-35.

Lipis, Allen H. "Costs of the Current U.S. Payment System," Communications of the ACM, 22(December 1979):644-47.

Lipis, Allen H. "Cost of the Current U.S. Payment System," Magazine of Bank Administration, October 1978, p. 30.

Long, Robert H. "Public Protection and Education with EFT." Communications of the ACM 22(December 1979)648-54.

Lundell, E. Drake, Jr. "Carter Readying Privacy Initiative." ComputerWorld, 25 December 1978, pp. 1,8.

Matthews, Gordon. "First National Bank of Chicago Plans Fingerprint, Voice ID Systems." American Banker, 10 February 1981.

Matthews, Gordon. "Safety at ATM Sites Draws Increasing Concern: Citibank Temporarily Reimburses Victims of Holdup." American Banker.

Matthews, Gordon. "Many ATM Frauds are All in the Family." American Banker, 18 February 1981.

National Association of Mutual Savings Banks. 1978 National Fact Book of Mutual Savings Banking. New York: author, 1979.

National Commission on Electronic Fund Transfers (NCEFT). EFT and the Public Interest: A Report of the National Commission on Electronic Fund Transfers. Washington, DC: Government Printing Office, 1977a.

National Commission on Electronic Fund Transfers. EFT in the United States: Policy Recommendations and the Public Interest. Washington, DC: Government Printing Office. 1977b.

National Commission on Electronic Fund Transfers. Programs, Plans, and Accomplishments of the National Commission on Electronic Fund Transfers: A Progress Report to the President and to the Congress. Washington, DC: Government Printing Office, 1976.

"National Interchange is Launched for Regional Teller Machine Nets." American Banker, 14 September 1981.

"New Bank Card Technology Looms as Challenger to the Chip-in-Card." American Banker, 29 April, 1981.

Osterberg & Associates. Security, Privacy, & Accuracy in EFT Networks. Chicago: U.S. League of Savings Associations, 1976.

Parker, Donn, and Nycum, Susan. Computer Crime: Criminal Justice Resource Manual. Washington, DC: Government Printing Office, 1979.

Parker, Donn; Nycum, Susan; and Dura, S. Computer Abuse. Menlo Park, Calif.: SRI International, 1973.

Parker, Donn, B. "Computer Abuse Assessment," Encyclopedia of Computer Science and Technology, Vol. 3. 1975.

Parker, Donn B. "Computer Abuse Research Update." Computer/Law Journal 2(1980).

Parker, Donn B. "Vulnerabilities of EFTS to Intentionally Caused Losses." Communications of the ACM 22 December 1979:654-60.

Pastore, Steven. "EFT and the Consumer." The Bankers Magazine, March-April 1979, pp. 35-42.

Payment Systems, Inc. Payment Systems Perspectives '78. Atlanta: author, 1978.

Peat, Marwick, Mitchell & Co. Trends in Electronic Funds Transfer. New York: author, 1979.

Peat, Marwick, Mitchell & Co. EFT: A Strategy Perspective. New York: author, 1977.

"Public Likes EFT if Change Not Radical." American Banker, 23 April 1980.

"Regulation E: Additions." Federal Reserve Bulletin 65(October 1979):833.

Robinson, James D., III. "Payments, People, Privacy: A Challenge of the Eighties." Computers & People 29(July-August 1980):7-9,22.

Roseberg, Robert R. "We Are Losing the Battle Against Bank Crime." Security Management, April 1980, pp. 43-45.

Rosenstein, Jay. "Volcker Doubts Tax Break on Interest Will Increase Savings." American Banker, 6 February 1981.

Rubenstein, James. "Chicago EFT Group Makes Plans to Solicit Banks for Shared Network." American Banker, 8 January 1981.

Sanathanan, L. "Estimating the Size of A Multinomial Population." Annals of Mathematical Statistics 43(1972):142-52.

Sanders, C.W.; Sandy, G.F.; Sawyer, J.F.; and Schneider, A. Study of Vulnerability of Electronic Communication Systems to Electronic Interception, Vol. 1. McLean, Virginia: MITRE Corporation, 1977.

Schabeck, Tim A. Computer Crime Investigation Manual. Madison, Wis.: Assets Protection, 1979. Cited in James R. Dudine, "Computer Fraud in Banking," Thesis, Rutgers University, 1980.

Schultz, Brad. "Heavy EFT Traffic, Related Crime in '78 Stimulates Concern Over Bank's Security." ComputerWorld, 11 December 1978, p. 6.

Schultz, Brad. "Nets Seen Easy Prey for Wiretappers. ComputerWorld, 25 June 1979, pp. 14,23-24.

Schultz, Brad. "Ribicoff Urges Banks to Endorse DP Crime Bill." ComputerWorld, 19 March 1979, p. 5.

Seber, G.A.F. The Estimation of Animal Abundance and Related Parameters. London: Charles Griffen, 1973.

"Settlement of Antitrust Suit Enables NY Shared EFT Networks to Go Forward." American Banker, 7 October 1980.

"Shared ATM Net Forms in Carolinas." American Banker, 11 December 1980.

Shenefield, John H. "Computers, Communications, and Antitrust: Some Current Myths and Realities." Computers and People 27(May 1978):14-17.

Shenefield, John H. "Computers, Communications, and Antitrust: Some Current Myths and Realities--Part 2." Computers and People 27(June 1978):10-11,16.

Shick, Blair C. "Privacy--The Next Big Issue in EFT." Banking, March 1976, pp. 70-76.

"Six Indicted for Defrauding Citibank." American Banker, 19 April 1982.

Snow, David. "The Advantages Of EFTS--For the Criminal." Security Management, November 1978, pp. 36-8.

"The Spreading Danger of Computer Crime." Business Week, 20 April 1981, pp. 86-92.

Statland, Norman. "Computers--Their Impact on People's Lives in the 1980's." Computers and People 28(November-December 1979):7-8.

Taber, John K. "A Survey of Computer Crime Studies." Computer/Law Journal 2(Spring 1980):275-329.

Tarwater, Joan L. A Guide for Security Control and Auditing of In-House Computers. Washington, D.C.: Federal Deposit Insurance Corporation, 1980.

"Technology Topics." American Banker, 3 February 1982.

"Texas ACH Weighs ATM-Switching Mechanism." American Banker, 24 December 1980.

Tien, J.M.; Barnett, A.I., and LoFaso, A. "On Estimating the Extent of Computer-Based Criminal Activity." Cambridge, Mass.: Public Systems Evaluation, Inc., 1981.

Trigaux, Robert. "AT&T Unveils Videotex Standards Critical to Spread of New Systems." American Banker, 21 May 1981.

Trigaux, Robert. "Big Banks Sign on ATM Network." American Banker, 4 April 1982.

Trigaux, Robert. "Citibank Acts to Beef Up Security At Its ATMs." American Banker, 9 April 1982.

Trigaux, Robert. "Study Predicts Proliferation of Home Banking Systems." American Banker, 3 March 1982.

Trigaux, Robert. "VISA Commits $10 Million to Push POS Terminal Expansion." American Banker, 8 July 1981.

Trigaux, Robert. "Visa Planning National Network of Shared ATMs." American Banker, 5 April 1982.

Trigaux, Robert and Arvan, Alice. "National ATM Systems in Works; Big 12-Bank Alliance Dubbed 'Cirrus'." American Banker, 11 February 1982.

"Two NY Shared ATM Nets Proceeding." American Banker, 2 October 1980.

"Tymshare's ATM System Gets Underway." American Banker, 24 December 1980.

Tyson, David O. "As Home Banking Hits Its Stride, Trust Officers Want Some Action." American Banker, 1 April 1982.

United States League of Savings Association. '81 Savings and Loan Sourcebook. Chicago: author, 1981.

U.S. Congress Senate. Subcommittee on Criminal Justice. Federal Computer Systems Protection Act of 1979 (Proposed). 96th Cong., 1st sess., 1979, S.B.240.

U.S. Department of Justice. Law Enforcement Assistance Administration. National Criminal Justice Information and Statistics Service. Computer Crime: Criminal Justice. Washington, D.C.: author, 1979.

U.S. Department of the Treasury. Geographic Restrictions on Commercial Banking in the United States. Washington, D.C.: Government Printing Office, 1981.

U.S. General Accounting Office. Electronic Funds Transfer--Its Potential for Improving Cash Management in Government. Washington, D.C.: Government Printing Office, 1980.

U.S. General Accounting Office. Vulnerabilities of Telecommunication Systems to Unauthorized Use. Washington, D.C.: Government Printing Office, 1977.

Vadasz, L.L. Quoted in Business Week, 2 March 1981, p. 116.

"VISA Authorization Pilot Expanded to Include All Members." American Banker, 20 November 1980.

"What's Ahead in Bank Telecommunications." Computers and People. 28(November-December 1979):4-8.

Wiseman, Toni. "Security Called Major Task for National EFT System." ComputerWorld, 21 June 1976, p.7.

"World ATMs Seen Reaching 246,819 by '85, 10 Times '78 Total." American Banker, August 1979.

Zimmer, Linda Fenner. "ATM Boom Ahead." Magazine of Bank Administration, May 1979, p. 33.

Zimmer, Linda Fenner. Statistical Data and Analysis With Selected Case Histories: Fourth Status Report. Parkridge, New Jersey: author, 1977.

Zimmer, Linda Fenner and Trotter, James W. "ATMs: A Strategic Assessment." American Banker, 19 November 1980.

Appendix A

Liability Under the EFT Act (Regulation E)

One of the primary tools in the hands of legislators to protect against unauthorized access to customer-initiated terminals is the allocation of liability for unauthorized use. The Electronic Funds Transfer Act (15 U.S.C. 1693, effective February 8, 1979) as implemented by Regulation E (12 C.F.R. 205, effective March 30, 1979) allocates the liabilities for unauthorized use between customers and financial institutions. The allocation of liability is somehwat complex. The consumer's liability in most cases will be held to $50 or less, but may be $500 in certain cases or unlimited in others.

Under Regulation E, the consumer bears no liability unless 1) the consumer has accepted the access device, 2) the issuing institution has procedures to identify the consumer to whom the device was issued, and 3) the institution has provided the consumer with the appropriate disclosures (which include a description of the liabilities, and a telephone number and address for reporting missing access devices). If these conditions have been met, the consumer may be liable.

In the event that a consumer discovers the access device is missing, the consumer's liability for its unauthorized use may be limited to $50 if the consumer notifies the issuing institution within two business days after discovering the device is missing. However, this liability provision allows a negligent consumer to claim that discovery of the missing device occurred within two days whether it actually did or not, and thereby avoid any liability in excess of $50. If the consumer is willing to admit that the access device was discovered missing more than two business days prior to notification of the financial institution, then the consumer's liability is limited to $500.

In the event that unauthorized access occurs without the consumer discovering the access device was missing, then the date that the unauthorized tranfer first appears on a periodic statement becomes important. The consumer is given 60 days from the date of transmittal of the periodic statement to discover the unauthorized access and to report it to the financial institution. If the consumer notifies the financial institution within 60 days, liability is limited to $50. If the consumer notifies the financial institution more than 60 days after transmittal of the periodic statement, then the consumer's liability is limited

to $500 for unauthorized access prior to expiration of the 60 days and unlimited until notification.

However, in order for the financial institution to impose liability on the consumer for failure to make timely notification of either a missing access device or evidence of an unauthorized use apparent on a periodic statement, the financial institution must establish that it could have prevented subsequent losses had the consumer made timely notification.

Appendix B

Senate Bill 240

(As reported out of the Subcommittee on Criminal Justice 11/6/79.)

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

IN THE SENATE OF THE UNITED STATES

January 25 (legislative day, January 15), 1979

Mr. Ribicoff (for himself, Mr. Percy, Mr. Kennedy, Mr. Inouye, Mr. Jackson, Mr. Matsunaga, Mr. Moynihan, Mr. Williams, Mr. Zorinsky, Mr. Domenici, Mr. Stevens, Mr. Chiles, and Mr. Nunn) 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, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Computer Systems Protection Act of 1979".

Sec. 2. The Congress finds that -

(1) computer-related crime is a growing problem in the Government and in the private sector;

(2) such crime occurs at great cost to the public since losses for each incident of computer crime tend to be far

greater than the losses associated with each incident of other white collar crime;

(3) the opportunities for computer-related crimes in Federal programs, in financial institutions, and in computers which operate in or use a facility of interstae commerce through the introduction of fraudulent records into a computer system, unauthorized use of computer faiclities, alteration or destruction of computerized information files, and stealing of financial instruments, data or other assets, are great;

(4) computer-related crime directed at computers which operate in or use a facility of interstate commerce has a direct effect on interstate commerce; and

(5) the prosecution of persons engaged in computer-related crime is difficult under current federal criminal statutes.

