

## Welcome to Unauthorized Use of the GPC

In this topic you will be introduced to the many possible misuses of the Government Purchase Card (GPC), including the definition of fraud and examples of fraudulent transactions. Your instruction will also include how to identify types of noncardholder-related fraud and how to handle the situation if it were to occur. As a follow up to our discussion of fraud you will also be provided an outline of the penalties and consequences of misuse.



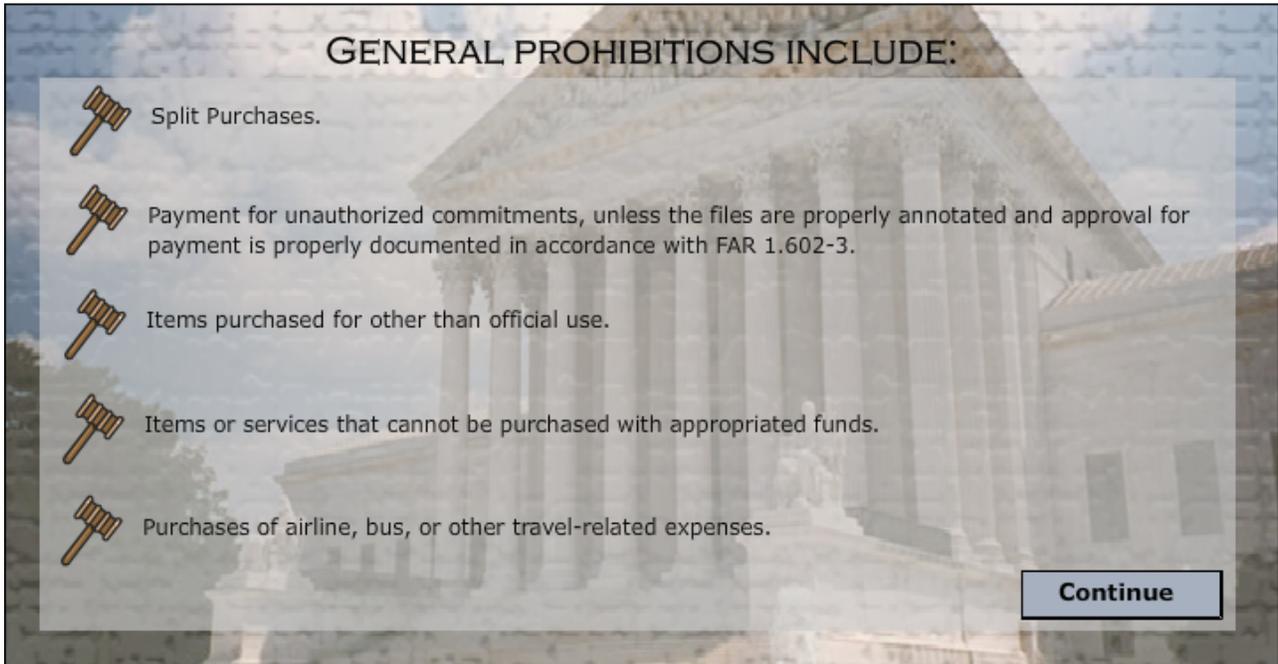
## Learning Objectives

Upon completion of this topic, you will be able to:

- Recognize restrictions on GPC use.
- Identify types of cardholder and noncardholder fraud.
- Recognize how to report GPC fraud.
- Define steps to follow if a GPC is lost or stolen.
- Recognize reissuing procedures for new cards and card records.
- Define penalties involved with fraudulent, improper, and abusive transactions.
- Recognize DoD's policy on misuse of the purchase card and personal accountability for government charge card abuse.

**GPC Prohibitions**

Before approaching the subject of fraud and the actions taken let's first identify some cases in which the use of the Government Purchase Card is prohibited.



D-Link Text:

This is an interactive flash module that addresses the prohibitions of the Government Purchase Card.

