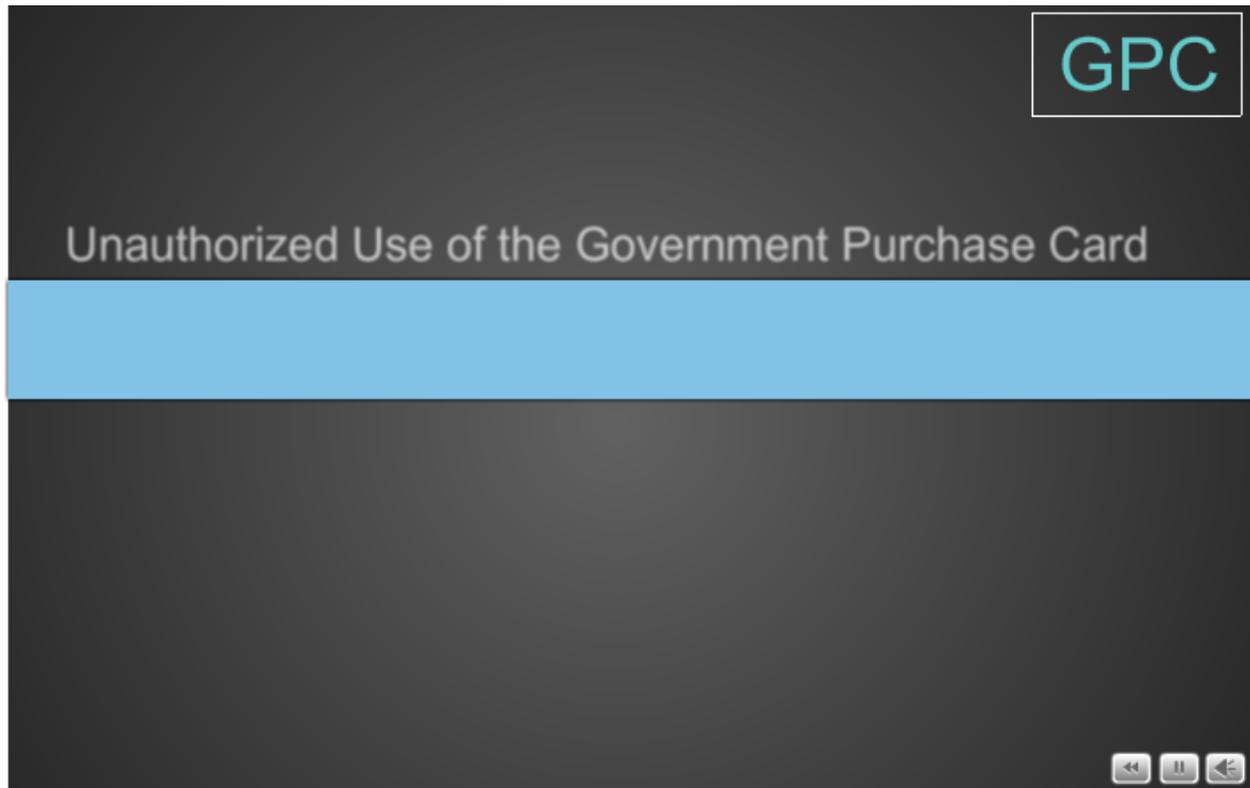


## Welcome to Government Purchase Card Program: Overview



### D-Link Text:

This is an animated splash page introduction. The initial animation includes the title of the topic "Unauthorized use of the Government Purchase Card" followed by drop text that appears below it. The text reads as follows:

"Restrictions on the use of the Government Purchase Card"

"Fraud and fraudulent use of the purchase card"

"Ethical standards of conduct in the use of the purchase card"

This text fades away and is followed up with a presentation of the topic's objectives. The text for the objectives reads as follows:

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

- Recognize restrictions on Government Purchase Card (GPC) use.
- Identify types of fraud.
- Recognize reporting procedures for fraudulent use of lost/stolen Government Purchase Cards.
- Identify ethical standards of conduct and their regulatory/legal foundations.

Close window to continue

## The Government Purchase Card (GPC)

The [Government Purchase Card \(GPC\)](#) is generally used to purchase the same types of things that were previously purchased with a purchase order or other contracting vehicle. Generally, goods and services that cost \$2,500 or less and that may be purchased through the local procurement office may be purchased with the GPC.

