



U.S. General Services Administration

Federal Acquisition Service

Conduct Effective Oversight of Your GSA
SmartPay Program

Erin VanDagna
Office of Charge Card Management
General Services Administration

2014 GSA SmartPay Virtual Training Forum
July 29 - 31, 2014



Relevant Legislation and Policies

Government Charge Card Abuse Prevention Act of 2012

On October 5, 2012, President Obama signed the Government Charge Card Abuse Prevention Act of 2011 (Public Law 112-194):

- OMB Memo M-13-21 and Smart Bulletin 021 were issued
 - <https://smartpay.gsa.gov/about-gsa-smartpay/policies/OMB-M-13-21/FAQs>
- OMB is in the process of drafting a letter to Congress on the analysis of the agency reports
 - Based on the results, there doesn't appear to be any significant or red flag issues to report on any agency card program(s).

Legislation

- ***Improper Payments Elimination and Recovery Improvement Act of 2012***
 - actively mitigate improper payments, fraud, waste, and abuse by accessing the Federal Do Not Pay List
 - to verify that vendors are eligible to receive government payments, including contracts.

- **S.1360 - Improper Payments Agency Cooperation Enhancement Act of 2013** (introduced 7/24/13)
 - Amends the Improper Payments Elimination and Recovery Improvement Act of 2012
 - SSA to maintain National Deaths Registry and provide data to IGs, States, Local governments etc. to facilitate payment recoveries

Legislation Continued

- **S.1360 - Improper Payments Agency Cooperation Enhancement Act of 2013** (introduced 7/24/13)
 - OMB to identify agencies that operate databases related to federal beneficiaries and annuity recipients
 - OMB to convene a task force to improve information sharing related to federal beneficiaries and annuity recipients
 - Secretary of Treasury to report to Congress as part of the Do Not Pay Initiative
 - SPS to provide access to address information

GAO Purchase Card Report

The Government Accountability Office (GAO) released a report in 2008 analyzing government GSA SmartPay Purchase Card transactions across the Federal government:

- GAO sought to identify internal control weaknesses in the GSA SmartPay Purchase Card Program
- Tried to identify examples of fraudulent, improper, and abusive activity
- GAO found that internal control weaknesses in agency Purchase Card programs exposed the Federal government to fraud, waste, abuse, and loss of assets

GAO Recommendations

- Strengthen/ improve oversight and internal controls
- Provide guidance to cardholders about documentation requirements (e.g., receipts)
- Require prior approval or purchase review
- Reminder: Employees must reduce “meals and incidental” claimed for travel vouchers if they receive paid-for-meals when on travel
- Guidance sensitive and pilferable property (i.e. easily converted for personal use)
- Cancel convenience check privileges for cardholders who improperly use checks



Definitions and Industry Trends

What is Fraud?

Fraud is defined as a deceitful practice or willful device, resorted to with intent to deprive another of rights or in some manner to cause injury.

Charge Card Fraud

There are several situations during which fraud may occur:

- Card issued from bank but cardholder did not receive the card
- Cardholder loses card or card is stolen
- Card or account information is replicated or counterfeited

** Please note that in the case of fraud occurring on lost or stolen cards/account numbers, the cardholder is not liable for transactions.

Common Examples of Fraud

- Stolen Cards
- Identity Theft
- Application Fraud
- Account Takeover
- Skimming
- Card Not Present
- Carding
- Phishing

Example 1 – Stolen Cards

Fraud

Abuse/Misuse

Fraudsters can use stolen charge cards at vendors before a cardholder can close or suspend an account. As the only preventative measure physically available on a traditional card is a cardholder's signature, fraudsters may be able to forge authorizing signatures at merchants. Additional notes include:

- In some jurisdictions, the law prohibits merchants from requesting supplemental identification
- Self serve payment stations (e.g., gas stations) are convenient targets for stolen cards

Food for Thought

Chip and PIN cards products may be effective in managing this risk.