Sec. 3. (a) Chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following new section:

Section 1028. Computer Fraud and Abuse

"(a) Whoever uses, or attempts to use, a computer with intent to execute a scheme or artifice to defraud, or to obtain property by false or fraudulent pretenses, representations, or promises or to embezzle, steal, or knowingly convert to his use or the use of another, the property of another, shall, if the computer:

"(1) is owned by, under contract to, or operated for or on behalf of:

"(A) the United States Government; or

"(B) a financial instituion;

and the prohibited conduct directly involves or affects the computer operation for or on behalf of the United States Government or financial institution; or

"(2) operates in, or uses a facility of, interstate commerce;

be fined not more than two times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned not more than five years, or both.

"(b) Whoever intentionally and without authorization damages a computer described in subsection (a) shall be fined not more than $50,000 or imprisoned not more than five years or both.

"(c) Definitions. For the purpose of this section, the term --

'computer' means a device that performs logical, arithmetic, and storage functions by electronic manipulation, and includes any property and communication facility directly related to or operating in conjunction with such a device; but does not include an automated typewriter or typesetter, or any computer designed and manufactured for, and which is used exclusively for routine personal, family, or household purposes including a portable hand-held electronic calculator.

'financial institution' means

"(1) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(2) a member of the Federal Reserve including any Federal Reserve Bank;

"(3) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(4) a credit union with accounts insured by the National Credit Union Administration;

"(5) a member of the Federal home loan bank systems and any home loan bank;

"(6) a member or business insured by the Securities Investor Protection Corporation; and

"(7) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934."

'property' means anything of value, and includes tangible and intangible personal property, information in the form of electronically processed, produced, or stored date, or any electronic data processing representation thereof, and services;

'services' includes computer data processing and storage functions;

'United States Government' includes a branch or agency thereof;

'use' includes to instruct, communicate with, store data in, or retrieve data from, or otherwise utilize the logical, arithmetic, or memory functions of a computer;

"(d) (1) In a case in which federal jurisdiction over an offense as described in this section exists concurrently with State or local jurisdiction, the existence of federal jurisdiction does not, in itself, require the exercise of federal jurisdiciton, nor does the initial exercise of federal jurisdiction preclude its discontinuation.

CONTINUED

2 OF 3

(2) In a case in which federal jurisdiction over an offense as described in this section exists or may exist concurrently with State or local jurisdiction, federal law enforcement officers, in determining whether to exercise jurisdiction, should conisder --

"(A) the relative gravity of the federal offense and the State or local offense;
"(B) the relative interest in federal investigation or prosecution;
"(C) the resources available to the federal authorities and the State or local authorities;
"(D) the traditional role of the federal authorities and the State or local authorities with respect to the offense;
"(E) the interests of federalism; and
"(F) any other relevant factor.

(3) The Attorney General shall --

"(A) consult periodically with representatives of State and local governments concerning the exercise of jurisdiction in cases in which federal jurisdiction as described in this section exists or may exist concurrently with State or local jurisdiction;
"(B) provide general direction to federal law enforcement officers concerning the appropriate exercise of such federal jurisdiction;
"(C) report annually to Congress concerning the extent of the exercise of such federal jurisdiction during the proceeding fiscal year; and
"(D) report to Congress, within one year of the effective date of this Act, on the long-term impact upon federal jurisdiction, of this Act and, the increasingly pervasive and widespread use of computers in the United States. The Attorney General shall periodically review and update such report.

(4) Except as otherwise prohibited by law, information or material obtained pursuant to the exercise of federal jurisdiction may be made available to State or local law enforcement officers having concurrent jurisdiction, and to State or local authorities otherwise assigned responsibility with regard to the conduct constituting the offense.

(5) An issue relating to the propriety of the exercise of, or of the failure to exercise, federal jurisdiction over an offense as described in this section, or otherwise relating to the compliance, or the failure to comply, with this section, may not be litigated, and a court may not entertain or resolve such an issue except as may be necessary in the

course of granting leave to file a dismissal of an indictment, an information, or a complaint.

Sec. 4. The table of sections of chapter 47 of title 18, United States Code, is amended by adding at the end therof the following:

"1028. Computer fraud and abuse."

Appendix C

The Criminal Law Aspects of Computer Crime

Prepared by Susan H. Nycum
July 1982

C.1 INTRODUCTION

At the outset of a discussion, it is customary to describe the subject matter and define its key terms. In the usual situation that procedure is straightforward and entails a setting down of generally accepted terminology that is well understood by the author and others conversant in the field. Its purpose is to constrain the limits of the discussion and serve as an easy reference point within those parameters.

In the present discussion, however, the task of formulating the boundaries and definitions of the subject matter is precisely the focus of this appendix. A major goal is to address the question, what is EFT crime? Presently, experts are divided in their opinions as to what constitutes EFT crime. One viewpoint is that EFT crime is restricted to those acts that entail an unauthorized manipulation of the computer system whereby data that has been properly inputted to the system is improperly processed. An example of such is a fraud or defalcation accomplished by means of a program that wrongfully diverts funds from one account to another or that attributes a withdrawal from an ATM to a cardholder when, in fact, the withdrawal is made by someone inside the financial institution. Another viewpoint is that EFT crime includes abuses to the input and output process wherein data is altered before it is entered into the system, but is altered for the purpose of perpetrating an abuse that is possible only because the data is to be processed electronically. These data may be amounts of money, names of payees or routing instructions for internal processing. Another approach includes any manipulation of an EFT-related mechanism. An example is Stanley Rifkin who obtained the confidential codes to effect wire transfers and impersonated the legitimate user of the wire transfer mechanism. The broadest viewpoint includes any crime having to do with computers or communications from which a researcher could learn something that would contribute to making EFT safer or more secure to use. This would include muggings at or near ATM's, acts in which legitimate owners of EFT cards or accounts are "conned" into turning over access to the system and breaches of physical security of computer installations.

As a legal matter, the study of computer crime and EFT can be approached from several directions. One direction is to view and describe EFT as an operation. This approach helps to understand how EFT works and relates legal principles to the methods and practices of EFT. A second direction is to view and describe EFT in the context of how and where EFT is different from traditional funds transfers. This approach might begin and end with computer processing and exclude data entry and wire transfers. A third approach is to look at all the existing crime laws that might apply to any of the above definitions of EFT abuses.

A two-step approach is used in this appendix. The first step is to look at EFT from a transaction and function standpoint and to distinguish the consumer and the back office or corporate function. The second step in the analysis is to apply existing state and federal criminal laws to these transactions and functions. It is expected that some immediate and comprehensive applicability will be apparent. It is also expected that some laws will almost, but not quite, pertain to the facts. Because criminal laws are strictly construed, these "almost" situations will not be directly applicable but can be instructive.

C.2 CATEGORIES OF EFT CRIME

EFT consists of two broad categories of transactions. The first category of transactions exists at the consumer level and entails telephone transfers and transactions using consumer-operated access devices such as Automated Teller Machines (ATMs). Crime in this context consists of unauthorized uses of those media. The second category involves the electronic transfer of funds from one corporate locus to another such as bank wire transfers. Crime in this context is described in the report as corporate EFT crime. It is recognized that two basic types of transactions are often integrated in an overall system. Nevertheless for the purpose of this discussion, the functions will be treated separately.

It is useful to distinguish between consumer and corporate EFT crime for two reasons. First, the frequency and the amount of loss associated with criminal occurrences varies between the two. For example, Consumer EFT crime has occurred more frequently, but it has resulted in far fewer dollars being lost in each criminal instance. Secondly, the methodology employed in the two forms of EFT crime has been different. Reported consumer EFT crime has predominantly involved the direct withdrawal of funds from specific accounts in the system by perpetrators using ATM cards.

Corporate EFT schemes, on the other hand, generally have been accomplished by manipulations among accounts by perpetrators posing as authorized transactors with the aid of authorization codes or by internal manipulation to the computer programs that allocate funds to accounts.

Consumer EFT Crime

There have been a number of reported cases involving ATM theft. The most common form of reported ATM theft involves family members, friends, or employees of ATM cardholders. Such persons have frequent access to both ATM cards and their accompanying identification codes. Thus, they may be able to acquire the ATM card, withdraw money from the cardholder's account, and return the card to its correct location without the cardholder's knowledge. Then, the perpetrator simply hopes that the ATM cardholder will overlook the withdrawal, or that no one will discover who actually accomplished the transaction.

More aggressive ATM thefts involve muggings in which the victim is forced to hand over his identification code number. In a case involving a less violent incident a perpetrator observed a cardholder begin an ATM transaction. An accomplice then lured the cardholder away by saying the machine was malfunctioning. As the machine remained activated, the perpetrator was able to complete the transaction and take the maximum withdrawal.[1*]

In another type of fraud one perpetrator opened an ATM account and gave the card to the other who traveled to the San Francisco Bay Area. The second perpetrator then made a large, fictitious deposit to the first's ATM account. As ATMs credit accounts immediately, the second was then able to drive to over twenty ATM machines in the Bay Area and make the maximum withdrawal at each location.[2]

Other ATM theft schemes have involved bank employees who have intercepted ATM cards and identification codes enroute to the account holder. The intercepted cards were each used in several fraudulent transactions before being destroyed. One such scheme allowed a bank employee to make withdrawals for eight months.[3]

Finally, the largest reported ATM theft to date may have involved the use of a counterfeit card or the bypassing of the need for the use of a card within the system. A customer complained the $8,200 was missing from his account. Bank investigation turned up the ATM card inside its original, unopened mailer.[4]

Often consumer EFT crime consists of family members or friends working in concert. Sometimes two friends may be intentionally working together; in other situations, one friend may simply be using another as an innocent dupe. In the latter situation the perpetrator obtains access to both the identification code number and the ATM card of the innocent friend. This can be accomplished by a quick search through the dupe's personal records and wallet or the perpetrator can simply look over the innocent friend's shoulder while the latter makes an ATM transaction. By watching what keys are pressed, the perpetrator learns the identification code number.

Once the perpetrator has both the ATM card and the code number, he simply makes several cash withdrawals and then returns the ATM card to its correct location. Nothing further happens until the innocent friend receives his monthly or quarterly bank statement. The innocent friend may complain to the bank about the absence of funds which he never withdrew.

The bank cannot be sure whether the alleged unauthorized withdrawals were actually made by a third person or whether the ATM card holder simply has forgotten about cash withdrawals which he had, in fact, made. Nor is the bank sure that the cardholder did not make the "unauthorized" withdrawals himself and is now fraudulently claiming he never made them. Finally, even if the cardholder has a pefrect alibi, the bank cannot be sure that the cardholder did not simply hand over his ATM card and code number to his accomplice friend and is now claiming he never authorized the withdrawals.

Corporate EFT Crime

The term corporate EFT crime, as it is used in this report, refers to the unauthorized diversion of funds from wire transfer systems and internal transactions. Thus, the cases of corporate EFT crime reviewed below involve banks. However, corporate EFT crimes may occur outside of financial instutions. Insurance companies, brokerage houses, retail stores and many other businesses employ wire systems that may transfer funds just as bank wire systems.

While the forms of corporate EFT may differ, the methodologies involved in the corporate EFT crimes reported to date have been similar. Although the number of perpetrations reported in this area of EFT crime has been fairly small, the amount of the loss has been large and the potential amount of loss in each crime can be enormous. More than $47 trillion are transferred on bank EFT wires annually

in 25 million separate transactions.[5] Moreover, a simple, large commercial bank transfers $30 to $60 billion each day with an average EFT transaction amounting to $1.9 million.[6] It has been said that the dollar volumes transferred are so large that Stanley Rifkin's $10.2 million transaction was not subject to any special scrutiny because it was of such routine size.[7]

From the cases reported in the Parker-Nycum file, it is possible to identify at least three stages in the execution of a corporate EFT theft. These steps are not intended to present an actual sequence of events in all corporate EFT crime, but rather, are intended to serve as an aid in understanding patterns of activity. This in turn may assist in the effective prosecution of corporate EFT crime.