Purchases made using the GPC, however, are subject to the restrictions and limitations cited in governing law or DoD policy. Let's look at some of these restrictions and limitations.



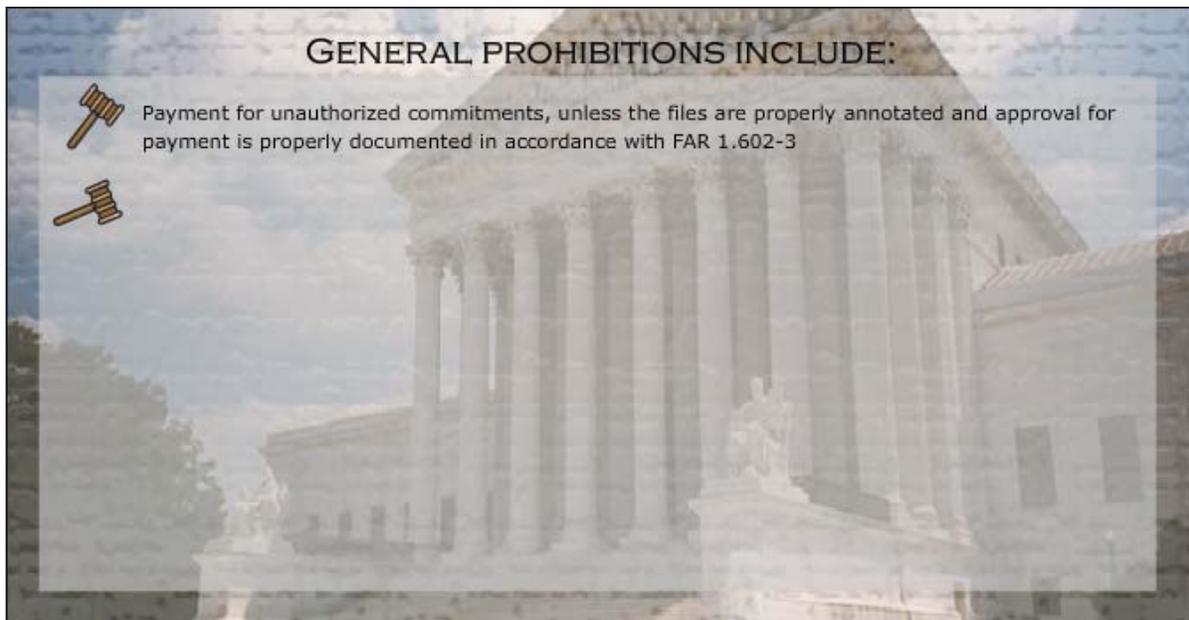
Popup Text:

### **Government Purchase Card (GPC)**

The Government Purchase Card is the name for the credit card used by designated DoD personnel to purchase goods and services for official Government purposes.

## 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 a flash animation that includes the following content concerning Government Purchase Card prohibitions.

### **GENERAL PROHIBITIONS INCLUDE:**

1. Payment for unauthorized commitments, unless the files are properly annotated and approval for payment is properly documented in accordance with FAR 1.602-3
2. Items purchased for other than official use
3. Items or services that cannot be purchased with appropriated funds
4. Purchases of airline, bus, or other travel-related purchases
5. Purchases made by individuals other than the authorized cardholder

### **POP-UP FOR: Travel-Related Purchases**

Expenses incurred for travel while an employee is on official business should be paid for with a Government travel card, rather than a Government Purchase Card. A Government travel card is a charge card issued to Federal employees and is used solely for payment of official travel-related expenses, such as food, lodging and car rental. Cash advances for official travel should also be obtained with a Government travel card. Certain circumstances permit the use of the Government Purchase Card for travel-related expenses. For example, you can use the Government Purchase Card to rent a hotel conference facility for official purposes. You should consult the Financial Manager and activity fiscal attorney before using the GPC to purchase food, hotel facilities, and other travel-related expenses.