Example 2 - Skimming

Fraud

Abuse/Misuse

Skimming is a broad term used to describe the act of a fraudster obtain an active card account number and security code. Examples include:

- Can be simple as a fraudster reading an account number over a cardholder's shoulder
- Account numbers may be lifted from discarded receipts or poorly/un-shredded account statements
- Electronic devices can be used at automatic tellers, on top of authentic card processors, or anywhere a cardholder physically swipes the card

Example 3 – Card Not Present

Fraud

Abuse/Misuse

Card Not Present (CNP) fraud occurs when fraudsters acquire enough account information and use accounts primarily at online vendors:

- Online merchants often only require account numbers, security codes, and addresses to process transactions
- Account information may be obtained through other methods such as phishing, stolen cards, or skimming

Food for Thought

Single Use Account products may be effective in managing this risk.

What is Abuse and Misuse?

Abuse and misuse occurs when a cardholder uses the card as a method of payment for unauthorized transactions that are not permitted in accordance with agency or division policy:

- In the case of GSA SmartPay Charge Cards, intentional use of the charge card for other than official government transactions constitutes misuse, and may involve fraud
- The cardholder is liable for all transactions classified as abuse and misuse

Example 1 - Unallowable

Abuse/Misuse

Fraud

In a 2009 agency Inspector General report on charge card use, findings included several instances where purchase cardholders made unauthorized purchases for fleet-related activities, violating agency Purchase Card policy. Additional findings include:

- In some of the instances, there was no evidence of the required written supervisor approval for transactions
- In accordance with the GSA SmartPay 2 master contract, fleet cards can only be used for fleet-related transactions.

Example 2 - Abuse

Abuse/Misuse

Fraud

In a 2013 agency Inspector General report analyzing more than 1 million travel card transactions, investigators found approximately 500 transactions that could not be associated with authorized government business.

- Violations included ATM cash advance withdrawals
- Many accounts also carried significant delinquent amounts, violating card program policy
- IG recommended manual review of all travel transactions to mitigate risk of abuse and misuse

Risks – Management Control

Abuse/Misuse

Fraud

Agency Inspector General and audit reports identify non-adherence to agency policies and weak management controls significant risks for abuse, misuse, and waste. Some examples include:

- Accounts not properly closed or transferred
- Card managers not consistently monitoring delinquent payment reports
- Weak processes for ensuring timely payment of charge card bills
- Cardholder training requirements not always completed or completed in a timely manner

Risks – Replica Receipts

Abuse/Misuse

Fraud

There are a number of online vendors who offer hardcopy receipt replica services. Although legal disclaimers indicate documents for recreational use only, replica documentation includes current corporate logos from major retailers, including those the government does business with. It may be difficult to differentiate between replicas and genuine receipts. Services from these replica vendors often include:

- Replica receipts with corporate logos
- Receipts from restaurants, hotels, and more
- Templates for users to create recurring replicas



Fraud and Abuse Prevention

Consequences of Abuse and Misuse

In instances of suspected abuse and misuse, it should immediately be reported to the proper authority. Should abuse and misuse be proven, there are disciplinary actions available, as appropriate and authorized. These may include:

- Employee is liable for transaction amount
- Reprimand
- Counseling
- Notation in employee performance evaluation
- Suspension or termination of employment
- Criminal prosecution

Identifying Fraud & Abuse (1 of 2)

When reviewing account activity, there may be some early warning signs or clues to fraudulent or abusive activity, which include but are not limited to **:

- Accounts closed due to fraud and new cards reissued
- Merchant address appears to be a home address
- Merchant Category Code (MCC) is outside the cardholder's general area of responsibility
- Cardholder frequently disputes transactions

** Note these early warning signs are indicators of "unusual or higher risk activity" and not necessarily of fraud or abuse. Agencies are responsible for monitoring, following-up, and addressing potential instances of fraud and abuse.

Identifying Fraud & Abuse (2 of 2)

- Multiple authorizations have been declined
- Transactions occur on non-business days
- Maximum spend limits are consistently reached
- Multiple transactions with one merchant in a short period of time and totals more than \$3,000
- No proof of purchase (e.g., receipts)
- Multiple transactions of even dollar amounts (e.g., \$20, \$100, \$300)
- Repeated transactions from repeating merchants

** Note these early warning signs are indicators of "unusual or higher risk activity" and not necessarily of fraud or abuse. Agencies are responsible for monitoring, following-up, and addressing potential instances of fraud and abuse.

