GSA SmartPay®
Supporting your mission

U.S. General Services Administration

Fighting Fraud With Knowledge:

The Best Protection for Your GSA SmartPay Account

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 accounts 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 emails, mail, and phone calls. Likewise, intentional misuse of a GSA SmartPay account by the account holder can result in fraud. In addition, non-account holder fraud involves the use of the account or account holder information by an unauthorized person. As a GSA SmartPay account holder, you should be aware and take necessary steps to protect your account and yourself. The following information will help you to do so.

Types of Fraud

Fraud types include:

- **Counterfeit Credit Cards** – To make fake cards, criminals use the newest technology to "skim" information contained on magnetic strips of cards and also to pass security features (such as holograms).
- **Lost and Stolen Cards** – Often, cards are stolen from a workplace, gym, or unattended vehicle.
- **Card Not Present (CNP) Fraud** – Internet fraud occurs whenever account 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) to help prevent this type of fraud.
- **Phishing** – Phishing occurs whenever an account holder receives a fake email directing them to enter sensitive personal information on a phony website. The false website enables the criminal to steal information from the account holder.
- **Non-Receipt Fraud** – This occurs whenever a new or replacement card is 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 You 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 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.

GSA SmartPay®

Supporting your mission

How Can You Protect Yourself Against Fraud?

Below are valuable tips to help you protect yourself against fraud:

1. Never leave your cards unattended.
2. Safeguard your personal identification number (PIN). Do not write it down – memorize it. Do not share your PIN.
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 account numbers with key contact information, in case you need to report the account as lost or stolen.
5. Immediately report lost/stolen accounts and/or 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 initiate the purchase, never give your account information over the telephone, through the mail, or on the Internet.
10. Consistently check your account for accuracy of personal and billing information. Notify the bank if your personal information and/or address need to be updated.
11. Never let a telemarketer or salesperson pressure you into agreeing to a deal.
12. Be aware of common 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 antivirus software on your computer.
15. Use the chip instead of swiping the magnetic strip, whenever possible.
16. Inspect ATMs and gas pumps before using for possible signs of skimming devices. If an ATM appears to be tampered with or the slot where the card is inserted is loose, do not use.

What Should You Do if You Suspect Your Account has Fallen Victim to Fraud?

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

Liability of the government for lost and stolen accounts is $0. If your account has been reported lost or stolen – or the account holder information has been stolen – the account will be 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 further protect yourself.

Sometimes, unauthorized transactions will appear on the account holder statement, even though the account was reported lost or stolen. You should report all unauthorized transactions by calling the customer service telephone number associate with the issuing bank. If your GSA SmartPay account falls victim to fraud, immediately contact your A/OPC and your agency's bank. For your convenience, the banks' email addresses and telephone numbers are listed below.

U.S. Bank®
fraud_help@usbank.com
(888) 994-6722

Citibank®
emailsproof@citigroup.com
(800) 790-7206

GSA SmartPay Program Support

gsa_smartpay@gsa.gov
(703) 605-2808
https://smartpay.gsa.gov

www.gsa.gov
December 2018
5-19-00263

View, download, and order publications via www.gsa.gov/cmls.