### **OTHER GPC PROHIBITIONS INCLUDE:**

1. Purchases by untrained individuals
2. Making purchases and returning them to the merchant for cash or merchant credit slips. (Instead, credit must be issued against the card on which the purchase was made.)
3. Purchases by contractors. (Contractors must obtain credit cards directly from the Bank, according to Agency procedures.)
4. Payments for rental or lease of land or buildings on a long-term basis
5. Cash advances
6. Purchases of gifts or mementos

**POP-UP FOR: Purchases of Gifts or Mementos**

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

Close window to continue

---

## Split Purchases

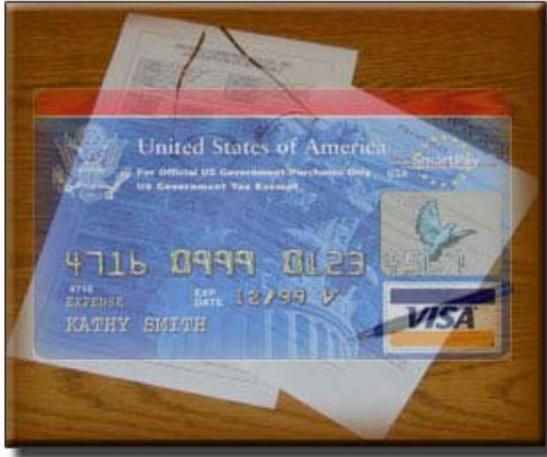
Another major prohibition is the split purchase. A split purchase means to break down a purchase that exceeds the micro-purchase threshold into several purchases. In this way, they are under the threshold. The purchase is split merely to:

- permit use of simplified acquisition procedures; or
- avoid any requirement that applies to purchases exceeding the micro-purchase threshold.

See [FAR 13.003\(c\)](#) for more information.



## Exceeding the Split Purchase Limit



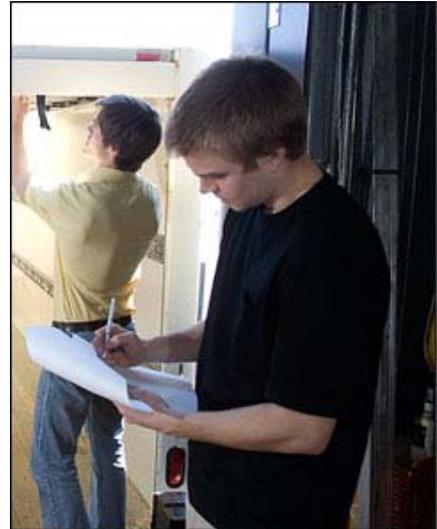
The Government Purchase Card can be used to purchase goods and services that cost \$2,500 or less. If the purchase exceeds the limit of \$2,500, it must be submitted to the Procurement Office for purchase, a more complicated and time-consuming process.

To circumvent the need to go through the Procurement Office, it might seem tempting to "split" a larger purchase into smaller ones. That way, the purchases fall under the \$2,500 threshold.

## Examples of Split Purchases

Examples of split purchases or split requirements include the following:

- A single cardholder makes multiple purchases from the same merchant on the same day. The total purchase amount exceeds the single purchase limit, and the total requirement was known at the time of the first purchase.
- A single cardholder purchases the same/similar item(s) from multiple merchants on the same day. The total purchase amount exceeds the single purchase limit, and the total was known at the time of the first purchase.
- A single cardholder makes multiple purchases of similar items from the same or multiple merchants over a period of time. The total purchase amount exceeds the single purchase limit, and the total was known at the time of the first purchase.
- Multiple cardholders under the same supervision/ approving official purchase the same/similar item(s) on the same day or in a compressed timeframe. The total purchase amount exceeds the single purchase limit, and the total was known at the time of the first purchase.



---

## Knowledge Review

Please select a correct answer.

**True or False?** Contractors may use a Government employee's GPC as long as its use has been authorized by the Contracting Office and the contractor notifies the Contracting Officer of all purchases made during the billing period.

- True
- False

Submit



---

## Knowledge Review

Please select a correct answer.

Normally, which of the following may not be purchased with a 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 source

Submit



---

## Knowledge Review

Please select a correct answer.

**True or False?** Splitting purchases to stay under a cardholder's single purchase limit is a prudent and efficient business practice permissible by law and regulation.

- True
- False

Submit



---

**What Is Cardholder Fraud?**

Fraud is any felonious act of corruption or attempt to deliberately cheat the Government or corrupt the Government's agents. More specifically, fraud is an act of deceit, misrepresentation, or an intentional perversion of truth in order to induce another individual to part with something of value or to surrender a legal right.

See 10 U.S.C. 932 for additional definition of fraud against the United States.



---

**What Is Cardholder Fraud?, Cont.**

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. If they don't, they may be using the card fraudulently.

Click each folder below to examine an instance of cardholder fraud.



D-Link Text:

This is a four option interactive flash module that includes the following content concerning fraudulent use of the Government Purchase card.