General prohibitions include:

- Split Purchases.
- Payment for unauthorized commitments, unless the files are properly annotated and approval for payment is properly documented in accordance with FAR 1.602-3.
- Items purchased for other than official use.
- Items or services that cannot be purchased with appropriated funds.
- Purchases of airline, bus, or other travel-related expenses.

Other GPC prohibitions include:

- Purchases made by individuals other than the authorized cardholder.
- Purchases by individuals not trained.
- Making purchases and returning them to the merchant for cash or merchant credit slips (credit must be issued against same card on which purchase was made).
- Purchases by contractors (according to agency procedures contractors must obtain credit cards directly from the bank).
- Rental or lease of land or building on a long-term basis.
- Cash advances.

Close window to continue

---

## Exceptions to GPC Prohibitions

There are special circumstances when there are exceptions to the GPC prohibitions in the instances of:

- Purchases of gifts or mementos.
- Purchases of food, drinks, lodging, and travel costs.

Generally, agencies may not purchase gifts or mementos. The cardholder must seek advice from the activity fiscal attorney when questioning purchases of gifts or mementos.



## Government Travel Card



If food is purchased when an employee is on official travel, it should be paid for with a Government travel card, not the Government Purchase Card. Other travel-related expenses, such as lodging and rental cars, should also be paid with the Government travel card. Cash advances for official travel should also be obtained with a Government Travel Card.

There are, however, certain circumstances that do permit the use of the Government Purchase Card towards travel-related expenses. One example, when using the Government Purchase Card can be directed toward travel related expenses is when you are renting a hotel conference facility for official purposes. Consult the Financial Manager and activity fiscal attorney before using the Government Purchase Card to purchase food, hotel facilities, and other travel related expenses.

## Knowledge Review

True or False.

Contractors may use a Government employee's Government Purchase Card as long as the Contracting Office authorizes its use and the contractor notifies the Contracting Officer of all purchases made by the contractor during the billing period.

- True
- False

Submit



---

## Knowledge Review

Please select a correct answer.

Normally, which of the following may NOT be purchased with the Government Purchase Card:

- Computer supplies from a GSA schedule.
- Food, drinks, clothing, lodging or travel related expenses.
- Furniture from Federal Prison Industries.
- Plumbing services from a commercial merchant.

Submit



---

## What Is Fraud?

Fraud is any felonious act of corruption or attempt to deliberately cheat the Government or corrupt the Government's agents. See [10 U.S.C. 932](#) for further definitions of fraud against the United States.

Cardholders have a responsibility to use the Government Purchase Card to procure supplies and services at the direction of the agency under official purchase authorization.



---

### Cardholder Fraud

Now that we have briefly outlined the definition of fraud, and you have taken a look at 10 U.S.C. 932, select each of the examples below to read more on situations that can constitute cardholder fraud.



D-Link Text:

This is an interactive flash module that includes the following examples of cardholder fraud.

#### **Cardholder Fraud: Example 1**

Example 1 is a cardholder who conspires with a business owner to make purchases not authorized by the cardholder's agency. The merchant circumvents the authorization process to allow the cardholder to make purchases for personal consumption. The cardholder approves the transactions.

#### **Cardholder Fraud: Example 2**

Example 2 is the cardholder who conspires with a local company to make fraudulent purchases. No receipts were found to support the purchase, and the amount of purchases from this company exceeds the normal expenditures of other cardholders. The fraudulent purchases are never delivered to the Government.

#### **Cardholder Fraud: Example 3**

Example 3 is the business owner who approaches cardholder and offers to provide kickbacks to the cardholder if the cardholder will make supply purchases from his business. The cardholder is authorized to make purchases of these supplies and the supplies are delivered. In return, the company provided false receipts for supplies. The cardholder continues to repeatedly make transactions with this company, and the company pays the cardholder a percentage of the sales price.

