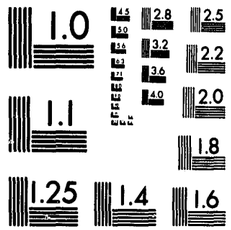
If you have issues viewing or accessing this file contact us at NCJRS.gov.

National Criminal Justice Reference Service

ncjrs

This microfiche was produced from documents received for inclusion in the NCJRS data base. Since NCJRS cannot exercise control over the physical condition of the documents submitted, the individual frame quality will vary. The resolution chart on this frame may be used to evaluate the document quality.



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

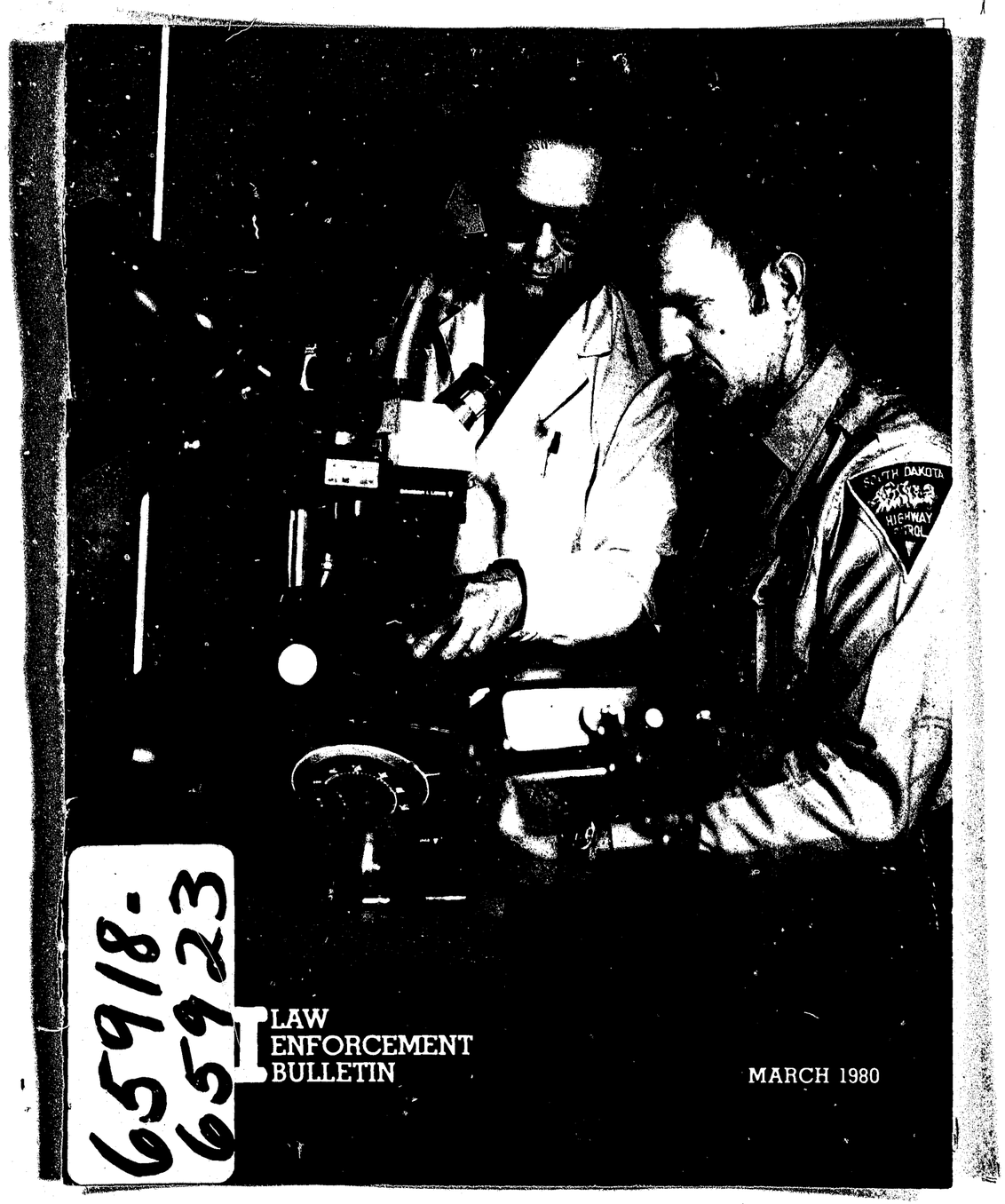
Microfilming procedures used to create this fiche comply with the standards set forth in 41CFR 101-11.504.