**Unauthorized Use**

In this situation, the cardholder conspired with a Merchant to make purchases not authorized by the cardholder's agency. The Merchant circumvented the authorization process to allow the cardholder to make purchases for personal consumption. The cardholder approved the transactions.

**Fraudulent Use**

In this situation, the cardholder conspired with a local company to make fraudulent purchases. No receipts were found to support the purchases. The amount of the purchases from this company exceeded the normal expenditures of other cardholders. The fraudulent purchases were never delivered to the Government.

**Kickbacks**

A business owner approached the cardholder and offered to provide kickbacks to the cardholder if the cardholder made purchases from his business. The cardholder was authorized to make purchases of these supplies, and the supplies were delivered. The company provided false receipts for supplies. The cardholder repeatedly made transactions with this company. The company paid the cardholder a percentage of the sales price.

Personal Use

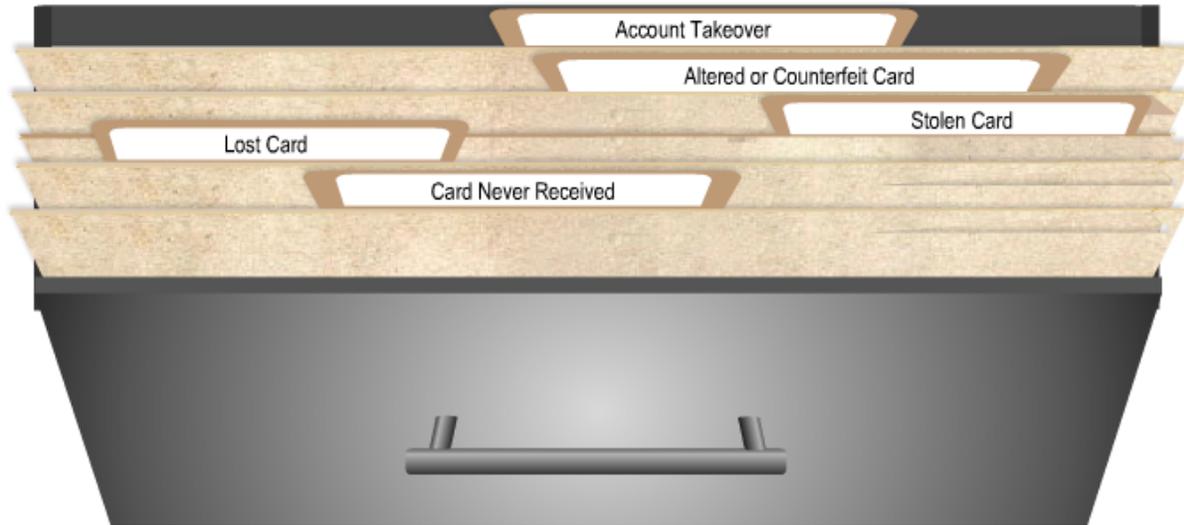
The cardholder obtained goods and services for personal use. The delivery address was the employee's home. A third party did not confirm receipt of materials. The cardholder advised the Merchant to split transactions to ensure they would not exceed the cardholder's single purchase limit.

Close window to continue

**What Is Noncardholder Fraud?**

Noncardholder fraud involves use of the card or cardholder data by an unauthorized person. The risk of Noncardholder fraud is higher in certain situations presented below.

Click on each folder tab for a more detailed examination:



[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 individual.

D-Link Text:

Five photos of various credit cards, labeled with the labels above. Please make sure that the credit cards are labeled with US Bank or Citibank logos, if there are logos.

When the student clicks the cards the following text displays:

FOR: Card Never Received

In this situation, a new card or a replacement card is mailed to the Cardholder but never received. Because the card could have been

intercepted by a third party, the Cardholder must notify the Bank to cancel the account. When a new card with a new account number is issued, the Cardholder must activate the new card by phone. This confirms that the new card has been received.

FOR: Lost Card

In the event that a Cardholder reports a misplaced or lost card, the account is closed, and a new card is issued. Reporting the card in either of these situations does not relieve the Government of its obligation to pay for transactions made by the Cardholder prior to reporting the loss. A Cardholder may be required to sign an affidavit confirming the card has been lost or misplaced.

If transactions not made by the Cardholder appear on the Statement of Account, the Cardholder should submit

a dispute form to the Card-Issuing Bank within 60 days of the statement. Failure to submit the dispute form and/or affidavit could result in liability to the Government.