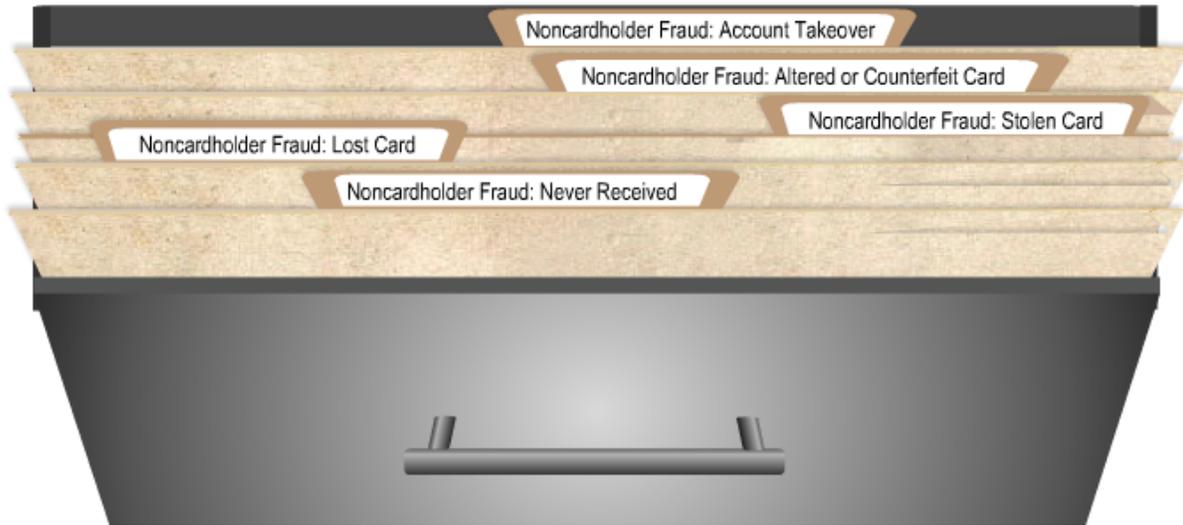
#### **Cardholder Fraud: Example 4**

Example 4 is the cardholder who obtains goods and services for personal use. In this case, the delivery address is the employee's home, and a third party cannot confirm receipt of materials. The cardholder also advises merchant to split transactions to ensure they do not exceed the cardholder's single purchase limit.

Close window to continue

**What Is Noncardholder Fraud?**

Noncardholder fraud is also possible and involves use of the card or cardholder data by an unauthorized person. The risk of noncardholder fraud is higher in certain situations, particularly in the cases listed below. Select from the list below to read about examples of noncardholder fraud.



[D](#)

The cardholder and Approving Official need to be vigilant in their statement reviews to identify purchases that may have been made by an unauthorized cardholder.

D-Link Text:

This is an interactive flash module that addresses the following cases of noncardholder fraud.

**Noncardholder Fraud: Never Received**

In this case, the new card or a replacement card is mailed to the cardholder but never received. Due to the possibility that the card could have been intercepted by a third party, the account must be cancelled by the bank upon notification from the cardholder that the card was not received. When a new card with a new account number is issued, cardholders are required to activate their cards by phone to ensure the cards have been properly received.

**Noncardholder Fraud: Lost Card**

If a card is lost, contact the bank immediately. Due to the possibility that the card could have been intercepted by a third party, the account must be cancelled by the bank upon notification from the cardholder that the card is lost.

**Noncardholder Fraud: Stolen Card**

In the event that a cardholder reports a card has been stolen, the account will be closed and a new card issued. Reporting the card as stolen does not relieve the Government of payment of any transactions that were made by the cardholder prior to reporting it stolen. Cardholders may be required to sign an affidavit confirming their cards were stolen.

If the cardholder did not make the transactions appearing on the cardholder statement, the cardholder should

submit a dispute form to the bank. Failure to submit the dispute form and/or affidavit could result in liability to the Government.

