<?xml encoding="UTF-8">

11-11. 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. Notify the CH's commander or second-line supervisor, as appropriate, and security manager 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. Whenever possible, this notification should take place within 72 hours of the initiation. See DoD Charge Card Guidebook A.1.11.

11-12. Violation and Disciplinary Categories

a. **Identifying the Violation**. DoD's GPC Disciplinary Category Definitions Guidance is a helpful resource when identifying the type of violation.

b. A/OPCs should be alert to the following indicators of possible fraud, waste, or abuse:

1) Repetitive buys from the same merchant

2) Lack of documentation for a purchase

3) Failure to safeguard cards and account numbers

4) CH or BO authorizing the use of their cards by others

5) Inadequate oversight by BOs and agencies

6) Payments made for items not received

7) Split purchases to avoid spending limitations

8) Lack of accounting for items requiring accountability

9) Payment delinquencies incurring interest penalties

10) Approval of a CH's statement of account by someone other than the CH or BO

11) Unauthorized purchases

12) CHs returning merchandise for cash or store credit vs. having credits issued back to the GPC

c. **Taking Corrective Action**. When an A/OPC discovers a violation of GPC policies, the A/OPC must take corrective action. The course of action will vary depending on the intentionality and severity of the infraction. A/OPCs should take one or more of the following corrective actions:

1) Document the purchase violation in IOD and the purchase file.

2) Require involved parties to attend training.

3) Inform the involved parties' supervisor or commander.

4) Suspend CH or BO account.

5) Terminate CH or BO appointment and account.

d. **Continual or Severe Violations**. Continual violation of GPC procedures by a CH or BO will result in termination of GPC privileges. A/OPCs will document the violation and action taken in their files for that particular CH/BO. A/OPCs will refer evidence of deliberate abuse to the CH and/or BO's supervisor, Commander, or SCO for appropriate action in accordance with the Uniform Code of Military Justice or civilian disciplinary rules. A/OPCs will refer evidence of internal fraud or other criminal activity to the Commander or SCO.

e. Any misuse of the GPC is subject to criminal, civil, Uniform Code of Military Justice, administrative, and disciplinary actions as appropriate. See below Table 11-6 for details. The Offenses and Penalties table in AR 690-752 is intended for use as a guide for selecting an appropriate penalty for infractions committed by civilian employees as it may not effectively address all situations. This table does not substitute for independent supervisory judgment and does not dictate penalties. A supervisor may choose the severity of action ranging from no penalty, informal disciplinary actions, to the maximum penalty of removal.

Table 11-6: Offenses and Penalties Guidance

Offense for Misuse of Government Charge Card	First Offense	Second Offense	Third Offense

Misuse of Government Travel Charge Card or Purchase Charge Card (for example, use for unauthorized personal expenses, failure to pay charge card bill in a timely manner, failure to properly safeguard the card or failure to use card for required expenses arising from official travel. Use of the Travel Charge Card at establishments or for purposes that are inconsistent with the official business of DoD, the Army, or applicable regulations).	Written reprimand to removal	5-day suspension to removal	10-day suspension to removal
Unauthorized use, failure to appropriately control or safeguard the use of a Government Purchase Card as a card holder or approving official responsible for use or oversight of the purchase card.	Written reprimand to removal	14-day suspension to removal	Removal

Parent topic: CHAPTER 11 - MANAGEMENT CONTROLS AND PROGRAM OVERSIGHT