11-9. Non-Cardholder Fraud

a. Non-cardholder fraud involves the use of the card account or CH data by an unauthorized person. Non-cardholder fraud is investigated by special units within the servicing bank. Any information acquired relating to non-cardholder fraud should be reported. The risk of non-cardholder fraud is higher in the following situations:

1) **Account/Card never received**. A new or replacement card has been mailed to the CH but was not received. This may be due to a third-party interception. In this case, the account should be cancelled, and new card issued.

2) **Lost or Stolen Account/Card**. If the CH reports the account as lost or stolen, the account will be cancelled and new one issued. Reporting the account as lost or stolen does not relieve the Federal Government for payment for any transactions that were made by the account holder prior to losing it.

3) **Altered or counterfeit cards**. This occurs when third parties obtain account information and used that information to make purchases with an altered or counterfeit card. If the bank recognizes a fraudulent pattern of use at the time of authorization, the bank will validate the use of the account with the CH and/or suspend the account.

4) **Account takeover/ Identity theft**. In this case, the account holder's identity has been compromised and a third party has requested a new account by providing confidential information about the account holder. Any CH who believes that he or she may have been subject to identity theft should contact the bank's customer-service department. Once a determination is made that an account has been compromised, investigation is the responsibility of the bank. Unless a government employee is determined to be involved in the fraud, the agency generally does not participate in the investigation. The account will be closed, and a replacement account opened.

b. **If Non-Cardholder Fraud Occurs**. If fraud is detected on the account, the CH must immediately report the incident to the following: BO, A/OPC and servicing bank. The servicing bank will block and/or terminate the account. If necessary, the bank will then issue a new card with a new account number. Also, the bank will mail a "Statement of Fraud" letter to the cardholder, which must be completed and returned promptly. Sometimes, unauthorized transactions will appear on the billing statement, even though the account was reported lost or stolen. Cardholders should report all unauthorized transactions by calling the bank's customer service telephone number.

c. **Non-Cardholder Fraud Methods**. Some of the different methods of fraud include the following:

1) **Counterfeit Accounts**. To make fake cards, criminals use the newest technology to "skim" information contained on magnetic stripes of cards and also to pass security features (such as holograms).

2) **Lost or Stolen Accounts**. Physical cards are stolen from a workplace, gym or unattended vehicle.

3) **Card Not Present.** Internet fraud occurs whenever account information is stolen and used to make online purchases. Merchant asks for the CVC code (located on the back of the card) to help prevent this type of fraud.

4) **Phishing**. Phishing occurs whenever a CH receives a fake email directing him or her to enter

sensitive personal information on a phony website. The false website enables the criminal to steal information from the account holder.

5) **Non-Receipt**. This type of fraud occurs whenever new or replacement cards are mailed and then stolen while in transit.

6) **Identity Theft**. A criminal applies for an account using another person's identity and information.

d. **Detecting Non-Cardholder Fraud**. One of the first signs that an individual is a victim of fraud is at least one "mystery expense" showing up in the monthly statement. To help detect fraud, cardholders should review their statement by performing the following actions:

1) Look for transactions you do not recall making.

2) Check for unknown vendors.

3) Search for account withdrawals you do not remember making.

e. **Avoiding Non-Cardholder Fraud**. Cardholders should use the following practices to avoid fraud:

1) Secure account number and information.

2) Safeguard your personal identification number (PIN). Do not write it down; memorize it. Do not share your PIN.

3) Monitor your card during transactions. When the card is returned, check to make sure it is yours.

4) Immediately report lost or stolen accounts and/or any questionable charges.

5) Sign the back of a new card as soon as you receive it. If you do not receive a replacement card before the expiration date of the older card, contact the bank.

6) Destroy unwanted or expired cards. Shred or secure monthly statements and receipts.

7) Electronically verify charges appearing on your monthly statement.

8) Unless you initiated the purchase, never give your account information over the telephone, through the mail, or on the internet.

9) Consistently check your account for accuracy of personal and billing information. Notify the bank if your personal information and/or address needs updating.

10) Never let a telemarketer or salesperson pressure you into agreeing to a deal.

11) Be aware of common scams and contact your A/OPC and the bank for unusual situations.

12) Inform your A/OPC if you won't be using your card for an extended time. The A/OPC will temporarily suspend the card or reduce the single purchase limit to $1.

Parent topic: CHAPTER 11 - MANAGEMENT CONTROLS AND PROGRAM OVERSIGHT