**Noncardholder Fraud: Altered or Counterfeit Card**

Altered or counterfeit cards are normally identified by the card-issuing bank's authorization process or by the cardholder when the cardholder statement of account is received. If the card-issuing bank recognizes a fraudulent pattern of use at the time of authorization, the bank will validate the use of the card with the cardholder and/or suspend the card. The cardholder may be asked to sign an affidavit verifying that the transactions were fraudulent. If the cardholder did not make transactions appearing on the cardholder statement of account, the cardholder should submit a dispute form to the card-issuing bank. Failure to submit the dispute form and/or affidavit could result in liability to the Government.

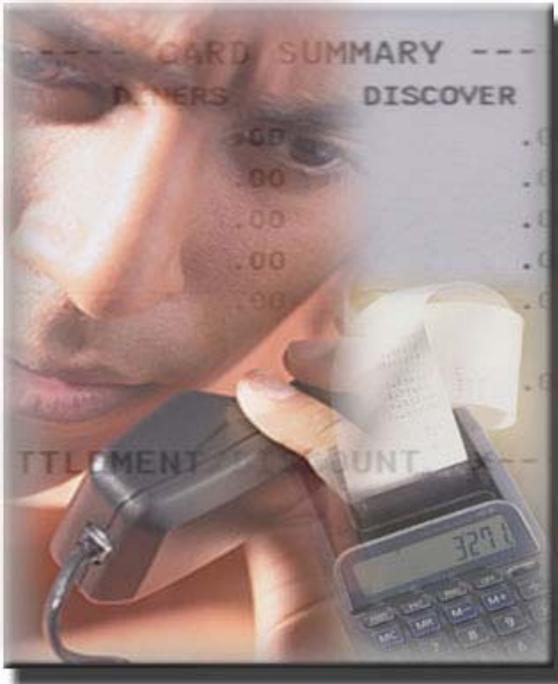
**Noncardholder Fraud: Account Takeover**

Account takeover is a situation that may be better known as identity theft, which means the cardholder's identity has been compromised by a third party. The third party may request a new card by providing confidential information about the card that was obtained illegally. Cardholders who may have been subject to identity theft should contact the card-issuing bank's customer service to prevent the thief from obtaining a card in the cardholder's name.