The first stage in a corporate EFT crime may begin when the perpetrator obtains access to the EFT System. That access may be authorized or may be unauthorized. Typically, the authority is obtained through the acquisition of code numbers or similar access devices. Stanley Rifkin obtained wire transfer code numbers through direct access to the bank's records. However, such direct access is not always necessary. Rudy Guiterrez, a high school dropout from Florida, was able to obtain access codes from Allstate Savings and Loan by calling up bank Brad Schultz and Tim Scannell, employees on the phone. Guiterrez, was later able to transfer $300,000 within the EFT System before being apprehended.[8] Another high school dropout, Adam Ramirez, used a similar scheme in attempting to transfer $1.5 million from Home Federal Savings & Loan.[9]

Criminal prosecution at this stage presents problems. First, it is often quite difficult to discern whether the acquisition of a code number is part of a criminal fraud or theft scheme or whether it is part of a computer technician's legitimate use of an EFT. It is difficult to detect criminal behavior at this stage. Whereas perpetrators of consumer EFT crime are often apprehended with stolen ATM cards in hand, we do not presently know of a case in which a corporate EFT crime perpetrator has been apprehended on the basis of unauthorized possession of code numbers. Moreover, even if corporate EFT criminals were apprehended at this stage, it might be difficult to prove that they actually intended to use the codes for criminal purposes.

The second stage in the perpetration of corporate EFT crime is the actual unauthorized use of the EFT system. It is at this stage that many EFT criminals have been first perceived. For example, when Robert Grant Jones, former controller of a company which Bausch & Lomb had recently

acquired, attempted to transfer $140,000 from Lincoln National Bank in New York to Security Pacific National Bank, Security Pacific employees thought something was wrong. Security Pacific therefore checked with Bausch & Lomb and found that the transaction was not authorized. Mr. Jones was later apprehended.[10] Similarly, when Barry Berenbaum attempted to transfer $2.8 million from the Bank of Nova Scotia in Vancouver to the Crocker Bank, Crocker Bank became suspicious and FBI undercover agents were able to apprehend Berenbaum.[11] Likewise, an attempt to transfer $21 million from Nigeria to the United States and then on to the Bahamas was thwarted when a California bank employee became suspicious and called in the FBI.[12]

The second stage is also the last point at which financial institutions still have complete control of the funds. The situation is analogous to that of a shoplifter who has not yet left the store. The property remains within the system. Yet the thief is able to move the property freely about. However, unlike the shoplifter, whose locus is confined within the walls of the shop, the corporate EFT criminal can rapidly move funds about the globe.

Stage two is therefore a particularly important area for study. As will be discussed in detail later, there are currently 17 state computer crime laws which are available for sanctioning this form of EFT criminal activity. In addition, in interstate and foreign corporate EFT transfers, the Electronic Funds Transfer Law,[13] which regulates EFT Systems, has a specific criminal provision. Unauthorized interstate and foreign EFT transfers have also been successfully prosecuted under the federal wire fraud statutes. Stanley Rifkin, for example, received an 8 year sentence for two counts of wire fraud.[14] However, in the 33 states which lack computer crime laws, adequate sanctioning of unauthorized, intrastate EFT crimes is likely to prove difficult. No "thing of value" has been converted into the control of the criminal. Therefore, it is difficult to characterize the crime as a theft. Moreover, without a "thing of value" having been acquired, fraud and embezzlement statutes are of little value. At best, the prosecution is left with avenues such as malicious mischief or criminal trespass which generally do not provide the strong sanctions required for deterrent purposes.

A third stage which can be identified in corporate EFT crime is the actual conversion of the transferred funds into currency or other material objects of value. At this stage in the crime, there are few prosecutorial problems remaining. The tangible property or currency in hand is proof that a theft has occurred. Moreover, even attempted conversion is

prosecutable under existing laws. One perpetrator who had transferred $78,000 to his own account was apprehended when he tried to cash checks drawn against the account. He was tried for attempting to cash worthless checks.[15] Similarly, Michael Joseph Kelley and Richard Albert Warren were tried for misapplication of funds from a federally insured bank when they were apprehended while attempting to convert into diamonds the $1.1 million they transferred from Beverly Hills to New York.[16] Statutes such as that in Alabama which makes illegal withdrawing or inducing payment of funds mistakenly credited to bank depositor, might also be used.[17]

Another problem at this stage is apprehending the criminal perpetrators. As previously mentioned, Stanley Rifkin was allegedly in possession of some $8 million in diamonds for over one week before any suspicion was aroused in Security Pacific National Bank.[18] During that time, Rifkin had traveled to Switzerland, Luxembourg and back to California with the diamonds in hand.

C.3 STATE LAWS APPLICABLE TO EFT CRIME

The state laws applicable to EFT crime include debit (and some credit) card crime laws as well as 17 computer crime laws. Both categories of laws are discussed below. Of the 17 state computer crime laws, two (those of Kentucky and Tennessee) also have provisions that deal specifically with debit cards and are discussed in this appendix as Debit Card Crime Acts.

Debit and Credit Card Crime Laws

Both ATM and telephone transfers require the use of a debit card or a debit card identification number. A few laws directly sanction debit card crime and some current credit card crime laws contain very broad definitions of the term "credit" card which might extend to debit card transactions.

The most directly applicable card law is a Georgia statute, "Illegal Use of Financial Transaction Cards."[19] In that statute, a "financial transaction card" is defined as follows:

> (1) "Financial transaction card" or "FTC" means any instrument or device, whether known as a credit card, credit plate, bank service card, banking card, check guarantee card, debit card, or by any other name, issued with or without fee by an issuer for the use of the cardholder:

(A) in obtaining money, goods, services, or anything else of value; or

(B) in certifying or guaranteeing to a person or business the availability to the cardholder of funds on deposit that are equal to or greater than the amount necessary to honor a draft or check payable to the other of such person or business; or

(C) in providing the cardholder access to a demand deposit account, savings account, or time deposit account for the purpose of:

(i) making deposits of money or checks therein; or

(ii) withdrawing funds in the form of money, money orders, or traveler's checks therefrom; or

(iii) transferring funds from any demand deposit account, savings account, or time deposit account; or

(iv) transferring funds from any demand deposit account, savings account, or time deposit account to any credit card account, overdraft privilege accounts, loan accounts, or any other credit accounts in full or partial satisfaction of any outstanding balance owed existing therein; or

(v) for the purchase of goods, services, or anything else of value; or

(vi) obtaining information pertaining to any demand deposit account, savings account, or time deposit account.

In addition to this comprehensive definition of financial transaction card, the statute also includes a term entitled "personal identification code" which is defined as a series of numeric or alphabetic codes, a signature, a photograph, a fingerprint, or any other means of electronic or mechanical confirmation used by the holder of a financial transaction card to permit authorized electronic use of that financial transaction card.

In addition to general rules defining financial transaction card fraud the Georgia statute specifically lists the fictitious, forged, altered or counterfeit use of an automatic banking device as a form of credit card crime. It also lists as a crime the false presentation of a financial transaction card or personal identification code. Finally, the Georgia statute makes it a crime to disseminate information concerning financial transaction cards or personal identification codes without the authority to do so.

Of particular note for purposes of this project is the fact that the statute deals directly with electronic criminal methodology and unauthorized ATM-related activity. The statute deals with the preliminary stages of consumer EFT crime such as the unauthorized dissemination of financial transaction card and personal identification code information. It is therefore possible to detect and prosecute perpetrators before an actual breach of an ATM or telephone system arises.

The Georgia statute contains an exhaustive enumeration of EFT-related unlawful activities. This type of statute has two distinct advantages. As it is specific, the exact boundaries of the law are clear. The need for prosecutorial discretion is therefore minimized. Secondly, there are no ambiguous words requiring interpretation by the judiciary. It must be noted, however, that the statute is limited by its very specificities so that new methods of theft from EFT or via telephone and wire transfers might fall outside its purview.

Two other state statutes, that of Kentucky and Tennessee, (which are generally counted among the 17 enacted state computer crime laws) are actually Debit Card Crime Acts. The two statutes are virtually identical. They provide sanctions against thefts including obtaining cards under false pretenses and using such after having reported them lost, falsely making or completing a card and fraudulently signing and/or using a card.

The key definitions used in each statute are:

(a) Automated banking device" means any machine which when properly activated by a "debit card" and/or a "personal identification code" will perform any of the following services:

(1) Dispense money as a debit to the cardholder's savings or checking account; or

(2) Print the cardholder's savings or checking account balances on a statement; or

(3) Transfer funds between a cardholder's savings and checking account; or

(4) Accept payments on a cardholder's loan; or

(5) Dispense cash advances on an open end credit or a revolving charge agreement; or

(6) Accept deposits to a customer's savings or checking account; or

(7) Receive inquiries or verification of checks and dispense information which verifies that funds are available to cover said checks; or

(8) Cause money to be transferred

electronically from a cardholder's acount to an account held by any business, firm, retail merchant, corporation, or any other organization.

(b) "Cardholder" means the person or organization named on the face of a debit card to whom or for whose benefit the debit card is issued by an issuer.

(c) "Debit card" means any instrument or device, known by any name issued with or without fee by an issuer for the use of the cardholder in obtaining money, goods, services and anything else of value, payment of which is made against funds previously deposited by cardholder.

(d) "Expired debit card" means a debit card which is no longer valid because the term shown on it has expired.

(e) "Issuer" means the business organization or financial institution, or its duly authorized agent, which issues a debit card.

(f) "Receives" or "receiving" means acquiring possession or control or accepting as security for a loan.

(g) "Revoked debit card" means a debit card which is no longer valid because permission to use it has been suspended or terminated by the issuer.

(h) "Debit card theft" means taking a debit card without consent and includes obtaining it by any felonious conduct, including but not limited to statutory larceny, common-law larceny by trespassory taking, common-law larceny by trick, embezzlement, or obtaining property by false promise or extortion.

(i) "Falsely makes" means a person who makes or draws, in whole or in part, a device or instrument which purports to be the debit card of a named issuer, but which is not such a debit card because the issuer did not authorize the making or drawing; or a person who alters a debit card which was validly issued.

(j) "Falsely embosses" or "falsely encodes" means a person who, without the authorization of the issuer, completes a debit card by adding any of the matter, other than the signature of the cardholder, which an issuer requires to appear on the debit card before it can be used by a cardholder.

(k) "Electronic Funds Transfer System" hereafter referred to as EFTS system means that system whereby funds are transferred electronically from a cardholder's account to any other account.

(l) "Presentation or Presents" as used herein shall be construed to define those actions taken by a cardholder or any person to introduce a debit card into an automated banking device or merely displaying or showing a debit card to the issuer, a person or

organization providing money, goods, services, or anything else of value or any other entity with intent to defraud.

(m) "Incomplete debit card" means that a part of the matter other than the signature of the cardholder, which an issuer requires to appear on the debit card before it can be used by a cardholder, has not yet been stamped, embossed, imprinted, written, or electronically encoded on it [Acts 1977, ch. 144 2.]

Aside from the Georgia statute described above, there are 11 states with comprehensive credit card crime laws: Alabama, Hawaii, Illinois, Indiana, Iowa, Maryland, Nevada, New Mexico, North Carolina, Rhode Island, and South Carolina.[20] It is possible that some of these laws could be applied to EFT crimes. The statutes all employ a similar definition of the term "credit card," such as that found in the Alabama statute:

> Any instrument or device whether known as a credit card, credit plate, credit card number or by any other name, issued with or without these by an issuer for the use of the cardholder in obtaining money, goods, services or anything else of value on credit.

The use of the words "instrument or device" rather than "object" suggests that the term "credit card" may well be able to include intangibles such as code numbers, which are used in telephone or wire transfers of money, even though the number may never have been stamped directly upon a plastic card. Thus, it appears that the use of credit card crime laws are not necessarily limited to thefts which employ plastic credit cards, but may also be extended to cover any consumer credit related offense employing the use of false identification numbers.

However, a severe limitation on prosecuting EFT crime is created by the inclusion of the term "on credit". The use of a debit card, fraudulently or otherwise, does not provide money, goods, services, or anything else of value on credit. Rather, debit cards only allow the return of monies previously deposited. As criminal statutes are strictly construed, the use of the credit concept prohibits or seriously limits the use of such laws in prosecuting consumer EFT crime.

There are two situations in which an argument might be made that a credit card statute is applicable. The most obvious involves dual function bank cards. Such cards may be used to purchase goods on credit as well as to make

withdrawals from ATMs. The fact that these cards may be used to purchase goods on credit arguably could bring any use of such cards within the purview of the credit card crime laws.