Points of view or opinions stated in this document are those of the author(s) and do not represent the official position or policies of the U. S. Department of Justice.

National Institute of Justice
United States Department of Justice
Washington, D.C. 20531

Date Filmed

2/26/81



65918-
65923

FBI LAW ENFORCEMENT BULLETIN

MARCH 1980

NCJRS
MAR 18 1980
ACQUISITIONS

FBI LAW ENFORCEMENT BULLETIN

MARCH 1980, VOLUME 49, NUMBER 3

Contents

The Cover: Law enforcement authorities conduct laboratory examination of speedometer. See article p. 11.

Federal Bureau of Investigation
United States Department of Justice
Washington, D.C. 20535

William H. Webster, Director

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law of the Department of Justice. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget through December 28, 1983.

Published by the Public Affairs Office, Homer A. Boynton, Jr., Executive Assistant Director

Editor—Thomas J. Deakin
Assistant Editor—Kathyrn E. Sulewski
Art Director—Carl A. Gnam, Jr.
Writer/Editor—Karen McCarron
Production Manager—Jeffery L. Summers

ISSN 0014-5688 USPS 383-310

65918

Crime Problems

Security in the Operation of a Bank Card System

By JOHN J. BUCKLEY
Assistant Vice President of Security
Credit Systems, Inc.
St. Louis, Mo.

Security has been defined as "the condition or feeling of being safe or sure; freedom from danger, fear, doubt, etc." Before relating this definition to the bank card field, one should first explore the field to determine how it has become responsible for an estimated one-half of all the retail/credit transactions in the country today.

In the 1960's, banking interests began to distribute plastic credit cards with several new aspects; that is, they were to be issued to customers to whom a line of credit had been extended. The banks would then contract with merchants who would honor these bank credit cards. The merchants deposited the credit card sales documents with the bank and received immediate credit. The banks then charged the cardholder's account and rendered him monthly statements.

By this time the computer had been developed to the point where it could process any credit card transaction within a fraction of a second and these transactions were designed to be handled in great volume. Computers are now capable of processing 9,000 to 10,000 sales documents per hour, around the clock.

Based upon bank credit card experience, banking interests began to explore additional methods by which they could extend new services to customers. Currently being developed are electronic fund-transfer systems, which transfer funds by electronic means from bank to bank. Automated teller facilities, which can be activated with a plastic account card to perform most of the functions in the banking system, are now available. Such plastic cards were initially referred to as "debit" cards for they did, indeed, perform debit instead of credit functions. Banks now refer to any plastics issued by banking interests as "bank cards." Therefore, in discussing the security aspects of a bank card system we will relate in general terms to the security considerations that should prevail when dealing with either debit cards or credit cards.

In the initial system/design phase of bank cards, serious consideration should be given to developing a security "image" or "posture." Banks are dealing with the funds and property of other persons and this requires that security be present and visible. This should, of course, involve a high resolve by top echelon in the bank to seek-out and prosecute those individuals who engage in fraudulent use of the accounts, including bank personnel themselves.

Creation of an Account or Cardholder Base

Why not send account cards to every customer of the bank? Simply, any bank has customers who are collection problems on loans, bad checks, and a host of other problems. To alleviate problems of this type, bank records of prospective cardholders should be evaluated, local credit bureau records should be assessed, and the results evaluated by knowledgeable credit personnel. Customers who have not had recent dealings with the bank should be contacted to ascertain whether the address on file is correct. Banks have, on occasion, issued cards to persons who were deceased.

