FRAUD/ IDENTITY THEFT

CREDIT CARD FRAUD (IN PROGRESS)

- Many fraud rings involve individuals that are involved in other criminal activities. (burglary, robbery, theft, etc.)
- Interview the clerk to determine what happened and why he or she suspects fraud.
- Secure the credit card for investigation (Use caution so as to not contaminate evidence with fingerprints).
- Interview the customer to determine if there is a plausible explanation for the factual circumstances.
- Compare names and other data.
- If necessary, contact the security office for the credit card company in an effort to obtain additional information about the rightful card owner.

-The security office should be able to provide the cardholder's full name, address, occupation, personal references, place of employment, date and amount of last payment.

CREDIT CARD FRAUD (NOT IN PROGRESS)

- At a minimum, the officer or employee accepting the initial report shall attempt to ascertain the following:

-Name of the store and address

-Name of the owner or manager of the store and a contact telephone number for the store.

-Name of the legitimate cardholder and his address, telephone number, business address, credit card number along with account number, and information relating to how the card was originally lost or stolen.

-Description of the item(s) fraudulently purchased, the amount of the sale, the clerk or cashier's name, especially if the latter witnessed the signing of the invoice.

-Complete identification and address information for all witnesses must be obtained to assist in locating witnesses

-For Internet and catalog orders, obtain the address where the merchandise was shipped, along with the Internet Provider address if available along with the phone number of the suspect order.

- Determine the name and contact telephone number for security personnel from the credit card company that may be involved in the investigation.

CREDIT CARD FRAUD (NOT IN PROGRESS)

-The decision whether or not to prosecute a perpetrator is not left entirely to the credit card company.

1. This is particularly true when the suspect is thought to be associated with other crimes, and it is in the interest of the common good for the State to prosecute the suspect.

-Most large credit card companies assign people to work with the police in cases of credit card fraud. These people are excellent investigative resources that can be contacted for assistance or to obtain technical information on the system used to manufacture and issue the cards.

- When investigating credit card fraud, obtain samples of handwriting from sales slips signed by the suspect.

1. If the card is obtained by false credit application, handwriting is available on the credit application form.

2. In large-scale operations, a warrant maybe be obtained to search the premises and vehicles of known offenders for copies of sales slips that may involve the card involved in the current investigation or other fraudulent cards/transactions

CHECK FRAUD

- Frequently it is not immediately clear whether a bad check case is a civil or criminal matter.
- Intent to defraud- used toseparate a criminal act from a careless oversight or bad bookkeeping.
- Cases involving insufficient or non-sufficient funds (NSF) fall into one of two categories:

1. Accidental – people carelessly overdraw their checking account and are generally not prosecuted unless they do so habitually.

2. Intentional – professionals open a checking account with a small deposit, planning to write checks for amount well in excess of the amount deposited.

- In cases involving closed accounts, the investigating officer should attempt to prove that the issuer received notification from the bank that the account was closed, or that the issuer wrote checks after closing the account himself. Either is usually sufficient to establish intent to defraud.
- In all bad check cases the victim will need to obtain and complete a Bad Check Packet before prosecution can be initiated against the issuer.

FORGERY

- An individual commits forgery by signing someone else's name to a document with the intent to defraud. (includes actually signing the name and using a rubber stamp or a check-writing machine)
- It is also forgery to alter the amount on the check or to change the name of the payee.

Physical description

Circumstances – the manner in which the check was cashed; the story given by the passer; the exact words used; credentials offered; conversation and behavior after the check was passed.

Date and time of occurrence.

Number of persons present – was the store or bank crowded at the time the check was passed.

History – a record of the establishment and/or the cashier in regard to cashing forged checks.

Handwriting – did the check passer sign or write the check in the presence of the person cashing the check?

FORGERY

Authenticity – the subject must either admit or deny that the signature is his.

Check handwriting habits- Handwriting specimens, signatures, and other writings similar to those forged, should be obtained.

Access to check forms. Where kept? Who has access to the area?

Records of employees and associates. Inquiries should be made about acquaintances.

Suspects – the subject should be encouraged to name any persons whom he may suspect and the reasons for his suspicions.

Financial matters – what is the condition of the subject's credit? Has he had any bad checks (NSF)? Has he been connected in any way with a previous forged check case?

The bank on which the check was drawn should be visited to ascertain certain facts.

IDENTITY THEFT

- ANYONE can be a victim of ID Theft at any time
- Younger Americans may be victimized at a higher rate because they are more likely to use the Internet which is the primary tool in many identity theft cases.
- Elderly Americans are highly vulnerable to identity theft schemes, particularly the various telephone scams used by perpetrators to acquire personal information.

METHODS OF ID THEFT

- Stealing wallets and purses containing personal identification, credit cards, and bank cards.
- Stealing mail, including mail containing bank and credit card statements, pre-approved credit offers, telephone calling cards, and tax information.
- Completing a false change-of-address form to divert the victim's mail to another location.
- Searching trash for personal data (a practice known as dumpster diving) found on such discarded documents as so-called pre-approved credit card applications or credit slips discarded by the victim.
- Obtaining credit reports, often by posing as a landlord, employer, or other person or entity that might have a legitimate need for, and right to, another's credit information.
- Obtaining personal information at the workplace or through employers of the victim

METHODS OF ID THEFT

- Discovering personal information during physical entries into the victim's home- lawful or unlawful
- Obtaining personal information from the Internet. This may be information stolen by hackers or freely provided by the victim in the course of making purchases or other contacts. Many victims respond to unsolicited e-mail (spam) that requests personal information.
- Purchasing information from inside sources such as store employees, who may for a price provide identity thieves with information taken from applications for goods, services, or credit.
- Pretexting- thief telephones the victim or contacts the victim via Internet and requests that the victim provide personal information.
- Shoulder Surfing- thief positions him or herself near a victim in order to obtain personal information by overhearing the victim or seeing the victim's actions.
- Skimming- electronic lifting of the data encoded on a valid credit or ATM card and transferring that data to a counterfeit card.

TIPS FOR CIVILIANS

- DO NOT pay any person who is asking for money, gift cards, etc over the phone- it is a scam
- Call police if you are unsure if it is fraud or not
- DO NOT give anyone authorization for your checks, bank information, etc.
- Keep your information private and in a safe place.

QUESTIONS?


IF YOU SEE SOMETHING, SAY SOMETHING.
REPORT SUSPICIOUS ACTIVITY TO THE POLICE - 911


DANGER
GRANDPARENT SCAM


SCAM ALERT