The second situation in which credit card crime laws may be used to prosecute unauthorized debit card use involves the concept of "going negative" and overdraft protection. The ability to go negative is a result of the way ATM systems are set up. ATM systems allow cardholders to withdraw a limited amount of cash whether or not actual funds to cover the withdrawal have been deposited. Some bank accounts when negative activate a customer credit line which is charged to the customer's bank credit card. It is therefore possible to argue that ATMs allow persons to obtain things of value on credit through "going negative."

Computer Crime Laws

There are currently 17 states which have computer crime laws. These states are Arizona, California, Colorado, Florida, Georgia, Illinois, Kentucky, Michigan, Minnesota, Montana, North Carolina, New Mexico, Ohio, Rhode Island, Tennessee, Utah, and Virginia. However, there are major differences among the laws of the 17 states and there does not appear to be any impetus for a uniform state law.[21] To date there have been very few indictments under any of the state computer crime laws, much less convictions. Therefore, in the absence of experience with the laws it is difficult to predict how the courts might interpret these statutes in reference to EFT crimes. The following analysis must, therefore, be taken as interpretive rather than as descriptive.

Two of the computer crime laws, those of Tennessee and Kentucky, have provisions dealing specifically with EFT Systems. They have already been discussed in part in this appendix as Debit Card Crime laws. The Kentucky EFT provision is entitled "Misuse of Electronic Information Prohibited". The Tennessee statute is entitled "Interference with EFTS." The Kentucky provision (which is nearly identical with that of Tennessee) reads as follows:

> § 39-1978. Interference with EFTS - (a) Any person who, with intent to defraud the issuer, the cardholder, or any other entity, intercepts, taps or alters electronic information between an automated banking machine and the issuer, or originates electronic information to an automated banking device or to the issuer, via any line, wire, or any other means of electronic transmission, at any junction or terminal, or at any location within the EFTS system, for the

> purpose of obtaining money, goods, services, or anything else of value, violates this subsection and is subject to the penalties set forth in subsection (b) of 39-1983.
>
> (b) Any person who, with intent to defraud the issuer, cardholder, or any other entity, intercepts, taps or alters electronic information between an automated banking machine and the issuer, or originates electronic information to an automated banking machine or to the issuer, via any line, wire, or other means of electronic transmission, at any junction or terminal, or at any location within the EFTS system, and therefore causes funds to be transferred from one account to any other account, violates this subsection and is subject to the penalties set forth in subsection (b) of § 39-01983. [Acts 1977, ch. 144, § 7.]

This section is applicable to stage two of corporate EFT crimes. It is a crime, under the statute, to intercept, tap, or alter electronic information between an "automated banking device" and the issuer. A definitional problem remains, however, the term "automated banking device" might be narrowly interpreted so as to include only ATMs. On the other hand, the term can be interpreted broadly to include such devices as computers, bank teller terminals, wire terminals, and even electronic cash registers. It is difficult to predict how the courts will interpret the statute's language.

Another computer crime law which is different in nature from the other statutes is Virginia's law entitled "computer time, services, etc., subject of larceny". It reads as follows:

> § 18-2-98.1. Computer time, services, etc., subject of larceny. Computer time or services or data processing services or information or data stored in connection therewith is hereby defined to be property which may be the subject of larceny under 18.2-95 or 18.2-96, or embezzlement under 18.2-111, or false pretenses under 18.2-178. (1978, c686.)

The statute simply defines certain computer-related items as property. However, its simplicity creates some problems. The definition uses broad terms which require further interpretation. In particular, it is not completely clear whether bank account entries stored in a computer constitute data.

More importantly, the statute returns us to the definitional problem of the term "control" which is contained

in theft, larceny and embezzlement statutes. Even if bank account entries are data which may be stolen, it is unclear whether such data is indeed stolen if it remains completely within the system and outside the direct control of the perpetrator who has merely caused a debit entry to be entered in one account and a credit entry to occur in another. The Virginia statute, though potentially quite useful in prosecuting thefts of trade secrets and confidential computer programs, may be of limited value in prosecuting corporate EFT crimes.

Montana's statute[22] is of similarly limited value in prosecuting EFT crime. It provides that electronically produced data, computer programs, etc. have a value and thus can be the subject of theft, etc. But the issue at hand in many EFT crimes is not whether something valuable was taken but whether anything was, in fact, taken at all.

The remaining 13 computer crime statutes vary in their construction but are all of similar value in the prosecution of EFT crime. For purposes of prosecuting corporate EFT crimes, the statutes of the 13 states perform two basic functions. First, they define data, information, etc. as property and therefore make them the subject of theft, larceny, embezzlement, fraud, and other related statutes.

Second, the 13 statutes make unauthorized access, use, modification, alteration, or obstruction of a computer system, computer program, or computer resources a crime if it is accompanied by a criminal mens rea. This permits prosecution at an early stage in the criminal scheme. Moreover, it may provide a strong deterrent to those tempted to perpetrate an EFT crime. It may even help set a standard of conduct for people in the industry.

One foreseeable problem is that courts might define access too narrowly. For example, a court could interpret the term access to require a criminal to directly input signals into the computer network via a keyboard or other input device. Although many states have taken steps to minimize the likelihood of such overly narrow interpretations, some lack these legislative safeguards. Examples of such safeguards are found in the computer crime statutes of California, Georgia, Florida, Michigan, North Carolina, New Mexico, and Rhode Island which make it a crime to "cause to access" a computer as well as to simply "access" a computer. Therefore, it is quite clear that those statutes may be used to prosecute the EFT criminal who causes a bank employee to access the computer system by posing over the phone as someone with the authority to transfer funds, e.g., Rifkin. On the other hand, Arizona and Utah do not have provisions

for causing to access and therefore we must rely on the courts to interpret the statutes broadly. The language of the Colorado and Illinois statutes is even more restrictive. These statutes rely on the term "use" and have no specific provision making it a crime to simply access a computer.

Similarly, many of the statutes explicitly provide that indirect access as well as direct access meets the requirements of the statute. The states which added the "indirect" language were concerned that the naked term "access" might not cover a situation in which the computer criminal substituted a modified tape or disc for the proper one and thereby modified an existing computer program. This method would, for example, be quite useful for the perpetrator attempting the "salami method" of EFT crime in which a modified computer program, which slices of small, unnoticeable bits of money from the system and diverts it to the perpetrator's accounts at frequent intervals, is substituted for the bank's normal programs.

Despite the possible narrow interpretation of the terms access and use, their definitions contain catch-alls such as "or otherwise make use of any computer...." These catch-alls suggest that the broadest interpretation of the statutes is warranted and available for prosecuted discretion.

As a practical matter, however, the prosecution's biggest problem is not likely to be centered around the interpretation of terms such as access or use. Rather, the prosecution is likely to find it extremely difficult to prove the presence of a criminal mens rea. Machines simply do not make good witnesses. Moreover, the technological environment in which EFT systems operate encourages intellectual exploration and curiosity. It will be quite difficult to separate unauthorized criminal access from not unauthorized intellectual curiosity.

C.4 FEDERAL LAWS APPLICABLE TO EFT CRIME

At present, the federal laws applicable to EFT crime include specific sections of the Electronic Funds Transfer Act and the wire fraud and mail fraud provisions of the Criminal Code. A federal computer crime law is currently pending but none has yet passed.

The Electronic Funds Transfer Act

Congress recognized the need for criminal sanctioning of unauthorized EFT transactions and enacted the following provisions within the Electronic Funds Transfer Act of 1978:

916. Criminal liability

"(a) Whoever knowingly and willfully--

"(1) gives false or inaccurate information or fails to provide information which he is required to disclose by this title or any regulation issued thereunder; or

"(2) otherwise fails to comply with any provisions of this title; shall be fined not more than one year, or both.

"(b) Whoever--

"(1) knowingly, in a transaction affecting interstate or foreign commerce, uses or attempts or conspires to use any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument to obtain money, goods, services, or anything else of value which within any one-year period has a value aggregating $1,000 or more; or

"(2) with unlawful or fraudulent intent, transports or attempts or conspires to transport in interstate or foreign commerce a counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument knowing the same to be counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained; or

"(3) with unlawful or fraudulent intent, uses any instrumentality of interstate or foreigh commerce to sell or transport a counterfeit, fictitious, altered, forged, lost, stolen or fraudulently obtained debit instrument knowing the same to be counterfeit, fictitious, altered, forced, lost, stolen, or fraudulently obtained; or

"(4) knowingly receives, conceals, uses, or transports money, goods, services, or anything else of value (except tickets for interstate or foreign transportation) which (a) within any one-year period has a value aggregating $1,000 or more, (B) has moved in or is part of, or which constitutes interstate or foreign commerce, and (c) has been obtained with a counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument; or

"(5) knowingly receives, conceals, uses, sells, or transports in interstate of foreign transportation, which (A) within a one-year period has a value aggregating $500 or more, and (B) have been purchased or obtained with one or more counterfeit, fictitious, altered, forged, lost stolen, or fraudulently obtained debit instrument; or

"(6) in a transaction affecting interstate or foreign commerce, furnishes money, property, services, or anything else of value, which within any one-year period has a value aggregating $1,000 or more, through

use of any counterfeit fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument knowing the same to be counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained--

shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

"(c) As used in this section, the term 'debit instrument' means a card, code, or other device, other than a check, draft, or similar paper instrument, by the use of which a person may initiate an electronic fund transfer."

Part (a) of section 916 is directed toward a different form of EFT crime than that upon which this appendix focuses. That section is concerned with the disbursement of information about bank customers; not with the theft of monies.

Parts (b) and (c) of section 916, however, directly address the form of EFT crime which is the focus of this appendix. Although part (b) creates the specific criminal provisions, part (c) delineates the scope of Title IX's criminal provision by defining "debit instrument". And "debit instrument" is defined broadly to include any non-paper instrument by which a person may initiate an electronic funds transfer. Despite this seemingly broad language, however, problems remain. What is meant by the term "instrument?" The statute lists cards, codes, or other devices. Does a fictitious phone call which causes a bank employee to make an unauthorized funds transfer meet the definitional requirement? Moreover, the term "initiate" is rather vague. Does the rewriting of a program which leads to automatic, but unauthorized funds transfers qualify under the language of "a person may initiate?" We must wait for judicial interpretation. However, one hopes, and presumably Congress intended, the term "debit instrument" will be read broadly enough to include criminal techniques such as the above mentioned.

Even presuming that "debit instrument" will be interpreted broadly, part (b) has a further limitation. The statute is restricted to interstate and foreign funds transfers. Intrastate transfers are not covered by the statute. The prosecutor should attempt to find that interstate commerce has been affected and hopefully this argument will succeed. However, technically intrastate commerce is not included since criminal statutes are strictly construed and construed against the prosecutor in case of doubt. The defense will undoubtedly raise the issue of jurisdiction. At this time, only Kentucky, Montana, New

Mexico, Tennessee and Utah have any criminal provisions in their state EFT acts. The Montana and Utah provisions, however, are aimed only at false or unauthorized disclosures of consumer information. Thus only New Mexico has met the need for a provision similar to section 916(b) and (c). New Mexico statute 58-16-16 reads as follows:

> 58-16-16. Criminal penalty.
> (A) Any person who knowingly and willfully violates any of the provisions of Subsections A or C of Section 12 [58-16-12 A or C NMSA 1978] of the Remote Financial Service Unit Act may be found guilty of a pretty misdemeanor.
> (B) Any person who makes an unauthorized withdrawal from the account of another with a financial institution, or who steals the credit card or account access device of another, or who makes an unauthorized use of the credit card or account access device of another, may be found guilty of larceny.

Section 916 avoids many of the definitional problems of access, use, modify, etc. by including the terms "attempts" and "conspires" to use. Thus, prosecution may be brought at any stage of the criminal scheme. Further, subsections (b)(2) and (3) provide for sanctioning the unauthorized dissemination of code numbers and similar information which might be used in executing an EFT crime. Additionally, Parts (b)(4), (5), and (6) provide sanctions for accomplices who aid in disbursing the fruits of the crime.

Presuming that the term "debit instrument" is interpreted broadly, the Act should prove to be an effective device for prosecuting EFT crime. However, there is a need for similar criminal provisiond at the state level to aid in the prosecution of intrastate funds transfers.