Close window to continue

---

### Reporting GPC Fraud: Who Is Responsible for Reporting

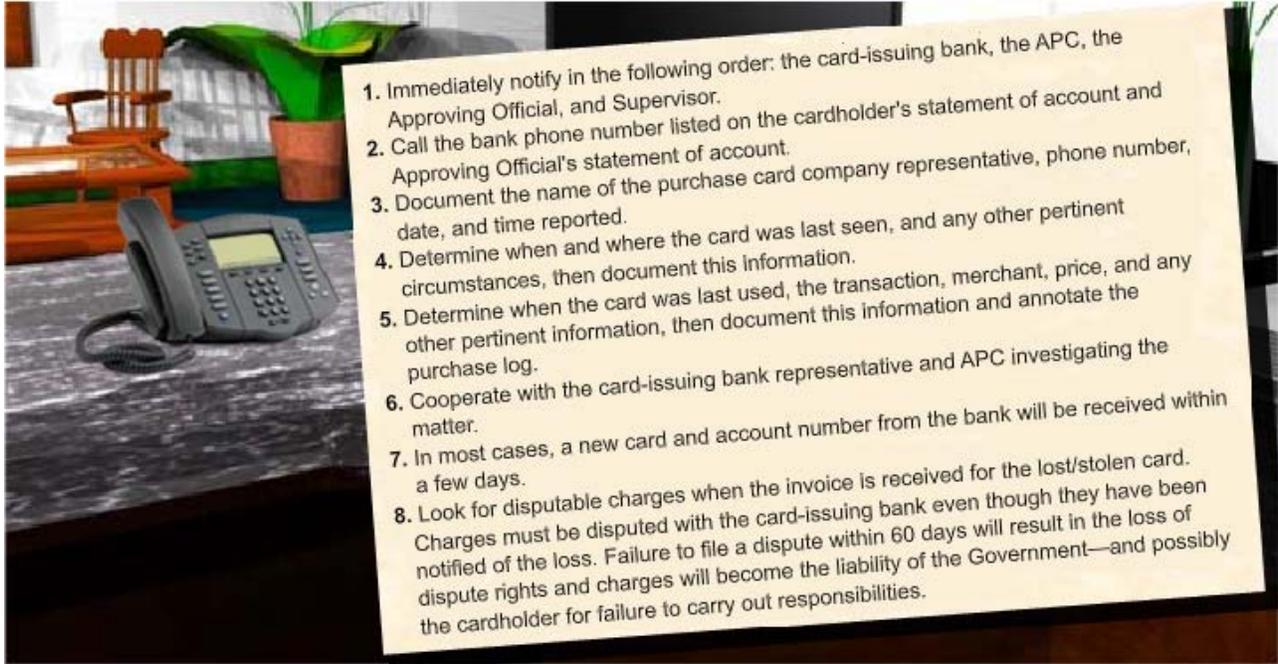


All Government employees have a duty to report all suspected instances of fraud to the appropriate authorities. This includes disputing any purchases believed to be fraudulent during monthly statement reconciliation.

The cardholder must also report cases of fraud to the card-issuing bank, their Agency/Organization Program Coordinator (APC), and their local procurement fraud advisor.

**Steps to Follow If the GPC Is Lost or Stolen**

If your card is lost or stolen there are an number of steps you may need to take in order to prevent noncardholder fraud. Below you will find a list of actions you can take to protect your account in case such a situation should arise.



D-Link Text:

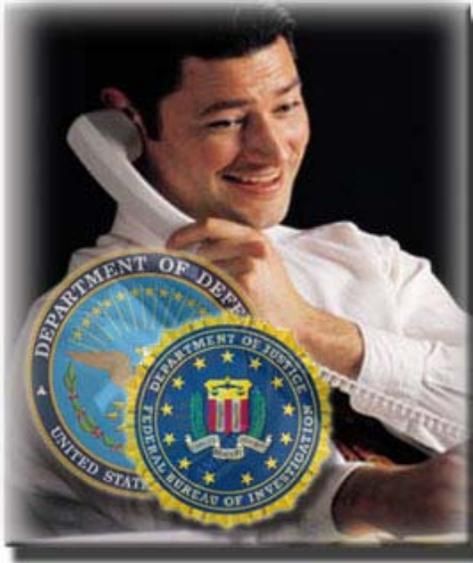
1. Immediately notify in the following order: the card-issuing bank, the APC, the Approving Official, and Supervisor.
2. Call the bank phone number listed on the cardholder's statement of account and Approving Official's statement of account.
3. Document the name of the purchase card company representative, phone number, date, and time reported.
4. Determine when and where the card was last seen, and any other pertinent circumstances, then document this information.
5. Determine when the card was last used, the transaction, merchant, price, and any other pertinent information, then document this information and annotate the purchase log.
6. Cooperate with the card-issuing bank representative and APC investigating the matter.
7. In most cases, a new card and account number from the bank will be received within a few days.
8. Look for disputable charges when the invoice is received for the lost/stolen card. Charges must be disputed with the card-issuing bank even though they have been notified of the loss. Failure to file a dispute within 60 days will result in the loss of dispute rights and charges will become the liability of the Government—and possibly the cardholder for failure to carry out responsibilities.

Close window to continue

---

## Reporting GPC Fraud

GPC cardholders should be on the lookout for merchants or contractors committing fraud. Examples of fraud could include billing for items not ordered or delivered, or delivering nonconforming items. Approving Officials should examine purchase documentation for unauthorized purchases by cardholders as well as for possible contractor fraud while reconciling monthly statements.



If fraud is suspected of a Government Purchase Card account, immediately contact the card-issuing bank first. As of January 2009, the relevant numbers are:

- U.S. Bank - 1-888-994-6722
- Citibank - 1-888-786-0818

Then call the APC, the DoD Fraud Hotline (1-800-424-9098), and the local procurement fraud advisor. In addition contact the organization's Criminal Investigation Command. The DoD Purchase Card Program Management Office has partnered with Operation Mongoose to provide oversight and fraud detection for the Government Purchase Card Program.