FOR: Stolen Card

In the event that a Cardholder reports that 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 its obligation to pay for transactions that were made by the Cardholder prior to reporting the card stolen. A Cardholder may be required to sign an affidavit confirming that the card was stolen.

If the Cardholder did not make the transactions appearing on the Statement of Account, 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.

FOR: Altered/Counterfeit Card

Altered or counterfeit cards are normally identified by the Card-Issuing Bank's authorization process or by the Cardholder when the 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 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.

Account Takeover

This situation may be better known as identity theft; 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 unit to prevent the thief from obtaining a card in the Cardholder's name.

Close window to continue

## Reporting GPC Fraud

All Government employees have a duty to report all suspected instances of fraud to the appropriate authorities.

GPC cardholders must:

- Dispute any purchases listed on his/her statement and believed to be fraudulent
- Report cases of fraud to the card-issuing bank, their [Agency/Organization Program Coordinator \(APC\)](#), and their local procurement fraud advisor



Popup Text:

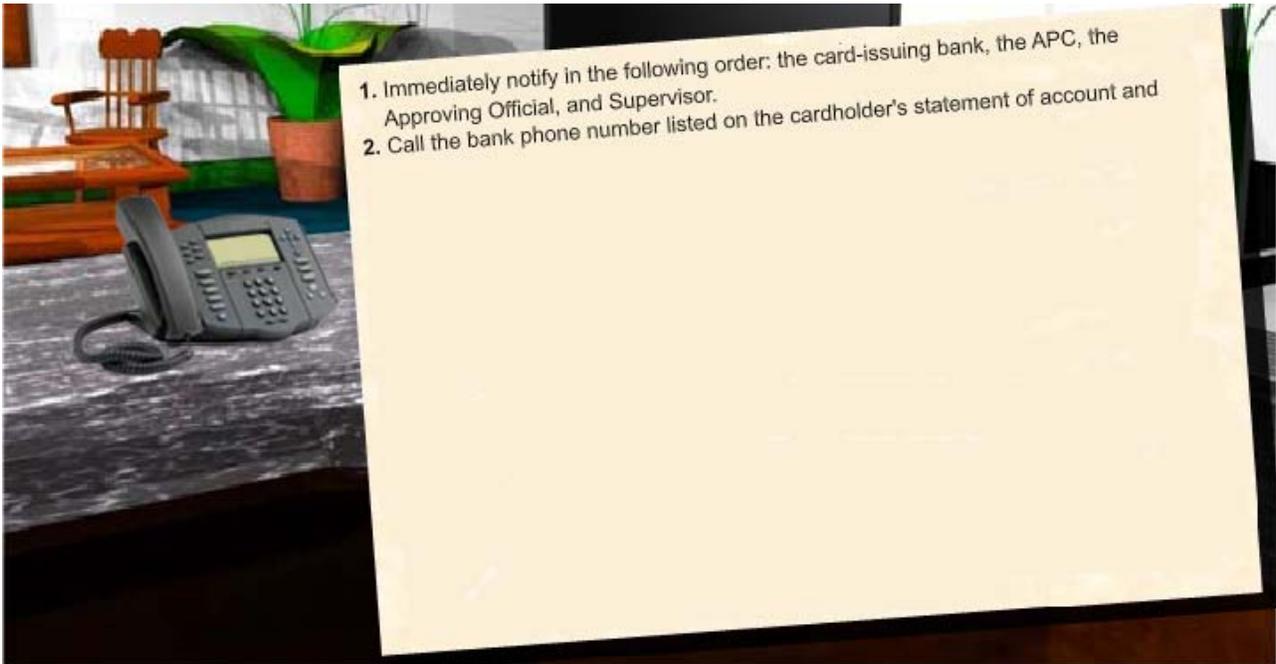
### **Agency/Organization Program Coordinator (APC)**

A Government employee designated to provide complete oversight of the local Government Purchase Card program. This individual is also referred to as an Agency Program Coordinator (APC).

---

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

If your card is lost or stolen there are a 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

---

## Fraud Oversight

GPC cardholders should be on the look-out for merchants or contractors who may be committing fraud. Examples of fraud could include billing for items not ordered or delivered, or delivering non-conforming items.

Approving Officials should examine purchase documentation for unauthorized purchases by cardholders as well as possible contractor fraud when reconciling the monthly statement.



