CREDIT/DEBIT/ATM CARD FRAUD

Overview

This Bulletin:
* Provides an introduction to Credit/Debit/ATM Card Fraud and a glossary of terms related to the credit card industry.
* Outlines current credit card schemes.
* Identifies related state statutes and Department Special Orders.
* Outlines procedures for processing credit card fraud cases including case report writing, preliminary investigation, and the recovery of documents.

GLOSSARY

Altered Card - a legitimately issued card which has been re-embossed, re-encoded, and/or otherwise modified to reflect a name, account number, expiration date, and/or signature other than the valid cardholder’s account information.

ATM - Automated teller machine.

ATM Card - A bank card that has no Visa, MasterCard, or other logo which is used for ATM transactions and certain limited purchases with the use of a PIN.

NOTE: For the purpose of this Education & Training Bulletin, a card that functions as an "ATM Card" but also has a Visa, MasterCard, or other logo will be referred to as a debit card.

Authorization - a process by which a transaction for a specified amount is approved by a card issuer for a merchant.

Bank Card - a card, such as a credit, debit, or ATM card, issued by a financial institution.

Card Activation - an alternative bank card delivery method in which issuers wait to confirm that a card has been received by the valid cardholder before activating the account. Cards are blocked at the time of mailing. For a card to be activated, the cardholder must call the issuer to confirm receipt and provide proof of identity.

Cardholder/Account Holder - the person or entity whose name is embossed on the face of a card or encoded on the magnetic stripe by the issuer.

Card Security Features - alphanumeric, pictorial, and other design and functional elements on bank cards, the exact physical dimensions and placement of which are specified by the company and are difficult to copy exactly. Card security features should be checked by merchants at the point of sale to ensure the card is valid.

Code 10 - the term used by merchants when they call an authorization center to let the center know they are suspicious of a card, cardholder, or transaction. Code 10 calls are generally switched to issuers for special handling.

Counterfeit Card - a payment device that has been fraudulently printed, embossed, and/or encoded to be used as a valid card.

Credit Card - a plastic card enabling the cardholder to obtain money, goods, or services, normally under a line of credit established by the card issuer. The
cardholder is billed periodically for any outstanding balance.

**Debit Card** - a plastic card enabling the cardholder to purchase goods or services, the cost of which is immediately withdrawn from his or her bank account. In addition, a debit card normally serves the functions of an ATM card.

**Electronic Data Capture** - an electronic system that uses a data-capture terminal located at a merchant's place of business to record and authorize transactions.

**Hologram** - a security feature that is a photographic image which appears to be three-dimensional when rotated and appears to move when tilted back and forth.

**Issuer** - a financial institution or commercial organization that issues bank cards, e.g., Citibank, Amalgamated, United Airlines Credit Union, etc.

**Magnetic Stripe** - a strip of magnetic tape on the back of the card. The stripe is encoded with identifying account information. On a valid card, the account information on the magnetic stripe matches embossed information on the front of the card.

**Personal Identification Number (PIN)** - an alphabetic and/or numeric code which may be used as a means of cardholder identification.

**Point of Sale (POS)** - the location at which the sale/transaction takes place.

**Transaction** - the act between the cardholder and merchant or cardholder and financial institution which results in the sale of goods or services.

**METHODS OF FRAUD**

With the proliferation of bank cards comes the expansion of credit/debit/ATM card fraud. Some of the common fraud schemes follow:

**Account Takeover:** This is an unauthorized takeover of an account including an unauthorized change of address.

The criminal gains access to the account information of a valid cardholder, often taking a monthly statement from the cardholder's mailbox. Posing as the cardholder, the criminal then contacts the issuer to request a change of address and an additional card in a second name. The criminal may also request a Personal Identification Number (PIN) for making cash withdrawals at automated teller machines.

**Altered Card:** This is a genuine credit/debit card manufactured by a certified printer that has one or more features changed by mechanical or electronic means. Criminals use a variety of methods to alter a card, usually by applying heat to flatten it out and embossing a new number.

**Counterfeit Card:** This is a card that is illegally manufactured, embossed, and sometimes encoded with information that has been electronically compromised. (See "Skimming.")