[Read about Operation Mongoose.](#)

Popup Text:

### Read about Operation Mongoose

The purpose of Operation Mongoose is to develop and operate an active Fraud Detection and Prevention Unit to minimize fraudulent attacks against Department of Defense assets. It comprises representatives from three DoD organizations:

1. Defense Finance and Accounting Service.
2. Defense Manpower Data Center.
3. Department of Defense Inspector General.

These organizations collaborate to identify fraud indicators and to screen questionable purchase transactions for referral to the appropriate criminal investigative agencies.

---

### New Cards and Old Records

Cards are normally reissued every 36 months to each cardholder. This is automatic unless the APC halts the reissue.

The bank will maintain the records of all transactions for six years and three months from the date of the transaction. The bank will provide the requested information concerning individual transactions within 45 business days of a request.

The Certifying Official must maintain certified billing statements for six years three months from the date of the purchase transaction. All other purchase card records for purchases \$3,000 and less must be maintained for three years, including:

- cardholder statements,
- merchant receipts, and
- packaging slips.

Note: Documentation supporting purchase card purchases greater than \$3,000 must be maintained for six years and three months.



---

### Fraudulent E-mails

U.S. Bank will not contact cardholders directly under any circumstances to verify account numbers or personal information. Cardholders will never receive a request via e-mail or telephone, and should not respond to either.

Cardholders have reported receiving requests via email that appear to come from U.S. Bank. The email claims that the recipient's accounts have been blocked and asks the recipient to enter his or her account number and other personal information.

In reality, no fraudulent activity has been reported and no cards have been suspended as this e-mail suggests. There was no breach of any secure account information. These e-mail messages are random and are being sent using a spam list that includes individuals who, in many cases, do not even have U.S. Bank accounts. Similar e-mail fraud campaigns have been reported using names of other banks.



---

### Reporting Fraudulent E-mail



U.S. Bank and the Federal Bureau of Investigation (FBI) are working diligently to stop illegal GPC e-mail activities. To help track these cyber-criminals, the U.S. Bank Fraud Department is requesting that anyone who has received a suspicious e-mail send a copy of it to the help desk at U.S. Bank, along with responses to the questions below.

- Do you have an account relationship with U.S. Bank?
- What Internet Service Provider (ISP) do you use?
- What type of connection do you use to access the Internet? Cable, dialup, DSL or other?
- Do you have a firewall installed on your computer?

---

## Knowledge Review

Please select a correct answer.

If you suspect fraud on your Government Purchase Card account, you should immediately:

- Notify your Agency Personnel office.
- Contact the merchant for verification of the transaction.
- Contact the card-issuing bank, APC, and local Procurement Fraud Advisor.
- Refer the matter to your organization's Criminal Investigation Command.

Submit



**Knowledge Review**

True or False.

The bank maintains the records of all transactions for six years and three months from the date of the transaction.

- True
- False

Submit



---

## Knowledge Review

Please select a correct answer.

Which of the following steps should you take first when a GPC is lost or stolen?

- Document the name of the purchase card company.
- Determine when and where the card was last seen.
- Cooperate with the card-issuing bank representative and APC investigating the matter.
- Call the card-issuing bank.
- Look for disputable charges when the invoice is received for the lost/stolen card.
- Immediately notify in the card-issuing bank, the APC, the Approving Official, and Supervisor.
- Determine when the card was last used, the transaction, merchant, price, and any other pertinent information, then document this information and annotate the purchase log.



Submit

---

## Knowledge Review

True or False.

The GPC is normally reissued every 12 months to each cardholder.

- True
- False

Submit



---

### What Are Fraudulent, Improper, and Abusive Transactions?

We have to this point outlined the many examples of both cardholder and noncardholder fraud. However, in the case of the cardholder there is a difference between what constitutes fraudulent transactions and what constitute improper and abusive transactions. Let's take a closer look at these differences by selecting the items below.