Additionally, a method should be devised to record and index rejected applications so that future applications can be evaluated in light of prior rejections. One person in a midwestern city recently submitted some 37 applications for bank cards to several banks in the city. Inquiry into the matter revealed that the applications were mailed from various parts of the country within a 3- or 4-day period. The applicant claimed to be a professional man of some means with a local address that was later found to be a parking lot. U.S. Postal authorities took the man into custody at the airport as he was preparing to leave the city after having fraudulently used a credit card he had obtained by falsifying an application.

Development of the Merchant Base

Files of early bank card issuers contain tales of the rush that occurred to "sign up" merchants who would accept the bank card transactions. They found that some of these merchants were merely "fronts" set up for the purpose of fleecing banks. A visit to a prospective merchant by bank personnel can verify the validity of the merchant's request. Empty shelves covered with drapes and the vague statement that the merchandise is "on order" should alert bank personnel to postpone activating the card until visible business interests are present.

Once a merchant's account has been approved, arrangements should be made to code the account through the computer. This enables the bank to have some expectation of the volume of business likely to be generated by the merchant. When these criteria have been established, arrangements should be made to bring any exceptions to the attention of the bank for evaluation.

Security personnel should be trained to conduct seminars for merchants in specific shopping areas or zones. Local police and retail merchant organizations can be of great assistance in arranging these seminars, which are invaluable tools in educating merchant personnel in elementary security procedures at the store level.

Procurement and Distribution of Plastic Cards

Having reviewed some of the elementary security considerations in the initial development of the bank card system, we must consider the phase of the bank card operation that could, if improperly designed and implemented, subject the entire card operation to a series of intolerable security failures. We may have established the tightest cardholder and merchant controls imaginable in the confines of the bank or service center, but unless we pay meticulous attention to every security phase of the procurement, processing, and distribution of the plastic cards themselves, we could endanger the entire operation.

Most bank card issuers use established plastic card manufacturers as sources for their cards. These companies must adhere to strict manufacturing, processing, and shipping specifications in dealing with bank cards. The manufacturers are periodically inspected to insure that all specifications are being followed. Many such manufacturers handle every phase of the manufacturing and distribution of the plastics. Some bank interests will purchase the raw plastics, process them, and then mail them from their own facilities. It is imperative, though, that each step in the handling process be clearly defined and continually inspected to insure the safe handling of the plastics. Audit trails should be established so that any unaccounted plastics are quickly identified and the matter immediately resolved.

The department of the bank that handles both the operation of the accounts and returned cards should be located in a limited access area. One can forecast the danger of having cards returned to the unprotected environment of a bank reception area open to all customers. When bank card operations are handled by a service bureau, the processing area for the cards should be in a limited-access area.

Most cards are distributed through the U.S. Mail. During the initial phases of the system design, local postal authorities should be consulted for advice as to logical days to place the cards in the mail stream. They can also identify areas where mail thefts are prevalent and cards for these areas should be delivered by bank messengers, etc. Grouping mail by ZIP code number not only assists the Post Office in the prompt handling of the mail but financial credits can also be gained by mailers who presort their mail. Getting the plastic into the mail quickly with a minimum amount of handling after it leaves the bank's control minimizes the chances of the mail being improperly delivered.

Reporting and Recording Lost and Stolen Cards

At this juncture, presuming we have implemented every imaginable technique to validate that our cardholder and merchant bases are legitimate and have taken every known precaution in the distribution of the plastic cards, one might surmise that we have only to sit back and wait until

John J. Buckley

James P. Dowd
Executive Vice President & Treasurer
Credit Systems Inc.

something happens to require security to go into action. Inevitably, some plastics are going to be stolen or lost, and a system for reporting losses must be developed. When a plastic is reported lost, stolen, or otherwise in errant use, the initial process should be the completion of an approved form. This information should then be put into the computer so that an "exception report" will generate a printout of each transaction on the account. This printout should be evaluated by security personnel so that fraudulent sales can be identified and recorded, and the sales documents can be retrieved for the scrutiny of investigative personnel. At this point, the initial lost or stolen report is a significant element, since the investigator will, in most instances, desire to interview the cardholder regarding the circumstances of the card loss.