---

## Reporting GPC Fraud

If GPC fraud is suspected, immediately contact the card-issuing bank:

US Bank - 1-888-994-6722  
Citibank - 1-888-786-0818

Then call the Agency Program Coordinator (APC), the DoD Fraud Hotline (1-800-424-9098), and the local procurement fraud advisor. In addition, contact the organization's Criminal Investigation Command.



---

### Detecting Fraud: Operation Mongoose



The DoD Purchase Card Program Management Office has partnered with [Operation Mongoose](#) to provide oversight and fraud detection for the Government Purchase Card Program.

The purpose of Operation Mongoose is to develop and operate an active Fraud Detection and Prevention Unit to minimize fraudulent attack against DoD assets. The unit includes 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.

Popup Text:

**Operation Mongoose**

A joint fraud detection and prevention program established by the Under Secretary of Defense (Comptroller)

---

## New Cards and Old Records

Cards are normally reissued every 24 months to each cardholder. This is automatic unless the APC halts 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 information about individual transactions within 45 business days of a request.

The Certifying Official must maintain certified billing statements for six years and three months from the date of the purchase transaction.

All other GPC records for purchases \$2,500 and less must be maintained for 3 years. These include:

- Cardholder statements
- Merchant receipts
- Packaging slips

Documentation supporting purchase card purchases greater than \$2,500 must be maintained for six years and three months.



---

## 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

Please select a correct answer.

The purpose of Operation Mongoose is to \_\_\_\_\_.

- Identify cardholder accounts that should be suspended
- Identify Billing/Certifying Official accounts that should be suspended
- Develop and operate an active Fraud Detection and Prevention Unit to minimize fraudulent attack against DoD assets
- Notify Agency/Organization Program Coordinators that additional cardholders should be appointed



Submit

---

## Knowledge Review

Please select a correct answer.

Which of the following is responsible for reporting GPC fraud?

- The cardholder
- The Approving Official
- The Agency/Organization Program Coordinator
- All of the above

Submit



---

## Ethics and Empowerment

In the past, the ability to obligate Government funds was reserved for a very few highly trained procurement professionals. These trained professionals were trained in the laws and regulations that applied to spending taxpayer money and in their responsibilities for compliance. With the explosion of the GPC usage, many nonprocurement people are now empowered to obligate Government funds.

This empowerment brings with it a responsibility to act ethically and within the bounds of laws and regulations.



---

## Regulation and Laws

Federal laws and regulations place restrictions on the actions of GPC cardholders.

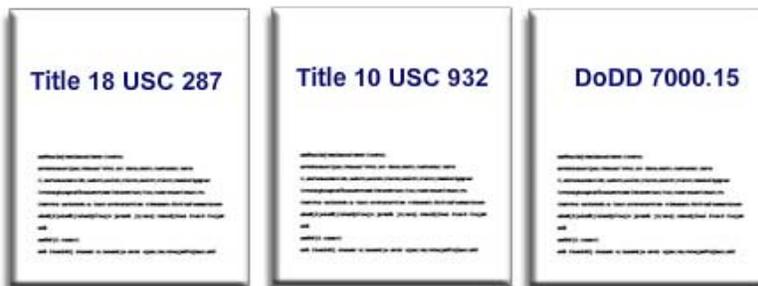
Intentional use of the GPC for other than official purchases:

- Will result in immediate cancellation of an individual's GPC.
- May be considered an attempt to commit fraud against the United States Government.
- May subject cardholders to penalties ranging from disciplinary action to criminal penalties. The cardholder will be held personally liable to the Government for the amount of any other than official transaction.



## Regulations and Laws, Cont.

Select each document for more information on regulations and laws related to the GPC.



D-Link Text:

This is a three option interactive flash module that includes the following information regarding:

- Title 18 USC 287
- Title 10 USC 932
- DoDD 7000.15

Title 18 USC 287 Under Title 18 U.S.C. 287, misuse of the purchase card could result in a fine of not more than \$10,000 or imprisonment for not more than five years or both.

LINK to Title 18: [http://www4.law.cornell.edu/uscode/html/uscode18/usc\\_sec\\_18\\_00000287----000-.html](http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00000287----000-.html)

Title 10 USC 932 Military members who misuse the purchase card may be subject to court martial under Title 10 U.S.C. 932, UCMJ Art. 132. Depending on the circumstances, other sections of the US Code may apply and may carry additional penalties.