D-Link Text:

This is an interactive flash module that includes the following content identifying the difference between the Fraudulent, Improper and Abusive transactions.

**Fraudulent Transactions are those made by an unauthorized or authorized individual** that were intended for personal use (i.e. items that are personal in nature and not likely to be a government requirement - jewelry, furs, adult entertainment).

**Improper Transactions are those intended for government use** but were not, or did not appear to be, for a purpose permitted by law. Examples include purchases that, by law, cannot be made with funds available to the DoD. For example, using research and development funds or construction only funds for operation and maintenance purposes.

**Abusive Transactions are those that were authorized** but in which the items were purchased at an excessive cost, and/or for a questionable government need, i.e. items or services that are centrally managed for which approval for local purchase has not been obtained, items or services purchased for a legitimate government requirement but which exceed those requirements (i.e. brand name briefcase rather than generic), and items or services that the cardholder was not authorized to purchase but which could have been purchased by an authorized contracting officer.

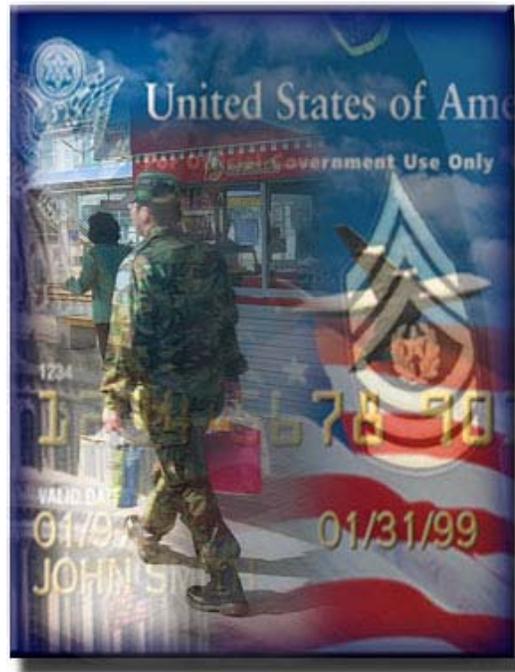
Close window to continue

---

### DoD Policy for GPC Misuse

Following reports of purchase card misuse within the Department, the DoD Charge Card Task Force identified personal accountability as essential to DoD's efforts to strengthen the Department's purchase and travel charge card programs. Personal accountability for government charge card misuse is also a focus of Congress.

It is DoD policy that for each case of improper, fraudulent, abusive, or negligent use of a government purchase or travel charge card by military personnel, the commander or supervisor of the responsible individual or parties be informed in a timely manner. This includes notification of any case of misuse at establishments for purposes that are inconsistent with the official business of DoD, or with applicable standards of conduct. The early notification of such activity to the Commander or Supervisor will allow for appropriate corrective or disciplinary action to be taken.



## Curtailling GPC Misuse

The best way to curtail GPC misuse is to prevent it through proper selection of cardholders, training, and leadership by example.



Actions available when military personnel misuse a purchase or travel charge card include:

- counseling,
- admonishment,
- reprimand,
- non-judicial punishment,
- court-martial, and
- administrative separation.