Wire Fraud Statute

18 U.S.C. 1343 (Wire Fraud) -- The wire fraud statute has two essential elements: (1) the use of wire and (2) the purpose of executing or attempting to execute a fraud or a scheme to obtain money or property under false pretenses. The courts have been generous in their definition of what is a fraud. The classic statement on this count was made by Judge Holmes, "[t]he law does not define fraud; it needs no definition; it is as old as falsehood and as versatile as human ingenuity." Weiss v. United States, 122 F.2D 675, 681 (5th Circ. 1941), cert. den. 314 U.S. 687 (1941). When one uses a remote terminal to perpetrate a computer fraud, or when one telephones an accompiice, so long as the "message" crosses state lines, the statute is applicable. All reported

cases involving 1343 have dealt with conversations that crossed state lines, leading one to believe that the message must, in fact, cross state lines. Since 1343 does not use the word "facility," jurisdiction hinges on use of an interstate wire, notwithstanding the fact that "[I]t cannot be questioned that the nation's vast network of telephone lines constitute interstate commerce." United States v. Holder, 302 F. Suppl. 296, 298 (D. Mont. 1969). It is not clear that the use of the word "facility" in any new legislation would embrace interstate calls either, see United States v. DeSapio, 299 F. Supp. 436, 448 (S.D.N.Y 1969) (construing phrase "facility in ...interstate commerce" as requiring insterstate calls for 18 U.S.C. 1952), because there may be a distinct difference between facilities "in" interstate commerce and facilities "of" interstate commerce.

Mail Fraud Statute

18 U.S.C. 1341 (Mail Fraud) -- The mail fraud statute has two essential elements: (1) the use of the mail (2) for the purpose of executing or attempting to execute a fraud or a scheme to obtain money or property under false pretenses. Thus the use of mailings including sending notices, giving transaction confirmations and making money transfers by mail would fall within the making of the mail fraud statute. Both mail fraud and wire fraud are very useful aids to the prosecution of EFT crime.

Other Federal Laws

In addition to the wire fraud and mail fraud statutes, there are other sections of the Federal Code that are potentially applicable to EFT crime. These include:

- 18 U.S.C. 912 Obtaining a thing of value by impersonating an officer or employee of the United States.
- 18 U.S.C. 1001 False representation
- 18 U.S.C. 1005,1006 Making false entry in a bank or credit institution record
- 18 U.S.C. 2113 Burglary of a bank
- 18 U.S.C. 2314 Interstate transportation of stolen property

C.5 LIMITATIONS OF THE TRADITIONAL CRIMINAL LAW

From the experience to date with federal prosecution of computer crime it appears that much of the criminal behavior involving EFT abuse is sanctionable under existing laws.

However, there are loopholes in criminal codes which have plagued the prosecutors of EFT crimes. These loopholes reflect the disparity between the rate of legal reform and technological advance.

An example of such a loophole is found in some of the more common theft statutes. A typical statute of this type reads: "No person, with purpose to deprive the owner of property or services, shall knowingly obtain or exert control over either [property or services]...."[23] The problem is that, at least in its initial stages, EFT crime often does not involve a taking of traditional "services" or "property." Nor is there always a discernable purpose to deprive. Rather, the computer criminal may only have caused a few electronic signals to entered into a bank computer. The results of entering the electronic signals may have been the diversion of some $10 million from Los Angeles to New York, but was there a theft? No money has actually left the bank system. No physical property or service has been obtained. And it is certainly arguable that the bank still exerts sole control over the funds in its system. Moreover, even if a prosecutor can convince a jury that there has been a taking, is there really much evidence confirming a purpose to deprive? The net result is the unauthorized transfer of a vast sum of money with no certain ability to prosecute the transfer as a theft.

A similar situation may arise in traditional definitions of fraud and deceit. Such statutes traditionally require a "willful misrepresentation of material facts to a person." Yet, the EFT criminal may never face a person at all. Any misrepresentations are made to a machine. Moreover, it is often difficult to characterize the giving of incorrect information to a machine as an actual misrepresentation.

Finally, prosecution under traditional forgery statutes is often hindered by the common law requirements of a signature and document. The EFT criminal need not sign anything. The computer criminal may only enter a false entry code and account number into a computer. Nothing is signed. No document changes hands.

The foregoing are examples of some of the problems facing the prosecutors of EFT crime. The list is by no means exhaustive. Nor does the list apply to all jurisdictions; many states have made concerted efforts to redefine theft, fraud, and forgery so as to encompass modern computer crime. The list serves only to point to the kinds of criminal loopholes with which a body of EFT law must deal.

C.6 CONCLUSION

From a legal perspective EFT crime can be considered a subset of computer crime. In this aspect of computer crime, funds that are stored or processed in electronic form are manipulated in order to steal or defraud. The theft or deception may be the stealing of specific funds or the perpetration may be a "kiting" or other scheme. The financial loss may be measured in fifty or one hundred dollar units or in millions depending on the type of perpetrator and the source of funds accessed. The means of the perpetration may be technically sophisticated violations of communications or computer technology such as salami techniques that siphon off parts of a penney from every account every month, or the simple stealing of properly issued codes or devices that access consumer accounts or effect wire transfers from corporate EFT such as in the Security Pacific bank theft by Stanley Rifkin.

The criminal laws invoked will vary depending on the nature and geographic spread of the crime. While many perpetrations are covered by existing law, some of which was specifically enacted to address EFT crime, loopholes and shortcomings in the law still exist. For example, the theft of electronic impulses that represent money is not specifically denominated a crime under any existing federal or state laws.

The data concerning the experience with investigation, reporting and prosecution of these crimes is scattered and lags the occurrences of crime. But the experience is growing. Indeed, in one bank's experiences with ATM fraud, civil prosecution by the bank against depositors resulted in some decisions in favor of the bank and at least one in favor of the depositor. In that latter case, the judge held that the depositor's testimony was preferred to that of the bank's "machine testimony." Subsequently, the Attorney General of the State of New York brought suit against the bank because the bank's ATM system had resulted in a high number of ATM scams.

As the technology advances, the acceptance of EFT increases, and links between and among systems grow, the need for understanding of the experience with EFT crimes will also increase. This need affects both the prosecutor of EFT crime and the victims, including the institutions and the customers.

FOOTNOTES

1. "Electronic Fraud Accompanies Move Toward Tellerless Banking," New York Times, Ralph Blumenthal, March 26, 1978. SRI File Numbers 77344, 77345 and 77346.

* SRI File Numbers are to the Parker-Nycum data base of reported cases of computer abuse which is available to the project.

2. "Two Indicted in ATM Fraud Caper," Computerworld, Catherine Arnst, December 12, 1977. SRI File Number 77329.

3. The Nilson Report, March 1980.

4. PSI Support Services Memorandum from Stanley Rifkin to Don Leonard, July 30, 1976. SRI File Numbers 74329, 75377, 76302, 76303 and 76304.

5. "Bank System: Shrouded in Secrecy," Los Angeles Times, Roger Smith, November 7, 1978, pp. 1,22. SRI File Number 78313.

6. Donn B. Parker, "The Potential Effects of Electronic Funds Transfer Systems on National Security".

7. "Bank's DR Consultant Held in $10.2 Million EFT Heist", ComputerWorld, November 13, 1978, pp. 1-2. SRI File Number 78313.

8. "Dialing for Dollars," New West, Eric Mankin, December 18, 1978, pp. 15-17. SRI File Number 78313.

9. ibid.

10. "X-Controller Admits Guilt in $140,000 Federal Theft," Brad Schultz, ComputerWorld, August 14, 1978, p. 1. SRI File Number 78308.

11. "Man in Bank Theft Plot Gets 3 Years," Los Angeles Times, Robert Rawitch, September 26, 1979. SRI File Number 79310.

12. Computer Fraud & Security Bulletin, June 1980, p. 15. SRI File Number 793XX.

13. 15 U.S.C. 1601 et seq.

14. "Expected Bank Plot to Fail; "Aghast" When Theft Succeeded: Rifkin," Los Angeles Times, Robert Rawitch, February 23, 1979, pp. 1, 27. SRI File Number 78313.

15. "2 DP Crimes Covered in One Day in Nashville," Alan Taylor, ComputerWorld, October 9, 1978. SRI File Number 77350.

16. "Charges Revised in Fraud Case," ComputerWorld, June 18, 1979; and "Still Another Wire Transfer Fraud," EDPACS, July 1979, p. 8. SRI File Number 79312.

17. Alabama's statute reads:

    13-3-62. Withdrawing or inducing payment of funds mistakenly credited to bank depositor. Any person who withdraws or causes to withdraw from any state or national bank any funds which he knows or has reasonable grounds to believe have been credited to the account of a depositor in such bank through mistake or error, or who induces any such bank to pay any such items to any person by making, drawing, uttering or delivering a check, drawn on order for the payment of money, with the intent to so induce such bank shall on conviction be punished as if he had stolen such funds.

18. "The Heist," Bruce Henderson and Jeffry Young, Esquire, May 1981. SRI File Number 78313.

19. See Georgia Code Annotated sections 26-1705 to 26-1705.10.

20. See Alabama Code Title 13, sections 4-32 through 4-41 (1977), Hawaii Revised Statute section 851-10, Illinois Statute Annotated Chapter 121 1/2, section 601 et seq. (Supp. 1978), Indiana Code Annotated section 35-43-41 to 35-43-55 (1979), Iowa Code Annotated sections 715.1 to 715.6 (West Supp. 1978), Maryland Criminal Law Code Annotated section 145 (Supp. 1978), Nevada Revised Statutes section 205.601205.810 (1977), New Mexico Statute Annotated section 30.16.24-30.16.38 (1978), North Carolina General Statutes section 14-1138-.17 (Supp 1977), Rhode Island General Laws sections 11-49-12 to 13 (Supp. 1978), and South Carolina Code sections 16-13-270 and 280 (1976).

21. Computer Law and Tax Report, Robert Bigelow, January 1980.

22. At the time of writing, only House Bill No. 621 was available. The bill was later passed and became law, but may have been modified somewhat.

23. From section 29.13.02 of the Ohio Criminal Code. The Ohio legislature was striving to update this statute at the time this appendix was written.

Appendix D

Example Cases Contained in the SRI Computer Abuse File

FILE 78308 KEYWORD "EFTS"

CONTENTS: Article, ComputerWorld 14 August 1978; article, American Banker 25 May 1978.

SUMMARY: Robert Grant Jones, former controller of a company that Bausch & Lamb had recently acquired, telephoned Lincoln National Bank in New York and identified himself as B&L Treasurer W. Henry Aughey III. He requested a transfer of $140,000 to the account of a third party at Security Pacific National Bank. Jones initiated the transfer by using B&L's Federal Reserve Communications System key code. He was caught when a SP employee thought the transaction seemed funny and called B&L. About a month later the Fed announced that a "complete security program" based on the federal Data Encryption Standard algorithm was planned.

FILE 78318 KEYWORD "EFTS"

CONTENTS: Several sets of notes apparently prepared by SRI.

SUMMARY: Insider/outsider collusion. The outsider called a Beverly Hills attorney and told him that he was negotiating an art deal and would wire money to the attorney's trust account. On a Friday, the insider--a bank clerk--found a large account and wired $150,000 from it by Telex to the trust account. On Monday the attorney picked up the money and gave it to the outsider. The victimized company received notice of the transfer and told the bank it was unauthorized. The perpetrators were caught because the bank clerk acted "suspiciously" in the ensuing investigation. Her friends were questioned and one squealed. A couple of safeguards were bypassed by the clerk but went undetected because they were often ignored. One, all accounts are classified as either authorized or unauthorized for wire transfers. This particular account was not wire transfer authorized, but that safeguard was often ignored because it took too much time. Two, all wire transfers were supposed to be verfied by a telephone call. This was rarely done because of the large volume of wire transfers.

FILE 77350 KEYWORDS "DEPOSIT," "PHONE"

CONTENTS: Notes prepared by SRI; article, ComputerWorld 9 October 1978; article, Nashville Banner 26 September 1978.

SUMMARY: A data processing employee telehponed from another branch and used an assistant manager's PIN code to credit over $78,000 to his account. When transactions came in on bank phones they were tallied immediately, but accounts were only balanced every 24 hours. He was caught when he tried to cash several checks within hours of the "deposit." He was tried for trying to cash worthless checks, not for computer crime, because of difficulties of proving that he had illegally used the EFT system.

FILE 74338 KEYWORD "CREDIT CARDS"

CONTENTS: Article, Ventura County Star Free Press 14 February 1975.

