11-10. Cardholder Fraud and Merchant Fraud

a. **Cardholder Fraud, Misuse and Abuse**. This type of fraud occurs when a cardholder uses their account to transact business that is not sanctioned, not authorized, not in one's official Government capacity, not for the purpose for which the card was issued, and/or not as part of official Government business. Intentional use of a GPC account for other than official Government business constitutes abuse, and depending on the situation, may constitute fraud.

b. **Consequences of Cardholder Fraud**. Cardholders have a responsibility to use the account to procure supplies and services at the direction of the Army under official purchase authorization. If a CH abuses the GPC or participates in fraud, the Army may cancel the purchase account and take appropriate disciplinary action against the CH. In the case of account abuse, any participating employee may be held personally liable to the Federal Government for the amount of any unauthorized transaction. Depending on the facts involved, an employee may be subject to fine or imprisonment for action relating to purchase account abuse and fraud. There are guidelines and procedures for disciplinary action to be taken against individuals for the improper, fraudulent, or abusive use of the purchase account. Purchase account abuse/fraud may have the following potential consequences:

1) Counseling

2) Cancellation of card account

3) Notation in employee performance evaluation

4) Reprimand

5) Suspension of employment

6) Termination of employment

7) Criminal prosecution

c. **If Cardholder Fraud Occurs**. If an A/OPC suspects that a BO or CH has committed fraud, the A/OPC should first contact the individual's command. The A/OPC may file a complaint with the Army Inspector General. Investigations are initiated upon receipt of a complaint or other information that gives a reasonable account of the wrongful or fraudulent act. The DoD hotline phone number is 800-424-9098 to report fraud. A/OPCs should be as specific as possible when reporting fraud. The following information should be provided:

1) Employee's full name

2) Rank or pay grade

3) Duty station

4) Specific suspected fraudulent act or wrongdoing

5) Specific dates and times

6) Specific location of where the suspected fraudulent act occurred

7) How the individual completed the alleged fraudulent act

d. **Merchant Fraud**. This type of fraud is committed by the merchant. Merchant fraud can occur either with or without the CH's knowledge or consent. Rotating sources may help prevent this type of fraud. Billing errors, such as duplicate charges, are not considered merchant fraud. Examples include:

1) A vendor intentionally charges for items not delivered/services not performed.

2) A vendor offers bribes and gratuities to a government employee in exchange for gaining purchasing activity.

Parent topic: CHAPTER 11 - MANAGEMENT CONTROLS AND PROGRAM OVERSIGHT