Between 70 and 80 percent of the plastics involved in fraud have been stolen from cardholders, making the theft of cards the greatest security threat. Cardholders should be encouraged to report promptly the loss or theft of their plastics to local law enforcement agencies. Many bank card frauds have been curtailed because a well-informed, local law enforcement agency has recovered errant cards from burglars, pickpockets, or purse snatchers during what would normally be a routine police matter.

Bank card security personnel should consider developing a program of regularly alerting cardholders to the danger of misplacing their cards. This could be accomplished by including a carefully worded message on the monthly account statements. A well-informed cardholder, continually reminded by such messages and by contacts with bank system personnel, can be a great asset in any bank card system. Security personnel investigating fraudulent practices probably have more day-to-day contact with cardholders than any other department in the bank. Security personnel should be encouraged to make good use of these contacts.

Many invalid plastics are retrieved by store clerks. Most bank card systems provide for rewards to be paid to merchant personnel when they succeed in retrieving these invalid cards.

In any event, a number of cards are returned to banks each day via returned mail, sometimes without prior notification. A system must be developed to handle such plastics under secure conditions. Most banks and service centers have secure mail boxes in which recovered cards can be deposited until later handled by security personnel. The bank is quick to recognize the danger of improperly handling returned "live" plastics, especially after one of its employees becomes involved in credit card fraud.

Detection of Fraud Usage

While we have discussed the most rudimentary phases of developing the bank card security system, we must now turn our attention to some of the more intricate aspects of the protection of the bank's accounts; that is, the detection, investigation, and prosecution of persons who are using accounts fraudulently.

Just as the system has, with the magic of the computer, been designed to handle a great number of financial transactions in a minimum amount of time, security personnel must use the magic of the computer to assist them in controlling fraud. We should be able to categorize and identify the types of merchants, geographical areas, and times and places such fraud is likely to occur. Computers can be programed to categorize fraud transactions in any imaginable manner for any given time.

We have discussed that the computer can be programed to monitor the merchant accounts and to report exceptions to recorded criteria in merchant activity. A program can also be designed to report any exceptions to data set forth on the cardholder file.

Information regarding cardholders who exceed the credit line, make purchases in excess of a given number within a certain time period, or make over-the-floor purchases exceeding a given limit should be furnished to account monitors for evaluation. Additionally, some systems are programed to mail to the cardholder a "first use notice," on a new account, ostensibly to thank the customer for using the card. However, this notice could also alert him to unauthorized usage of his card.

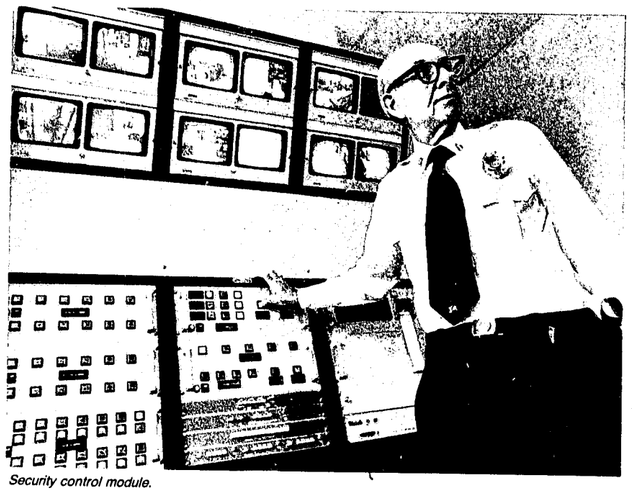
Fraud is sometimes detected after an alert cardholder has noticed that his card is missing, the account has been statused on the computer, and subsequent sales activity generates an exception report for evaluation. Once the fraud has been detected, immediate steps should be taken to place the account number on any available list of wanted cards, or arrangements should be made to notify promptly merchants of the illegal use of the card. Two major bank card systems have developed regular wide-spread listings of restricted or wanted account card numbers.

Prosecution for Fraudulent Use of Accounts and Cards

Prosecution for fraudulent use of bank cards lies with local city, county and/or State prosecuting officials and/or with the offices of the U.S. attorneys where Federal laws have been violated. Federal prosecution is usually handled by U.S. postal inspectors and is usually confined to large-scale fraud operations between several States or to matters that involve the theft or misuse of the U.S. Mail. Postal inspectors are very capable contacts for implementation of security efforts in exercising fraud control.