SUMMARY: Defendant found a way to enter high credit ratings into the credit card verification system, allowing him, and many of his friends, to make huge purchases and have them verified.

FILE 78307 KEYWORD "ATM"

CONTENTS: Article, Florida Times-Union 23 February 1978.

SUMMARY: Defendant stole checks from his company and deposited them via teller machine. He was detected when he tried to deposit a huge one inside the bank rather than through the teller machine.

FILES 77344, 77345, 77346 KEYWORD "ATM"

CONTENTS: Article, New York Times 26 March 1978.

SUMMARY: Article describes three ATM crimes -

(1) At Citibank a man put in his card and punched in his number. He was then waved away by another man at the emergency phone who said it wasn't working. The customer walked away leaving the machine activated and the criminal took the maximum withdrawal.

(2) A woman's maid obtained her employer's ATM card and authorization number when they arrived in the mail and used them to obtain money without informing her employer that they had arrived.

(3) After a man withdrew money from an ATM he was accosted and forced to turn over his card and PIN. The crooks withdrew $400.00 from the victim's account even though he only had $127.80 in his account. To save

money the ATM had been "offline"--not connected to the central computer--so the overdraft went unnoticed.

The article also mentioned that people are trying to defraud banks by claiming they never took the money out. It is possible to make this claim because customer's do not leave a signature when they make an ATM withdrawal. However, video cameras are helping to prevent this.

FILES 75377, 74329, 76302, 76303, 76304 KEYWORD "ATM"

CONTENTS: Memo from Stan Rifkin.

SUMMARY: Memo describes five ATM crimes -

(1) Account holder found $1,320 missing from his account. Told bank he though his card was stolen. By blocking the account the card was retrieved the next day.

(2) $1,250 was stolen in $250 daily increments. Card was captured a day or two after the unauthorized withdrawals were brought to the bank's attention.

(3) $8,200 was withdrawn from a customer's account. Customer said he never received his card. Bank had the card inside its original mailer, but not his authorization number mailer. The card used to gain ATM access was never recovered. Possible case of card counterfeiting.

(4) A withdrawal hold on an account was mysteriously lifted and the next day $400 was withdrawn in four $100 transactions.

(5) $1,000 was withdrawn from an account via ATMs. The bank was suspicous because the account holders never used ATMs. The bank found the card and authorization number mailers unopened at the bank. ATMs were programmed to capture the card the next time it was used, but there was no further ATM activity on the accounts. Possible case of insider card counterfeiting.

FILE 78305 KEYWORD "ATM"

CONTENTS: Article, San Francisco Examiner 5 June 1978.

SUMMARY: Woman's account was debited $1,350 by someone who apparently got her ATM card and authorization number. Her complaint and others like it led the House Banking Committee

to consider a bill limiting customer ATM liability to $50. As of the date of the article, customers had no way to prove whether they had made a disputed withdrawal.

FILE 77347 KEYWORD "ATM"

CONTENTS: Article, ComputerWorld 17 January 1977; SRI notes; Letter from SRI to Rivertown Times.

SUMMARY: Customer assaulted an ATM when it did not return his bank card after a transaction.

FILE 77329 KEYWORDS "ATM," "ACCOUNTS"

CONTENTS: Article, ComputerWorld 12 December 1977.

SUMMARY: Bucarz applied for ATM card, then went to California. Gave Richardson his authorization number, told him to pick up the card when it arrived at his home. Richardson made phony deposits by punching in credits to the account and entering blank envelopes. ATMs credit the account imediately, so Richardson was able to withdraw money. He was caught because he bragged about it around town.

FILE 70311 KEYWORDS "ATM," "ACCOUNTS"

CONTENTS: SRI notes; article, Trenton, New Jersey newspaper 3 May 1977; article, Philadelphia Bulletin 3 May 1977; article, Philadelphia Daily News 3 May 1977.

SUMMARY: Head of computer operations set up fake account which he controlled. Then changed the program so it would automatically transfer money to the fak account. It was also reprogrammed to make up the difference and balance the daily accounts.

Appendix E

Federal Regulator Forms

1. FDIC Report of Crime

FDIC FORM P-2 (1971)

FEDERAL DEPOSIT INSURANCE CORPORATION

REPORT OF CRIME

Pursuant to the Bank Protection Act of 1968 and section 326.5(d) of the rules and regulations of the Federal Deposit Insurance Corporation.

This report must be filed within a reasonable time after a robbery, burglary, or non-employee larceny is perpetrated or attempted at an office of an insured State nonmember bank. Copies of such report shall be filed with the appropriate State supervisory authority and four copies of such report shall be filed with the Regional Director of the Federal Deposit Insurance Corporation Region in which the main office of the bank is located.

FOR OFFICE USE ONLY
State _____ Bank _____
Certificate Number (1) _____
Branch (7) _____ Cyrd (11) ___

(Mark or enter the appropriate information. Leave blank non-applicable items.)

1. Name and address of bank head office:
2. If crime being reported occurred at a branch office, give name and address:
3. Type of crime:
   a.(12) ___ Robbery.
   b.(13) ___ Burglary.
   c.(14) ___ Non-employee larceny.
4.(15) (_____ (For office use only)) ____ 19__ Date of crime
5.(21) (_____ (For office use only)) _____ Day of week
6.(22) (_____ (For office use only)) _____ Time of day. (If actual not known, estimate)
7. Amount of loss (to the nearest dollar.):
   a.(29) $_____ Currency loss.
   b.(35) $_____ Securities loss.
   c.(44) $_____ Damage to bank property. (May be estimated)
   d.(53) $_____ Other, specify

(IF CRIME OF ROBBERY HAS BEEN PERPETRATED OR ATTEMPTED ANSWER THIS SECTION)

8.(62) ___ Number of robbers participating in crime.
9. Weapons:
   a. Did robber(s) have weapon(s) or did it appear they may have had weapons?
      (64) ___ No.
      (65) ___ Yes. Specify kind _____
   b. Was other intimidation used?
      (66) ___ No.
      (67) ___ Yes. Specify _____
10. Were robber(s) wearing masks or otherwise disguised?
    a.(68) ___ No.
    b.(69) ___ Yes. Indicate how _____
11. Was a description of the robber(s) obtained and recorded?
    a.(70) ___ Yes.
    b.(71) ___ No. Why? _____
12. Was a description and/or license number of vehicle(s) obtained?
    a.(72) ___ Yes.
    b.(73) ___ No. Why? _____
13.(74) _____ Estimated minutes between beginning and end of robbery.
14. Modus operandi:
    a. Did robber(s) pass a note to teller demanding money?
       (77) ___ Yes.
       (78) ___ No.
    b. Did robber(s) vocally demand money?
       (79) ___ Yes.
       (80) ___ No.
       Card (11) _____ (For official use only)
    c. Did robber(s) subdue employee(s) and take money from containers?
       (12) ___ Yes.
       (13) ___ No.
    b.(14) ___ Other, specify _____
15. Harm to persons:
    a. Were either employees or customers physically harmed?
       (16) ___ Yes.
       (16) ___ No.
    b. Were other persons harmed?
       (17) ___ No.
       (18) ___ Yes. Give details _____
16. Was a hostage or threat of holding a hostage used?
    a.(19) ___ No.
    b.(20) ___ Yes. Give details
17. Was cash or valuables taken from other than teller drawers?
    a.(21) ___ No.
    b.(22) ___ Yes. Specify _____
18. Was "bait" money given out or taken during the robbery?
    a.(23) ___ No.
    b.(24) ___ Yes.
    If yes, was the identification of this money furnished to the law enforcement officers?
    c.(25) ___ Yes.
    d.(26) ___ No. Why? _____
19. Was the cash contained in the teller drawer(s) within the maximum permitted by the bank's security program?
    a.(27) ___ Yes.
    b.(28) ___ No. Why? _____
20. Cameras (or other surveillance device) (check one):
    a.(29) ___ Camera(s) recorded useful pictures during this robbery.
    b.(30) ___ Camera(s) did not record useful pictures during this robbery. Why?

2. Federal Reserve Report of Crime

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
FORM P-2

REPORT OF CRIME

Pursuant to the Bank Protection Act of 1968 and
Section 216.5(c) of Regulation P

This report must be filed within a reasonable time after a robbery, burglary or non-employee larceny is perpetrated or attempted at an office of a State member bank that is subject to Regulation P. One copy of the report must be filed with the appropriate State supervisory authority and one copy must be filed with the Federal Reserve Bank for the District in which the main office of the reporting bank is located.

FOR OFFICE USE ONLY
State (1) ___-___. Bank (3) ___-___-___-___.
Branch (7) ___-___-___-___. Card (11) ___.
FR Dist (12) ___-___. Class (14) ___-___.
Total Deposits (16) ___-___-___-___-___-___.

Check or enter the appropriate information. Leave blank non-applicable items.)

1. Name and address of bank branch office:

2. If crime being reported occurred at a branch office, give name and address:

3. Type of crime:
   a. (24) ___. Robbery.
   b. (25) ___. Burglary.
   c. (26) ___. Non-employee Larceny.

4. (27) (___-___-___-___-___-___) _____ 19__ Date of crime.
   (For office use only)

5. (33) (___) _____ Day of week.
   (For office use only)

6. (34) (___-___-___-___) _____ Time of day. (If (For office use only) actual not known, estimate)

7. Amount of loss (to the nearest dollar):
   a. (28) $___-___-___-___-___-___-___. Currency loss.
   b. (47) $___-___-___-___-___-___-___. Securities loss.
   c. (56) $___-___-___-___-___-___-___. Damage to bank property. (May be estimated)
   d. (65) $___-___-___-___-___-___-___. Other, specify

(IF CRIME OF ROBBERY HAS BEEN PERPETRATED OR ATTEMPTED ANSWER THIS SECTION)

8. (74) ___-___. Number of robbers participating in crime.

9. Weapons:
   a. Did robber(s) have weapon(s) or did it appear they may have had weapons?
      (76) ___. No.
      (77) ___. Yes. Specify kind _____
   b. Was other intimidation used?
      (78) ___. No.
      (79) ___. Yes. Specify _____

Card (11) 1 (For office use only)

10. Were robber(s) wearing masks or otherwise disguised?
    a. (12) ___. No.
    b. (13) ___. Yes. Indicate how _____

11. Was a description of the robber(s) obtained and recorded?
    a. (14) ___ Yes
    b. (15) ___. No. Why? _____

12. Was a description and/or license number of vehicle(s) obtained?
    a. (16) ___. Yes.
    b. (17) ___. No. Why? _____

13. (18) ___-___-___. Estimated minutes between beginning and end of robbery.

14. Modus operandi:
    a. Did robber(s) pass a note to teller demanding money?
       (21) ___. Yes.
       (22) ___. No.
    b. Did robber(s) vocally demand money?
       (23) ___. Yes.
       (24) ___. No.
    c. Did robber(s) subdue employee(s) and take money from containers?
       (25) ___. Yes.
       (26) ___. No.
    d. (27) ___. Other, specify _____

15. Harm to persons:
    a. Were either employees or customers physically harmed?
       (28) ___. Yes.
       (29) ___. No.
    b. Were other persons harmed?
       (30) ___. No.
       (31) ___. Yes. Give details _____

16. Was a hostage or threat of holding a hostage used?
    a. (32) ___. No.
    b. (33) ___. Yes. Give details _____

17. Was cash or valuables taken from other than teller drawers?
    a. (34) ___. No.
    b. (35) ___. Yes. Specify _____

18. Was "bait" money given out or taken during the robbery?
    a. (36) ___. No.
    b. (37) ___. Yes.
       If yes, was the identification of this money furnished to the law enforcement officers?
    c. (38) ___. Yes.
    d. (39) ___. No. Why? _____

19. Was the cash contained in the teller drawer(s) within the maximum permitted by the bank's security program?
    a. (40) ___. Yes.
    b. (41) ___. No. Why? _____

20. Cameras (or other surveillance devices) (check one):
    a. (42) ___. Camera(s) recorded useful pictures during this robbery. _____
    b. (43) ___. Camera(s) did not record useful picture during this robbery. Why? _____

21. Robbery alarm (check one):
    a. (44) ___. Alarm was effective during this robbery. How? _____
    b. (45) ___. Alarm was not effective during this robbery. Why? _____

22. Did robber(s) leave note or other item which was retained and preserved for use of enforcement officers?
    a. (46) ___. Yes. What? _____
    b. (47) ___. No. Explain if necessary _____