**Fraudulent Applications:** This is a fraud that occurs by obtaining a bank card through misrepresentation of information provided to the issuer on the application. Use of a true name with a false address on the application is a common way to obtain the card illegally. An example of this fraud involves organized gangs obtaining several different telephone numbers in one apartment, then applying for cards using one or more of the telephone numbers as the fraudulent applicant's work number. A gang member is always available in the apartment to "confirm" the applicant's place of employment.

**Lost/Stolen Cards:** These involve transactions on a card that has been reported lost or stolen by the cardholder. Bank cards are often stolen from glove compartments of parked cars, from a jacket or purse left unattended or unsecured in the workplace, from recreational facilities, health clubs, golf courses, etc., or during thefts from the person.

**No Card Present Fraud:** This is a fraud that occurs on an account where the card is not physically present for the transaction, such as purchases via the telephone, mail, or Internet. The account number is
valid, but its use is not authorized. This is a popular fraud used to obtain computer and electronic items, jewelry, and other high priced goods via the mail.

**Not Received Items (NRI):** These are transactions on a new or replacement card that was mailed to, but not received by, the cardholder, and that was not returned to the issuer. Frequently, mailboxes in apartment blocks are favorite targets for credit card thieves. Cards are also compromised at mail and postal facilities. Sometimes the thief knows when the cards are being delivered and follows the letter carrier’s route.

**Skimming:** This is a counterfeiting technique in which the account information encoded on the magnetic stripe of a valid card is copied onto the magnetic stripe of a counterfeit card. Because the magnetic stripe of the counterfeit card contains an exact replication of the data encoded on the genuine card, issuers’ authorization processes are deceived into believing that the counterfeit card is genuine. A number of easily accessible small electronic devices are used by the criminal to obtain valid magnetic stripe data. The most common skimming scenario involves data compromised at a merchant location for a legitimate transaction with the card owner unaware that the account information has been compromised.

**PALM SIZE DATA CAPTURE DEVICES**

The items pictured to the right are data capturing devices recovered in various criminal cases around the world. Each of these devices can be used to copy and store data from the magnetic stripe of credit, debit, ATM, and other cards. Some can be used to write data onto the magnetic stripe of genuine, altered, or counterfeit cards. Pager size devices are also in circulation.

*When you come across such devices, handle them carefully.* If unsure, do not touch any switches, press any buttons, or attempt to open the device. There may be built-in self destruct features, which, when activated, delete the data in storage and ruin chances of collecting valuable evidence. As with all computer equipment, any attempt to extract data from these devices should be done by a technician from the Crime Analysis Technical Group of the Detective Division.

Be aware of counterfeit manufacturing paraphernalia such as blank or printed cards, lists of accounts, and computer equipment including diskettes, CD writers, notebook computers, and cables, which can provide vital clues to the magnitude of counterfeiting activity.
**PRELIMINARY INVESTIGATIONS**

When responding to a call regarding credit/debit/ATM card fraud:

1. Follow procedures outlined in the Department Special Order entitled "Recovery of Altered, Lost or Stolen Credit/Debit Cards."

2. Examine the card in question, look for identification and security features. Refer to the Card Security Features guide attached to this bulletin.

3. Check the status/validity of the card by calling the appropriate Law Enforcement Hotline for Visa, MasterCard, Discover, American Express, etc.

   **LAW ENFORCEMENT HOTLINES**

   - American Express 1-800-528-2121
   - Diner's Club 1-800-525-9040
   - Discover 1-800-347-3102
   - MasterCard 1-800-231-1750
   - Visa 1-800-FOR-VISA

   If the card was issued by a local merchant, e.g., Carson's, Marshall Field's, or Sears, contact the issuing merchant for verification. For merchant telephone numbers, refer to the addendum to the Department Special Order entitled, "Recovery of Altered, Lost or Stolen Credit/Debit Cards." Document the name of the person contacted. If unable to make contact, indicate this in the narrative of the case report.

   The associations, e.g., Visa and MasterCard, do not maintain account records and information on the account holders, but are able to provide the name and phone number of the issuing bank based on the account number. Department members can contact the associations on their Law Enforcement Hotlines to obtain information on the issuing bank.

