What Happens if I Become a Victim?

If you discover that someone else has used your card, promptly report the incident to your A/OPC and your bank's customer service representative.

Liability of the government for lost or stolen cards is $0. Once your card (or the cardholder information) has been reported lost or stolen, the card is immediately blocked. The bank will then issue you a new card with a new account number. Also, your bank will send you a letter explaining the steps you can take to protect yourself further.

Sometimes, unauthorized transactions will appear on the cardholder statement, even though the card was reported lost or stolen. You should report all unauthorized transactions by calling the customer service telephone number on the back of your card.

If your GSA SmartPay card falls victim to fraud, contact your A/OPC and your agency's bank immediately. (For your convenience, banks' e-mail addresses and telephone numbers are listed below.)

U.S. Bank®
fraud_help@usbank.com
(877) 595-6256

J.P. Morgan®
abuse@chase.com
(888) 297-0781

Citibank®
emailsproof@citigroup.com
(800) 274-6660

GSA

U.S. General Services Administration

GSA SmartPay Program Support
www.gsa.gov/gsasmartpay
(703) 605-2808
gsa_smartpay@gsa.gov

www.gsa.gov
August 2010
5-10-00602

Order additional copies at gsa.gov/cmls.

F Federal Audience

M Military Audience

Federal Recycling Program ♻ Printed Using Recycled Materials

GSA SmartPay
Supporting your mission

Knowledge:

The Best Protection for Your GSA SmartPay Card

Tips to Help You Detect and Avoid Fraud

What is Fraud?

Fraud can be defined as a deception deliberately practiced with the motive of securing unfair or unlawful gain. Specific to our topic here, fraud can be an attempt to cheat the government — and corrupt its agents — by using government issued GSA SmartPay® cards for transactions not part of official government business. Like any deception, charge card fraud has its fair share of victims — and the purpose of this brochure is to help you, your agency, and the federal government avoid being victimized.

Fraud can come in many disguises, such as false e-mails, mail, or phone calls. Likewise, intentional misuse of a GSA SmartPay card by the cardholder can result in fraud. In addition, non-cardholder fraud involves the use of the charge card or cardholder information by an unauthorized person.

As a GSA SmartPay cardholder, you should be aware and take necessary steps to protect your card and yourself. This brochure will help.

Types of Fraud Include:

Counterfeit Credit Cards — To make fake cards, criminals use the newest technology to "skim" information contained on magnetic stripes of cards, and also to pass security features (such as holograms).

Lost or Stolen Cards — Often cards are stolen from a workplace, gym or unattended vehicle.

Card Not Present (CNP) Fraud — Internet fraud occurs whenever charge card information is stolen and used to make online purchases. Usually, a merchant will ask for the CVC code (located on the back of the card itself) to help prevent this type of fraud.

Phishing — Phishing occurs whenever a cardholder receives a fake e-mail directing him or her to enter sensitive personal information on a phony website. The false website enables the criminal to steal information from the cardholder.

Non-Receipt Fraud — This occurs whenever new or replacement cards are mailed and then stolen while in transit.

Identity Theft Fraud — Whenever a criminal applies for cards using another person's identity and information, this type of fraud occurs.

How Can I Detect Fraud?

One of the first signs that you have been a victim of fraud will be at least one "mystery expense" showing up in your monthly charge card statement. To help detect fraud, you should verify your statement by:

- Looking for transactions you do not recall making;
- Checking for unknown vendors; and
- Searching for account withdrawals you do not remember making.

How Can I Avoid Fraud?

Below are 14 valuable tips to help you avoid charge card fraud:

1. Never leave your cards unattended.
2. Safeguard your personal identification number (PIN). Do not write it down — memorize it. Share your PIN with no one.
3. Monitor your card during transactions. When the card is returned, check to make sure it is indeed yours.
4. Make a list of your card numbers with key contact information, in case you need to report cards lost or stolen.
5. Immediately report lost/stolen cards and/or any questionable charges.
6. Sign the back of a new card as soon as you receive it. If you do not receive a replacement card before the expiration date of the older card, contact the bank.
7. Destroy unwanted or expired cards and shred (or secure) monthly statements and receipts.
8. Always verify charges appearing on your monthly statement. Note that online statements provide a faster, more efficient way to check for fraudulent activities.
9. Unless you initiated the purchase, never give your charge card information over the telephone, through the mail, or on the Internet.
10. Consistently check your card account for accuracy of personal and billing information. Notify the bank if your personal information and/or address needs to be updated.
11. Never let a telemarketer or salesperson pressure you into agreeing to a deal.
12. Be aware of common charge card scams. If you are unsure of a situation, please contact your A/OPC or the bank.
13. Examine your credit report at least once a year.
14. Update the anti-spyware and -virus software on your computer.