23. Was conduct and performance of employees in conformance with Regulation P and the bank's security procedures?
    a. (48) ___. Yes.
    b. (49) ___. No. Explain _____

(IF CRIME OF BURGLARY HAS BEEN PERPETRATED OR ATTEMPTED ANSWER THIS SECTION)

24. How did burglars gain entrance to the premises?
    a. (50) ___. Break-in. Where and how? _____
    b. (51) ___. Other, specify _____

25. Vault (check one):
    a. (52) ___. No apparent attempt was made to gain access to vault.
    b. (53) ___. Penetration of vault wall, floor or ceiling was made or attempted. How? _____
    c. (54) ___. Vault door was opened or penetrated. How? _____
    d. (55) ___. Other, specify _____

26. Were the lights required by Regulation P in good working order and turned on?
    a. (56) ___. Yes.
    b. (57) ___. No. Explain _____

27. Were safe deposit boxes broken into or opened?
    a. (58) ___. No.
    b. (59) ___. Yes. Indicate extent and how _____

28. Money safe (check one):
    a. (60) ___. No apparent attempt made to gain access to contents.
    b. (61) ___. A penetration or an attempted penetration of safe was made. How? _____
    c. (62) ___. Safe door opened or an attempt made to open. How? _____
    d. (63) ___. Other, specify _____

29. Night depository (check one):
    a. (64) ___. No attempt was made to gain access to contents.
    b. (65) ___. Contents taken or attempted by "fishing" or "trapping" methods. How, if known? _____
    c. (66) ___. Night depository penetrated or access door opened. Explain _____
    d. (67) ___. Other, specify _____

30. Burglary alarm (check one):
    a. (68) ___. Alarms were of value in connection with this crime. How? _____
    b. (69) ___. Alarms were not of value in connection with this crime. Why? _____

31. (70) ___-___-___. Estimated length of time during which burglary was being committed. (in minutes)

(IF CRIME OF NON-EMPLOYEE LARCENY HAS BEEN PERPETRATED OR ATTEMPTED ANSWER THIS SECTION)

32. Modus operandi of larceny (check one):
    a. (73) ___. Money or valuables exposed where thief had access. Explain _____
    b. (74) ___. Theft by trick or pretext. Explain _____
    c. (75) ___. Other, specify _____

(ALL BANKS ANSWER THIS SECTION)

Card (11) 2 (For office use only)

33. (12) ___-___-___. Length of time after beginning of crime when call for help was transmitted to appropriate law enforcement agency. (in minutes)

34. (15) ___-___-___. Length of time after beginning of crime before first law enforcement personnel arrived at the bank office. (in minutes)

35. Did law enforcement personnel arrive at bank office before violators had departed?
    a. (18) ___. Yes.
    b. (19) ___. No.

36. Arrests of violators (check all applicable categories):
    a. (20) ___. None have been arrested as of the date of this report.
    b. (21) ___. Some or all arrested before they escaped from the bank office.
    c. (22) ___. Some or all arrested subsequent to leaving the bank office.

37. Would improvements in protection facilities or employee performance be helpful in preventing or handling any future similar occurrences?
    a. (23) ___. No.
    b. (24) ___. Yes. Indicate what plans the bank has to take corrective action _____

38. Set forth below any information about the crime or the protection measures that is not adequately covered previously: (Use additional pages and/or furnish photographs or sketches if necessary to completely describe the crime being reported.)

Signature _____
(Security Officer)

Name (typed) _____

Title _____

Date _____

3. FDIC Internal Crime Report

FEDERAL DEPOSIT INSURANCE CORPORATION REPORT OF APPARENT CRIMINAL IRREGULARITY	FDIC CERTIFICATE NUMBER	DATE OF REPORT
NAME AND LOCATION OF BANK *(Specific Branch, if applicable)*	APPLICABLE SECTION(S) AND TITLE(S) OF U.S.C.	
	PROBABLE AMOUNT INVOLVED	RESTITUTION MADE TO DATE *(If any)*

FULL NAME *(Including maiden name of a married woman)*, POSITION, DATE OF BIRTH, AND SOCIAL SECURITY NUMBER OF EACH APPARENT PARTICIPANT *(Indicate suspects by (S) and those involved but not suspected by (I).)*

NATURE OF IRREGULARITY AND DESCRIPTION OF TRANSACTIONS AND CIRCUMSTANCES *(Be concise.)*

DESCRIPTION OF EVIDENTIAL MATERIAL *(If such material is available in the Bank, indicate the location thereof and the name of the individual controlling the same.)*

PRESENT STATUS OF SUSPECT(S) *(If applicable, indicate date of resignation or discharge; present whereabouts; and place of employment.)*

REMARKS *(Include any information not covered elsewhere which may aid the investigatory agency, i.e., name of officer cognizant of the apparent criminal act and his opinion as to the contributing elements.)*

INVESTIGATORY AGENCY *(having jurisdiction or which has initiated an investigation)*

☐ Federal Bureau of Investigation ☐ U.S. Secret Service ☐ Postal Inspection Service ☐ Other *(Specify)*

NOTIFICATION TO U.S. ATTORNEY	NAME AND DATE OF REPORT, IF ANY *(Sent to other prosecuting authority.)*
☐ Copy attached ☐ No letter prepared as investigatory agency is acting	
SIGNATURE OF EXAMINER *(or other authority)* / DATE	

FDIC 8710/08 (10-75) (PAGE ONE) *Detach Here*

INSTRUCTIONS

I. GENERAL

This form shall be utilized in reporting irregularities. The original of the detachable Report of Apparent Criminal Irregularity form is to be transmitted to the U.S. Attorney or other prosecuting authority as outlined below. Use concise language with emphasis on brevity. After initial identification of apparent participants, last names may be used in subsequent narrative.

II. DISTRIBUTION AND DOCUMENTATION

When a report to the U.S. Attorney *is* required, Examiner will:

1. Prepare cover letter; (refer to Section W, Manual of Examination Policies for sample),
2. Prepare Form and complete to maximum possible extent;
3. Submit to Regional Director:
   (a) Cover letter and attached completed upper original section of Form;
   (b) Page two of Form;
   (c) Copies of exhibits, if necessary;
   (d) Copies of notice to and acknowledgement from bank's fidelity insurer, and any other relevant material.
4. Retain copy of cover letter, page three of Form, and duplicates of other material transmitted to Regional Director in Field Office file in sealed envelope.

When a report to the U.S. Attorney *is not* required, Examiner will:

1. Complete Form (Pages two and three only);
2. Submit to Regional Director:
   (a) Page two of Form;
   (b) Copies of exhibits, if any;
   (c) Copies of notice to and acknowledgment from bank's fidelity insurer, plus any other relevant material.
3. Retain page three of Form plus duplicates of material transmitted to Regional Director in Field Office file.

If additional space is needed for the preparation of a report, the employment of appropriately marked follow-pages, attached to the Form, is acceptable.

Appendix F

New Regulation on Federal Reporting Requirements

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

12 CFR Parts 21, 216, 326 and 563a

Joint Notice of Elimination of External Crime Reports Required Under Regulations Implementing the Bank Protection Act

AGENCIES: The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Federal Home Loan Bank Board, and the Office of the Comptroller of the Currency.

ACTION: Final rule.

SUMMARY: These amendments revise 12 CFR 21.5, 216.5, 326.5 and 563a.5 by deleting the requirement for submission of external crime reports and by replacing it with a record to be prepared by each institution after each attempted or completed external crime and to be filed and maintained in a central location at the main office of the institution. Currently, the five regulatory agencies represented on the Examination Council have regulations which require financial institutions to submit a form report within a reasonable time after the commission or the attempted commission of certain external crimes against those institutions. These form regulations are contained in 12 CFR 21.5(c) (Comptroller of the Currency Form CC-9030-02); 12 CFR 216.5(b) (Federal Reserve Board Form P-2); 12 CFR 326.5(c) (Federal Deposit Insurance Corporation Form P-2); 12 CFR 563a.5(b) (Federal Home Loan Bank Board Form P-2); and 12 CFR 748.5(b) (National Credit Union Administration Form, Appendix to Part 748). All these agencies, excluding the National Credit Union Administration, are now eliminating these forms. The National Credit Union Administration agrees with the rationale for these amendments, but will publish a separate amendment at a later time.

EFFECTIVE DATE: October 6, 1981.

FOR FURTHER INFORMATION CONTACT: Board of Governors of the Federal Reserve System, Stephen M. Lovette, 202-452-3622; Federal Deposit Insurance Corporation, Jesse G. Snyder, 202-389-4415; Federal Home Loan Bank Board, Edward Taubert, 202-377-6527; Office of the Comptroller of the Currency, Peggy L. Shriner, 202-447-1165.

SUPPLEMENTARY INFORMATION: The agencies represented on the Examination Council have reviewed the reporting requirements imposed on financial institutions under the above regulations. These regulations (except for those imposed by the National Credit Union Administration) were originally adopted pursuant to the Bank Protection Act (12 U.S.C. 1881-84). The agencies have determined that certain of these reporting requirements impose unnecessary reporting burdens upon the financial institutions. Accordingly, in keeping with the objective of removing regulations that are no longer justified, all the agencies except the National Credit Union Administration are deleting the requirement that the institution file a "Report of Crime" after the commission or the attempted commission of robberies, burglaries or nonbank employee larcenies. In its place the agencies are imposing the requirement that the victimized institution maintain an informal, internal record of each external crime and file all such records in the main office of the institution. These records will then be available for inspection upon examination of the institution.

The agencies unanimously agree that the Report of Crime can be eliminated with no appreciable detraction from the agencies' ability to supervise the institutions. Since the implementation of the Bank Protection Act regulations in 1969, information on external crimes has been collected by the agencies via the Reports of Crime. The purpose of requiring these reports was to collect data useful in deterring external crimes and to assist in the apprehension of perpetrators; however, the agencies believe that the value of the collected data in establishing methods to deter external crime and to apprehend perpetrators of these crimes has not been sufficient to justify continuing this reporting requirement. Moreover, information on such crimes maintained by the Federal Bureau of Investigation is available to the agencies.

By substituting the informal recordkeeping requirements for the requirement that institutions file a formal Report of Crime, the agencies will lessen an administrative burden on their respective institutions. The institution will simply maintain an informal record of each external crime, file all such records at the main office of the institution and make the records available upon the examination of the institution. It is contemplated that the records will be sufficient for the institution to respond to inquiries as to where, when and what type of crime was committed or attempted; the amount of loss, if any; and whether security measures were appropriate. These records may incorporate, for example, reports prepared by or for others. They will be used by the agency examiners to evaluate the effectiveness of the institution's security devices and procedures.

Regarding matters which may be considered "catastrophic," the agencies will request that the institution notify them by phone or mail of such occurrences; no forms are necessary for this purpose.

Because these amendments delete a reporting requirement and replace it by an informal recordkeeping process, their implementation will have no adverse effect upon banking institutions. To the extent that they will have an effect, the amendments will shorten the time required by bank officers to record the particulars of an external crime. The changes will have no effect on the competitive status of banking institutions. In this light, the agencies have concluded that a cost-benefit analysis (including a small-bank impact statement) regarding the changes is unnecessary. A Regulatory Flexibility analysis is unnecessary because the amendments will have no significant economic impact on small entities. Also, because the amendments lessen the reporting burden on banking institutions and do not mandate specified records, they are in furtherance of and in compliance with the Paperwork Reduction Act of 1980 without Office of Management and Budget clearance. Complete elimination of all recordkeeping requirements relative to external crimes is not feasible because records maintained by the Federal Bureau of Investigation are currently insufficient to pinpoint highly vulnerable individual banking offices in a timely and efficient manner.

Inasmuch as these amendments will benefit banking institutions by deleting reporting requirements and adoption of these amendments will not affect the public at large, the agencies have determined, in accordance with 5 U.S.C. 553, that public procedure requirements and delayed effectiveness are unnecessary and that good cause exists for waiver of the 30-day deferral of the amendments' effective date.

The notices of individual agency actions to amend their respective regulations follow.

Adoption of Amendments:

Office of the Comptroller of the Currency

12 CFR Part 21

12 CFR Part 21 is amended as follows:

PART 21—MINIMUM SECURITY DEVICES AND PROCEDURES FOR NATIONAL AND DISTRICT BANKS

1. The authority citation for Part 21 is as follows:

Authority: 12 U.S.C. 1881–1884.