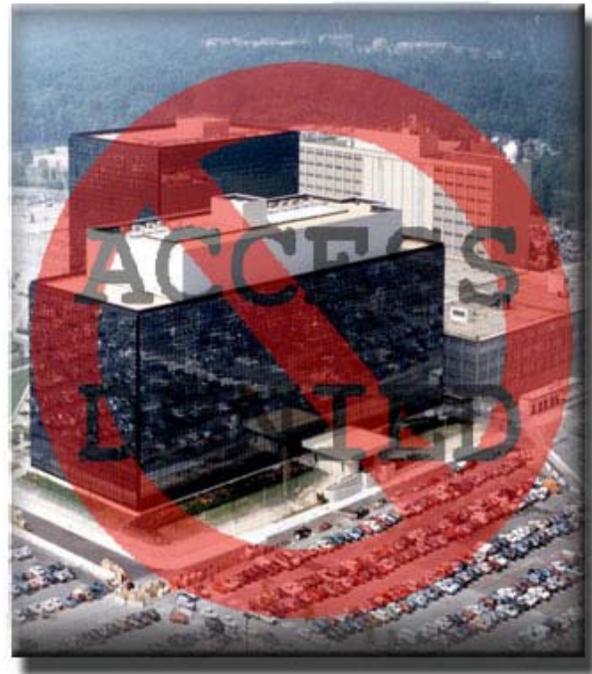
There is no single response appropriate for all cases. Commanders or supervisors shall use the procedures established for each action by the appropriate Military Department and consult with their legal advisors as necessary.

---

## Revoking Access to Classified Information

In addition to corrective or disciplinary action, military personnel who misuse their government charge cards may have their access to classified information modified or revoked if warranted in the interests of national security. Commanders or Supervisors shall ensure that security clearance reviews are conducted when the holder of a GPC comes under investigation for misuse.

DoD Components shall incorporate these guidelines into their own policies. Additionally, each Military Department shall have a regulation providing that a violation of any of the rules governing the use of the GPC.



---

**Relationship to Security Clearances**



The review of the security clearance of the individual involved (or the modification or revocation of such security clearances in light of this review) in credit card misuse or abuse cases is not a disciplinary action and should not be treated as such. However, this does not preclude a separate and independent review of such misuse or abuse by the appropriate security managers in accordance with DoD Policy.

The modification or revocation of a security clearance will result in appropriate action, which could include reassignment or removal for failure to meet or maintain a condition of employment.

**Defense Civilian Personnel Data System**

The Defense Civilian Personnel Data System (DCPDS) documents formal disciplinary and/or adverse actions taken for misconduct related to the GPC.

Disciplinary Actions/Penalties:



D-Link Text:

This is an interactive flash module that includes the following information concerning Civilian and Military disciplinary actions and penalties.

**Civilian**

The chart below is one example of potential charge card offenses and remedies or penalties for such offenses. Components must otherwise comply with all applicable law and regulatory guidance in determining whether to impose disciplinary or adverse action in any specific case:

Offenses	First Offense	Second Offense	Third Offense
Misuse of GPC	Letter of Counseling to Removal	5-day suspension to removal	10-day suspension to removal
Unauthorized use of, or failure to control the use of, the GPC	Letter of Counseling to Removal	14-day suspension to removal	30-day suspension to removal

**Military**

Military members are subject to penalties in the Uniform Code of Military Justice. Actions available when military personnel misuse a purchase or travel charge card include:

- Counseling,
- Admonishment,
- Reprimand,
- Non-judicial punishment, and
- Administrative separation.

Close window to continue

---

## Knowledge Review

Please select a correct answer.

Which of the following choices are examples of penalties or disciplinary actions involved when charged with illegal use of the GPC?

- Revoked security clearance.
- Jail sentence.
- Revoked GPC account.
- All of the Above

Submit



---

## Knowledge Review

Please select a correct answer.

What is DoD's policy regarding purchase card misuse and personal accountability for GPC abuse?

- DoD accepts all liability for purchase card misuse.
- DoD expects full accountability from the card-issuing bank.
- Improper, fraudulent, abusive, or negligent use of a government purchase is prohibited and appropriate corrective or disciplinary action will be taken.
- DoD defers to the individual policies of each activity.



Submit

### Summary

Now that you have completed this topic, you should be able to:

- Recognize restrictions on GPC use.
- Identify types of cardholder and noncardholder fraud.
- Recognize how to report GPC fraud.
- Define steps to follow if a GPC is lost or stolen.
- Recognize reissuing procedures for new cards and card records.
- Define penalties involved with fraudulent, improper, and abusive transactions.
- Recognize DoD's policy on misuse of the purchase card and personal accountability for government charge card abuse.