LINK to Title 10: [http://www4.law.cornell.edu/uscode/html/uscode10/usc\\_sec\\_10\\_00000932----000-.html](http://www4.law.cornell.edu/uscode/html/uscode10/usc_sec_10_00000932----000-.html)

DoDD 7000.15 As explained in the DoD Directive 7000.15, "DoD Accountable Officials and Certifying Officers", and DoD 7000.14, "DoD Financial Management Regulation", Volume 5, Chapter 33, Certifying Officials are pecuniarily liable for erroneous payments resulting from the negligent performance of their duties. Such liability may be relieved under specific circumstances (Title 31 USC Section 3527 and 2538). Furthermore, cardholders are held responsible for erroneous payments resulting from the negligent performance of their duties.

LINK to DoDD 7000.15: [http://biotech.law.lsu.edu/blaw/dodd/corres/pdf/d700015\\_070898/d700015p.pdf](http://biotech.law.lsu.edu/blaw/dodd/corres/pdf/d700015_070898/d700015p.pdf)

Close window to continue

## Accountability for Illegal or Improper Use of the GPC

Cardholders and Approving Officials have been held accountable for illegal or improper use of the GPC. Click the gavel below to read some examples.



D-Link Text:

A graphic of a (judge's) gavel. When the student clicks the graphic, the gavel comes down. Then a pop-up box appears. The pop-up box has a NEXT button, and it contains the following text:

### Example #1

One former DoD employee pled guilty to conspiracy to defraud the Government using his official purchase card. He was sentenced

in U.S. District Court, Eastern District of Virginia, to 2 years probation, and ordered to pay restitution and other fees of \$70,100. He also received six months of electronic monitoring.

Click the Next button for another example.

When the student clicks NEXT, another pop-up box appears. It contains the text below. This continues until all four examples have displayed.

### Example #2

Another former DoD employee pled guilty to using a Government credit card to buy a television for personal use. He was terminated from DoD employment and sentenced in Federal Court in the Eastern District of Texas to a \$3,000 fine and ordered to pay \$1,400 restitution.

Click the Next button for another example.

**Example #3**

Another former DoD employee pled guilty to one-count criminal information charging him with theft using a Government credit card. He

was sentenced in U.S. District Court, Eastern District of Virginia, to 4 months imprisonment, 4 months home detention, 3 years probation and ordered to pay \$61,465 in restitution and other fees.

Click the Next button for another example.

NOTE: The last button has a CLOSE button, rather than a NEXT button.

**Example #4**

Yet another former employee pled guilty to conspiracy in a fraudulent scheme involving the misuse of a purchase card while assigned

to DoD. He was sentenced in U.S. District Court, Eastern District of Virginia, to serve a jail term of 12 months and one day, 24 months probation, and ordered to pay restitution and other fees totaling \$120,100.

Close window to continue

---

**Standards of Conduct: Regulatory Guidance**



Federal Acquisition Regulation (FAR 3.101) and 5 CFR Part 2635 establish general standards of conduct guidelines for all agencies.

- Subpart D forbids any conflict of interest in Government-Contractor relationships.
- Subpart B says that no Government employee may solicit or accept any gratuity, gift, favor, entertainment or anything of monetary value from any party doing business with or seeking to obtain business with the employee's agency.
- 5 CFR 2635, Subpart G governs misuse of position, including government resources.

---

## Joint Ethics Regulation

All Government agencies are required to prescribe their own standards of conduct. These should outline agency exceptions to FAR 3.101 and disciplinary actions for persons violating the standards detailed in [DoD Directive 5500.7-R](#), Joint Ethics Regulation, and Standards of Conduct for Employees of the Executive Branch (5 CFR Part 2635). It is the responsibility of each employee to know and follow all general and agency standards.

Under the Joint Ethics Regulation, there is an obligation to report suspected ethics violations. This includes reporting by Certifying Officials, Supervisors or fellow employees of suspected misuse of the Government Purchase Card. Reports should be made to the supervisor, the ethics official, Commander, Director, Defense Criminal Investigative Service or the DoD Hotline.