2. Section 21.5 is amended by changing its heading and by revising paragraph (c) to read as follows:

§ 21.5 Filing by banks of reports and maintenance of records

* * * * *

(c) *Records of external crime.* After a robbery, burglary or nonemployee larceny is committed or attempted at a banking office of a bank, the bank shall keep a record of the incident at its main office. The record may be a copy of a police, insurance or similar report of the incident. Alternatively, the bank may wish to develop its own record indicating the office at which the incident occurred, the type of crime, when the crime occurred and the amount of any loss; whether operational or mechanical deficiencies might have contributed to the crime; and what has been or will be done to correct any deficiencies.

Board of Governors of the Federal Reserve System

12 CFR Part 216

12 CFR Part 216 is amended as follows:

PART 216—MINIMUM SECURITY DEVICES AND PROCEDURES FOR FEDERAL RESERVE BANKS AND STATE MEMBER BANKS

1. The authority citation for Part 216 is as follows:

Authority: 12 U.S.C. 1881–1884.

2. Section 216.5 is amended by changing its heading and by revising paragraph (b) to read as follows:

§ 216.5 Reports and records.

* * * * *

(b) *Records of external crime.* After a robbery, burglary or nonemployee larceny is committed or attempted at a banking office of a State member bank, the bank shall keep a record of the incident at its main office. The record may be a copy of a police, insurance or similar report of the incident. Alternatively, the bank may wish to develop its own record indicating the office at which the incident occurred, the type of crime, when the crime occurred and the amount of any loss; whether operational or mechanical deficiencies might have contributed to the crime; and what has been or will be done to correct any deficiencies.

Federal Deposit Insurance Corporation

12 CFR Part 326

12 CFR Part 326 is amended as follows:

PART 326—MINIMUM SECURITY DEVICES AND PROCEDURES FOR INSURED NONMEMBER BANKS

1. The authority citation for Part 326 is as follows:

Authority: 12 U.S.C. 1881–1884.

2. Section 326.5 is amended by changing its heading and by revising paragraph (c) to read as follows:

§ 326.5 Reports and records.

* * * * *

(c) *Records of external crime.* After a robbery, burglary or nonemployee larceny is committed or attempted at a banking office of an insured State nonmember bank, the bank shall keep a record of the incident at its main office. The record may be a copy of a police, insurance or similar report of the incident. Alternatively, the bank may wish to develop its own record indicating the office at which the incident occurred, the type of crime, when the crime occurred and the amount of any loss; whether operational or mechanical deficiencies might have contributed to the crime; and what has been or will be done to correct any deficiencies.

Dated: September 18, 1981.

William W. Wiles,

Secretary, Board of Governors of the Federal Reserve System.

Dated: August 17, 1981.

Hoyle L. Robinson,

Executive Secretary, Federal Deposit Insurance Corporation.

Dated: September 18, 1981.

J. J. Finn,

Secretary to the Board, Federal Home Loan Bank Board.

Dated: September 17, 1981.

Charles E. Lord,

Acting Comptroller of the Currency, Office of the Comptroller of the Currency.

[FR Doc. 81-28969 Filed 10-5-81; 8:45 am]

BILLING CODE 6722-02-M

Appendix G

FBI Accomplishment Report

FD-515 (Rev. 12-15-80)

ACCOMPLISHMENT REPORT

Submit within 30 days from date of accomplishment

Date _____

TO: **DIRECTOR, FBI**

FROM: **SAC,**

SUBJECT:

Bureau File Number

Field Office File Number

Squad or RA Number

Investigative Assistance or Techniques Used

Were any of the investigative assistance or techniques listed below used in connection with accomplishment being claimed? ☐ No ☐ Yes - If Yes, rate each used as follows:
1 = Used, but did not help
2 = Helped, but only minimally
3 = Helped, substantially
4 = Absolutely essential

1. Acctg Tech Assistance	Rating	6. ELSUR - Title III	Rating	11. Lab Div Field Support	Rating	16. Surveil. Sqd Asst	Rating
2. Aircraft Assistance		7. Hypnosis Assistance		12. Pen Registers		17. SWAT Team Action	
3. Computer Assistance		8. Ident Div Assistance		13. Photographic Coverage		18. Telephone Toll Records	
4. Consensual Monitoring		9. Informant Information		14. Polygraph Assistance		19. Undercover Operation	
5. ELSUR - FISC		10. Lab Div Exams		15. Show Money Usage		20. Visual Invest - Analysis (VIA)	

A. Preliminary Judicial Process (Number of subjects)	Complaints	Informations	Indictments

B. Arrests, Locates & Summonses (Number of subjects)	Subject Priority (See Reverse)		
	A	B	C
FBI Arrests -			
FBI Locates -			
Criminal Summons -			
Number of Subjects of FBI Arrests Who Physically Resisted			
Number of Subjects of FBI Arrests Who Were Armed			

D. Recoveries, Restitutions, Court Ordered Forfeiture or Potential Economic Loss Prevented (PELP)

Property or PELP Type Code *	Recoveries	Restitutions	Court Ordered Forfeitures	Potential Economic Loss Prevented
	$	$	$	$
	$	$	$	$
	$	$	$	$
	$	$	$	$

C. Release of Hostages: (Number of Hostages Released)

Hostages Held By Terrorists _____ All Other Hostage Situations _____

E. Civil Matters

	Government Defendant	Government Plaintiff
Amount of Suit	$	$
Settlement or Award	$	$

Enter AFA Payment Here

F. Final Judicial Process: Judicial District _____ / _____ (Use two letter state abbreviations per U.S. Post Office Guide. For Example - The Northern District of Texas as ND TX. The District of Maine as ME in the state field only.)
District State

Subject 1 - Name -

Subject's Description Code * -

☐ Pretrial Diversion ☐ Dismissal ☐ Acquittal

- Convictions - Enter conviction and sentence data in space at right. If more than four sections are involved, limit to the four most relevant.

☐ Felony ☐ Misdemeanor ☐ Plea ☐ Trial

Conviction: Title	Section	Counts	In-Jail Term: Yrs	Mos	Suspended: Yrs	Mos	Probation: Yrs	Mos	Fine
									$
									$
									$
									$

Subject 2 - Name -

Subject's Description Code * -

☐ Pretrial Diversion ☐ Dismissal ☐ Acquittal

- Convictions - Enter conviction and sentence data in space at right. If more than four sections are involved, limit to the four most relevant.

☐ Felony ☐ Misdemeanor ☐ Plea ☐ Trial

Conviction: Title	Section	Counts	In-Jail Term: Yrs	Mos	Suspended: Yrs	Mos	Probation: Yrs	Mos	Fine
									$
									$
									$
									$

Subject 3 - Name -

Subject's Description Code * -

☐ Pretrial Diversion ☐ Dismissal ☐ Acquittal

- Convictions - Enter conviction and sentence data in space at right. If more than four sections are involved, limit to the four most relevant.

☐ Felony ☐ Misdemeanor ☐ Plea ☐ Trial

Conviction: Title	Section	Counts	In-Jail Term: Yrs	Mos	Suspended: Yrs	Mos	Probation: Yrs	Mos	Fine
									$
									$
									$
									$

Attach additional forms if reporting final judicial process on more than three subjects.

Remarks.

2 - Bureau
2 - Field Office

* See codes on reverse side. Subject description codes in Section F are required only when reporting a conviction.

FBI/DOJ

Property Type Codes *

Code No	Description
1	Cash (U.S. and foreign currency)
2	Stock, Bonds or Negotiable Instruments (checks, travelers checks, money orders, certificates of deposit, etc)
3	General Retail Merchandise (clothing, food, liquor, cigarettes, TVs, etc)
4	Vehicles (autos, trucks, tractors, trailers, campers, motorcycles, etc)
5	Heavy Machinery & Equipment (heavy equipment, computers, etc)
6	Bulk Materials (grain, fuel, raw materials, metals, wire, etc)
7	Jewelry (including unset precious and semiprecious stones)
8	Precious Metals (gold, silver, silverware, platinum, etc)
9	Art, Antiques or Rare Collections
10	Dangerous Drugs
11	Weapons or Explosives
12	Businesses or Assets Forfeited
20	All Other Recoveries (not falling in any category above)

Potential Economic Loss Prevented (PELP) Type Codes *

Code No	Description
21	Blank Negotiable Instruments or Tickets
22	Counterfeit Stocks, Bonds, Currency or Negotiable Instruments
23	Counterfeit or Pirated Sound Recordings or Motion Pictures
24	Bank Theft Scheme Aborted
25	Ransom, Extortion or Bribe Demand Aborted
26	Theft From, or Fraud Against, Government Scheme Aborted
27	Commercial or Industrial Theft Scheme Aborted
30	All Other Potential Economic Loss Prevented (not falling in any category above)

*The case file must contain an explanation of the computation of the recovery value or loss prevented. An explanation airtel must accompany this report if the recovery is $1 million or more, or if the PELP is $5 million or more.

Subject Description Codes *
- Enter Description Code Only When Reporting a Conviction -

Organized Crime Subjects:
- 1A Boss, Underboss or Consigliere
- 1B Capodecina or Soldier
- 1C Possible LCN Member or Associate
- 1D OC Subject Other Than LCN

Known Criminals (Other Than OC Members):
- 2A Top Ten or I.O. Fugitive
- 2B Top Thief
- 2C Top Con Man

Foreign Nationals:
- 3A Legal Alien
- 3B Illegal Alien
- 3C Foreign Official Without Diplomatic Immunity
- 3D U.N. Employee Without Diplomatic Immunity
- 3E Foreign Students
- 3F All Others

Terrorists:
- 4A Known Member of a Terrorist Organization
- 4B Possible Terrorist Member or Sympathizer

Union Members:
- 5A International or National Officer
- 5B Local Officer
- 5C Union Employee

Government Official Or Employees:
- 6A Federal - Elected Official
- 6B Federal - Nonelected Executive Level
- 6C Federal - All Other
- 6D State - Elected Official
- 6E State - Nonelected Executive Level
- 6F State - All Other
- 6G Local - Elected Official
- 6H Local - Nonelected Executive Level
- 6J Local - All Other

Bank Officers Or Employees:
- 7A Bank Officer
- 7B Bank Employee

All Others:
- 8A All Other Subjects (not fitting above categories)

*If a subject can be classified in more then one of the categories, select the most appropriate in the circumstance.

Instructions

Subject Priorities for FBI Arrest or Locates:
- A - Subject wanted for crimes of violence (i.e. murder, manslaughter, forcible rape, robbery and aggravated assault) or convicted of such crimes in the past five years.
- B - Subjects wanted for crimes involving the loss or destruction of property valued in excess of $25,000 or convicted of such crimes in the past five years.
- C - All others

Claiming Convictions Other Than Federal:
It is permissible to claim a local (state, county or local) conviction if the FBI's investigation significantly contributed to the successful local prosecution. A succinct narrative setting forth the basis for claiming a local conviction must accompany this report. When claiming a conviction other than Federal, enter the word "LOCAL" in the "Conviction-Section" block, disregard the number of conviction counts, but enter the sentence in the appropriate blocks. Enter "LF" in the "In-Jail" block for all life sentences and "CP" for all capital punishment sentences.

Reporting Convictions:
Convictions should not be reported until the sentence has been issued. There are two exceptions to this rule. The conviction information can be submitted by itself if:
1. The subject becomes a fugitive after conviction but prior to sentencing.
2. The subject dies after conviction but prior to sentencing.

An explanation is required in the Remarks section for either of the above exceptions.

Rule 20 Situations:
The field office that obtained the process (normally the office of origin) is the office that should claim the conviction, not the office where the subject enters the plea in cases involving Rule 20 of the Federal Rules of Criminal Procedures.

Investigative Assistance or Techniques (IA/Ts) Used:
- Since more than one IA/T could have contributed to the accomplishment, each IA/T must be rated.
- The IA/T used must be rated each time an accomplishment is claimed. (For example - if informant information was the basis for a complaint, an arrest, a recovery and a conviction and if separate FD-515s are submitted for each of the aforementioned accomplishments, the "informant information" block must be rated on each FD-515 even if it was the same information that contributed to all the accomplishments.)

*U.S. GOVERNMENT PRINTING OFFICE: 1982-0-361-233/1888

Other BJS Publications on Computer Crime

Computer Crime: Criminal Justice Resource Manual, NCJ-61550

Computer Crime: Legislative Resources Manual, NCJ-78890

Computer Crime: Expert Witness Manual, NCJ-77927

Computer Crime: Computer Security Techniques, NCJ-84049

END