The greater majority of prosecutions for fraudulent use of bank cards is handled by local city, county, and State prosecuting authorities, who will usually require a written police report. Many prosecutors will accept well-prepared reports of experience bank card security investigators, along with reports of investigating police officers.

Investigators checking account numbers through microfiche.



Security control module.

Once the fraudulent tickets have been accumulated by the security investigator, he should consider an in-depth interview of the cardholder to obtain details concerning the loss of the card and any pertinent information that might lead to establishing the identity of the unauthorized card user. Cardholders should be advised to report their losses to local police agencies. Any hesitancy to do this should give rise to the suspicion that there is no actual errant card involved in the alleged fraud transactions.

The most logical sources for information concerning the fraud user are the clerks who actually handled the questioned sales. Interviewing clerical personnel in large volume outlets in an effort to determine who purchased items described on a sales ticket as "mdse" several weeks prior to the interview is usually nonproductive, while interviewing low-volume merchants regarding the sale of an item that is well-described in the sales document could be more productive. An experienced bank card investigator will become familiar with the sales and merchants from whom he can hope to develop information relating to the sale. Merchants should not be interviewed by telephone; nothing in the business can take the place of a well-planned and executed personal interview. At the conclusion of the interview, the investigator's notes should be reviewed in order to discern whether there are other logical things that the merchant personnel can recall about the transaction.

Plant Protection

The bank card operation should be subject to very tight access control. In the event the bank operates its own bank card department, the department should be apart from other sections of the bank and be in an area where the access is limited to those who have a legitimate need to be there. The area where the plastics are processed should be an area where access is limited to management personnel and those actually performing card-handling duties. A facility being used to house the bank card operation should be subject to 24-hour guard protection, and access to the facility should be limited to those employed at the plant and those having legitimate business interests there.

It is strongly recommended that the card storage area, the card processing area, and the computer room be a limited access area within the facility. Access should be limited to management personnel, maintenance personnel accompanied by employees, and to employees actually working in those areas. A sign-in and sign-out book will limit those going into the area.

In any type of operation it is most necessary that the information put into the system be under the strictest controls. Most computer entries in the systems today can be accomplished by hardcopy, computer tape, and/or by terminals with typewriter keyboards. Sign-in codes that limit access to the system are a must, and these codes must be revised on a regular basis to guard against compromise. The output of the system must also be subject to strict controls. Printouts that show account and financial data should be shredded, as should the carbon paper used in the printout process. Computer programs should be indexed and stored in a limited-access file or library, and a record of persons using these files should be maintained. Backup tapes for emergency use should also be stored at an offsite library.

There are many documents which set forth security guidelines in connection with computer installations. Security personnel should insure that these documents are reviewed periodically, that plant protection measures are followed, and that audit trails are maintained. Security personnel should follow these trails in the event of a breech in the security of an installation.

Every well-designed bank card security operation should have a published emergency plan disseminated to management employees so that every employee knows what is expected in the event of an emergency. Security representatives are responsible for the design and implementation of such an emergency plan.

Conclusion

Bank card security is a challenge to the security professional. The field is as modern as the computer, and there are new developments each day. The professionals in the field today were, for the most part, in another field 10 to 15 years ago. There will always be a need for trained, professional security personnel in the bank card field.

Security personnel now in the field and those interested in such positions should consult with local bankers regarding courses in bank card security being offered by the American Bankers Association, the Bank Administration Institute, and by colleges and universities in the country.

Membership in the International Association of Credit Card Investigators, which includes members from many parts of the world, has greatly enhanced the performance of many bank card security professionals. Seminars conducted at the various regional and national meetings are invaluable tools for the individual engaged in the investigation of fraudulent bank card practices.

The banking industry has been greatly influenced by developments in the bank card field and by the experience it has gained in the field. Bank card security personnel have made major contributions to the field by the measured application of sensible security procedures. **FBI**

END