   When contacting the issuing bank, Department members should request to speak with a fraud investigator who can provide the necessary information and serve as a witness, if necessary. Since account holder information is confidential, the issuing bank may not release the account holder's address and telephone number. Instead, the fraud investigator may request the law enforcement officer's name and phone number in order for the account holder to contact the officer.

**CASE REPORTING AND CHARGING**

Complete the appropriate case report and refer to the current Incident Reporting Guide for the applicable Offense/Incident Classification.

**Classification:**

- For fraudulent use of, or possession of credit or debit cards with intent to defraud, complete a General Offense Case Report, using IUCR Code 1150, Primary Box: Deception; Secondary Box: Use of Stolen, Lost, Fictitious Credit Card. The appropriate state statutes are found under 720 ILCS Act 250, the Illinois Credit Card and Debit Card Act.

- For fraudulent use of an ATM card, complete a General Offense Case Report, using IUCR Code 1152, Primary Box: Deception; Secondary Box: Illegal Use Cash Disp. Card. The appropriate state statute is 720 ILCS 5/16-1(a) (4), Theft.

- For possession of any ATM card with intent to defraud, complete a General Offense Case Report, using IUCR Code 1151, Primary Box: Deception; Secondary Box: Possession Cash Disp. Card. The appropriate state statute is 720 ILCS 5/17-1(C)(4), Deceptive Practices.

**Address of Occurrence:** In general, the address of occurrence is the location where the property changes possession (or the attempt, if unsuccessful). Normally, this will be the address of the merchant where the face-to-face transaction occurred. In cases of mail orders, the address to which the merchandise was delivered should be the address of occurrence. If contacted by an account holder who has been informed that his account number was used fraudulently, but does not
know where, the account holder's address may be used as the address of occurrence.

**Victim:** Credit/debit/ATM card fraud is often reported to the police when it is yet undetermined what party will sustain the financial loss: the merchant, the account holder, or the bank card issuer. Unless the circumstances of the case dictate otherwise, the party that contacted the police will normally be listed as the victim.

**Witnesses:**
- The person to whom the fraudulent card was presented is needed as a witness for prosecution.
- When the merchant is reporting the offense, the account holder must be contacted and listed as a witness on the case report. The account holder must verify that he did not authorize the offender to have or to use the card.
- For cases in which the card is suspected to be counterfeit or altered, an agent from the issuing bank must be contacted to verify that the card is counterfeit or altered and to state the specific reasons for the determination.

**NOTE:** The State's Attorney's Office requires the name, sex, race, home address, date of birth, and social security number for every victim and witness involved in the case. Whenever an offender is in custody, the preliminary investigator should obtain this information from all victims and witnesses.

**Narrative:**
- Document all pertinent data in the narrative, including the name of the issuing company, the name of the cardholder, the account number embossed on the card, how the card came to the attention of the Department, and in arrest situations, charges and court information.
- It is important to include all identifiers on the offender, such as driver's license or state ID numbers. Any statements or admissions made by the offender to witnesses or the arresting officers should also be recorded in the narrative.

**EVIDENCE**

In cases with no arrest, the bank card and other related documents, if possible, should be held by the victim for the follow-up investigator. If it is necessary to inventory the evidence immediately, the preliminary investigator should ensure that the complainant has a legible photocopy of the documents for review by the follow-up investigator.

If an arrest has been made, inventory the bank card and related documents, any photos or videotape of the offender, etc., according to Department directives. The preliminary investigator should hold legible photocopies of all inventoried documents for the follow-up investigator.

**NOTIFICATIONS**

Notify the Detective Division for:
- Felony arrests.
- Major thefts of $10,000 or more.
- Newsworthy occurrences requiring immediate attention.
- Recovery of altered, lost, or stolen credit/debit cards if an offender is in custody.

Notify the U.S. Secret Service on Pax 0551 for cases involving altered or counterfeit credit cards or bank cards, in accordance with the Department Special Order entitled, "United States Secret Service." Photocopies of the card in question should also be available for forwarding.

**Contributors:**
Detective Mark Reiter (630)
Detective Maria Jacobson (650)
Detective Thomas Manaher (606)
Detective Mary L. Schuler (606)
Detective Darlene Vosis (630)
Police Officer Diane Tamberlin (124)