11-10. Reporting and Monitoring for Fraud

a. **Reports for Identifying and Preventing Fraud**. A/OPCs should use the following reports to identify potential card misuse and fraud and to prevent fraud from occurring:

1) **Declined Transaction Authorizations Report**. This report identifies cardholders who have attempted to use an account to buy an item for which they are not authorized, that exceeds their single purchase limit, that exceeds their monthly purchase limit, or from a merchant that falls under a blocked MCC.

2) **Transaction Detail Report**. This report identifies the date, merchant, reason code, dollar amount, and status of each dispute filed by CH. BOs and A/OPCs should track and follow up on disputes to determine their outcomes. Cardholders should attempt to resolve disputes directly with merchants prior to filing a disputes report. If a merchant is consistently appearing on the disputes report, the A/OPC should determine whether the merchant may have billing issues, quality issues, or is attempting to commit fraud by submitting false transactions.

3) **Unusual Spending Activity Report**. This report identifies transactions that may warrant further review.

4) **Account Status Change Report.** This report lists accounts with a change status of lost/stolen, closed, or reopened accounts. This status may either be an indicator that the CH needs to secure the account or that the CH is attempting to disguise misuse or fraudulent activity by denying the charges.

b. **Reporting Fraud**. All identified instances of suspected fraud or abuse must be reported. Various channels of reporting include the Chain of Command, the A/OPC, the command's procurement fraud advisor (Staff/Command Judge Advocate), the servicing Criminal Investigation Division office, internal review organizations, and Inspector Generals at all levels. When a Defense criminal investigative organization or Defense organizational element responsible for investigating potential misconduct involving the GPC initiates an investigation into allegations of charge card violations regarding a GPC, the CH's commander or second-line supervisor, as appropriate, and security manager must be notified. Whenever possible, this notification should take place within 72 hours of the initiation. See DoD Charge Card Guidebook A.1.11.

Parent topic: Chapter 11 - Management Controls and Program Oversight