---

## Ethical Conduct

Executive Orders (EOs) [12674](#) and [12731](#) establish Ethical Conduct and are the foundation for policy. The broad principles of these EOs illustrate why poor judgment could cause an employee to inadvertently do something unethical. These EOs specify that employees are to avoid any action that might result in or create an appearance of:

- Using public office for private gain
- Giving preferential treatment to any private organization or individual
- Adversely affecting public confidence in the Government's integrity
- Making unauthorized commitments
- Defrauding the Government or failing to report fraud

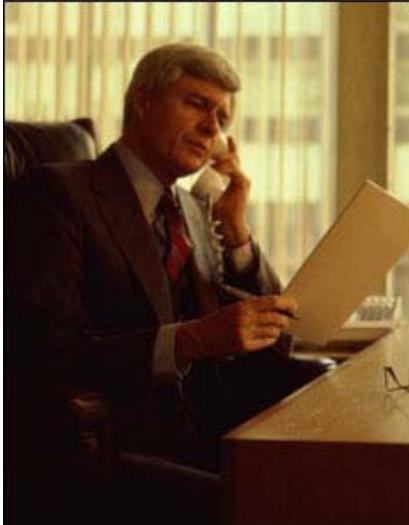
The Agency Ethics Counselor is available to resolve questions or concerns about the standards of conduct and ethical behavior.

---

## Specific Provisions for Government Employees

Specific ethics provisions for Government employees:

- Using Government property only for authorized purposes. (5 CFR Section 2635.704)
- Satisfying financial obligations. (5 CFR Section 2635.809)
- Directing any questions on the standards of conduct to the Agency Ethics Counselor.



If a GPC Cardholder learns that unauthorized persons have placed charges against a card for which he/she is responsible, the Cardholder should immediately notify both the Bank and the agency program officials responsible for the program.

Accountability for Cards - DoD components must ensure that GPC Cardholders are responsible and that authorization for use of the card is withdrawn when a Cardholder uses the card irresponsibly. Commands should conduct periodic audits to ensure that charges are appropriate and that only authorized charges are being made.

---

**Knowledge Review**

Please select all that apply by clicking on the check box.

Read the statement below. Then click the individual(s) to whom the statement applies. Select all individuals that apply. Then click the SUBMIT button.

- Certifying Official
- Supervisor
- Agency/Organization Program Coordinator
- Agency Ethics Official

Submit



Scenario



D-Link Text:

This is an interactive flash scenario. You are presented with a 3-D environment where you are sitting at a desk with a phone and a computer.

When you see the pop-up on the computer screen, indicating that you have one unread message, click on the screen to view the message.

When the phone is selected an interface appears presenting the headshot of a women and the following narrative:

Hi, this is Joan Reynolds, and I am a Purchase Cardholder. My office wants a television for the conference room, so I purchased one for \$750.99. After returning to the office I realized that I should have purchased one for the other conference room as well. The purchases totaled \$3003.96. I am calling to determine if I should have made these purchases?

Is this an example of an unauthorized use of the Government Purchase Card? **Yes** or **No**

**Yes**

Yes, you are right! This is an example of an unauthorized use of the Government Purchase Card (GPC) because a single cardholder should not make multiple purchases from the same merchant on the same day.

**No**

Sorry, that is incorrect. This is an example of an unauthorized use of the Government Purchase Card (GPC)

because a single cardholder should not make multiple purchases from the same merchant on the same day.

When you see the pop-up on the computer screen, indicating that you have one unread message, click on the screen to view the message.

When the computer is selected an interface appears presenting the headshot of a man and you receive the following email:

From: James Calhoun

Subject: Travel Card vs. Purchase Card

Hi, I am on a business trip and when I arrived at the airport I needed a rental car. I used my Government travel card instead of my Government Purchase Card. Was that a wrong move on my part? Let me know. Thanks!

Is this an example of an unauthorized use of the Government Purchase Card? **Yes** or **No**

**Yes**

Sorry, that is incorrect. This is not an example of an unauthorized use of the Government Purchase Card (GPC) because travel-related expenses, such as lodging and rental cars, should be paid with the Government travel card, not the Government Purchase Card.

**No**

Yes, you are right! This is not an example of an unauthorized use of the Government Purchase Card (GPC) because travel-related expenses, such as lodging and rental cars, should be paid with the Government travel card, not the Government Purchase Card.

Close window to continue

## Topic Summary

This topic discussed restrictions on GPC use, fraud and ethical standards related to GPC use. You should now be able to:

- Recognize restrictions on Government Purchase Card (GPC) use.
- Identify types of fraud.
- Recognize reporting procedures for fraudulent use of and lost/stolen Government Purchase Cards.
- Identify ethical standards of conduct and their regulatory/legal foundation.

You have now completed this topic. Please select the next topic from the table of contents to continue.

Click [here](#) for a print version of this topic.