Fraud Liability

One of the benefits of using the GSA SmartPay Program as a method of payment is that in instances of fraud, GSA SmartPay contractor banks assume the liability of payment and agencies are not responsible for paying balances in the instance of authentic fraud.

- Information available in cardholder agreements with GSA SmartPay contractor banks and network agreements

Reminder

Agencies (cardholders) are not liable in instances of fraud, however cardholders can be held liable for payment for abuse and misuse.

Addressing Fraud and Abuse

Agency card managers are the front lines of defense:

- Promote appropriate use of GSA SmartPay solutions
- Establish agency specific policies and procedures
- Ensure cardholders receive appropriate training and take refresher training at a minimum once every three years, or more frequently (as required by your agency/organization)
- Monitor account activity and manage delinquencies
- Take appropriate action to address fraud, abuse, and misuse

A/OPC Leading Practices (1 of 2)

Card managers must help establish clear to prevent abuse and misuse through reconciliation guidance and risk management controls, such as:

- Controls on cards – credit, single purchase limit, Merchant Category Code blocks
- Cash advances (Travel) and convenience check limits (Purchase)
- Managing delinquencies
- Using reporting tools to monitor card activity, including requiring certain standard and ad hoc reporting

A/OPC Leading Practices (2 of 2)

Card managers should also:

- Establish a hierarchy and providing guidance on functionality for levels of A/OPCs such as authorities to open, close, and maintain accounts and process for account cancellation
- Clearly communicate consequences for abuse
- Outline frequency and processes for auditing card programs
- Communicate policy and refresher training requirements for cardholders – implement and maintain documentation

Cardholder Responsibilities

Card managers should remind cardholders of their roles in preventing fraud, waste, and misuse:

- Use of GSA SmartPay solutions in accordance with policy, laws, and governmental regulations
- Understand preventative actions to avoid fraud and misuse and what to do if it occurs
- Understand consequences to abuse and misuse
- Comply with training and refresher training requirements
- Review “Cardholder Dos and Don’ts” and the GSA SmartPay Fraud brochure

Responding to Fraud

Card managers are responsible for reporting any suspected or actual fraud to the GSA SmartPay contractor bank and the agency Inspector General. Card managers should work with cardholders to ensure that:

- A complaint is filed with the agency Inspector General
- Fraud is reported to the agency fraud hotline, as available
- GSA SmartPay contractor bank is contacted for available tools and resources



Resources

GSA SmartPay Website



- What's New
- Program Statistics
- New Legislation
- State Tax Information
- Managing Your Program
- GSA SmartBlog
- Accepting GSA SmartPay® Cards
- Online Training for Cardholders and A/OPCs

<http://smartpay.gsa.gov>

<https://interact.gsa.gov>

General Contact Information

GSA Contact Information:

- GSA SmartPay Program Support (<http://www.smartpay.gsa.gov>)
Helpline: (703) 605-2808

Bank Contact Information:

- Citibank (<http://www.cards.citidirect.com/welcome.asp>)
Customer Service: (800) 790-7206
- JP Morgan Chase (<https://www.paymentnet.com/Login.asp>)
Customer Service: (888) 297-0781
- U.S. Bank (<https://access.usbank.com/cpsApp1/index.jsp>)
Customer Service: (888) 994-6722

Additional GSA SmartPay Courses

GSA SmartPay 2 Program Update

Conduct Effective Oversight of Your GSA SmartPay Program

GSA SmartPay 2 Master Contract Basics

GSA SmartPay Saves: Innovative Payment Solutions

GSA SmartPay Purchase Management Essentials

GSA SmartPay Travel Management Essentials

GSA SmartPay Fleet Management Essentials

GSA SmartTax: What You Should Know About State Taxes

GSA SmartPay Website

Audience Questions

**Thank you for your time and
attention!**

Contact Information

Erin VanDagna
erin.vandagna@gsa.gov

Please provide your feedback and thoughts on our website, available at
<http://smartpay.gsa.gov/feedback>.