

The GSA SmartPay Purchase Program





Table of Content

- Chapter 1:**
Overview of the GSA SmartPay Purchase Program – Supporting Your Mission 5
- Chapter 2:**
Policies10
- Chapter 3:**
Roles and Responsibilities within the Program.....12
- Chapter 4:**
Strategic Payment Solutions.....16
- Chapter 5:**
Misuse/Abuse/Fraud21
- Chapter 6:**
Liability27
- Chapter 7:**
The Review Process.....28
- Chapter 8:**
Electronic Access System (EAS)/Reporting30
- Chapter 9:**
Preventative Measures32
- Chapter 10:**
Joining the Community.....37
- Appendix**39

Introduction



The GSA SmartPay® program is the largest government charge card and payment solutions program in the world. The program has more than 3 million purchase, travel, fleet, and integrated accounts and supports more than 560 agencies/organizations. Since the award of the inaugural GSA SmartPay Master Contract in 1998, the GSA SmartPay program has provided convenient, efficient, and effective payment solutions for the federal government and tribal organizations, with a comprehensive portfolio of payment solutions.

Specific to purchase, the GSA SmartPay program:

- Provides commercial payment solutions and associated services in support of official government purchases;
- Streamlines ordering, payment, and procurement procedures;
- Reduces administrative costs;
- Improves government operations by simplifying the financial process; and
- Allows a platform to improve government operations and accountability.

Through a master contract with multiple banks, the GSA SmartPay program enables agencies/organizations across the federal government to obtain payment solutions to support mission needs. The GSA SmartPay Master Contract, administered by GSA, is a fixed-price, indefinite-delivery/indefinite-quantity (IDIQ) type of contract. The base period for the master contract is four years with three three-year options. Agency/organization task orders should be written with this period of performance in mind.

To participate in the program, an agency/organization issues a task order under the GSA SmartPay Master Contract and selects one of the GSA SmartPay contractor banks, Citibank, N.A. (Citi®) or U.S. Bank®, for its program. The agency/organization then receives payment solutions and related

services through the task order with the selected contractor bank. The task order enables the agency/organization to work directly with that GSA SmartPay contractor bank to receive purchase business line products –and services. Through the task order, Agency/Organization Program Coordinators (A/OPCs) set up accounts for account holders, manage accounts using the bank’s Electronic Access System (EAS), and resolve issues and questions by working directly with their assigned Customer Relationship Manager (CRM) or other designated bank representative.

A purchase account is provided to the agency/organization and designates an individual or individuals to be responsible for purchases made on the account. Account holders are either appointed by their A/OPC or designated by an Approving Official (AO). Any government employee who is authorized to use the GSA SmartPay program and completes the necessary training is eligible to become an account holder. Personal credit history is not a criterion for receiving a purchase account, and any use of the purchase account will not affect personal credit history.

Benefits

By awarding a task order under the GSA SmartPay Master Contract, agencies/organizations benefit from:

- A faster contract acquisition process as compared with a full and open competitive procurement
- Favorable negotiating platform and contract terms
- Awards to contractor banks based on a competitive proposal process
- Established relationships with contractor banks
- A broad range of flexible products and services for agencies/organizations, as well as the flexibility to access “value added” products and services specific to the contractor bank
- Ongoing support for the agency/organization

Introduction (continued)



Agencies/organizations also benefit from:

- **Universal Acceptance:** Because GSA SmartPay purchase accounts are either Visa® or Mastercard® brands, they can be used at any merchant that already accepts these brands for payment.
- **Refunds:** Agencies receive monetary payments provided by the contractor bank based on the dollar or spend volume during a specified time period, which results in millions of dollars back to agencies/organizations each year.
- **EAS to Data:** The GSA SmartPay contractor banks provide an EAS, which provides account access, account management, and a variety of reports for A/OPCs to assist in the effective management of the program. The EAS also functions as a document repository for all GSA SmartPay transactions for a period of six (6) years after final contract payment, as defined by the agency/organization in the task order.

Use of the purchase account benefits the government in many ways:

- The GSA SmartPay accounts save the government time, money, and resources.
- The GSA SmartPay purchase program provides the government with financial and cash management control over low-dollar value and high-volume procurements, and it can serve as a payment tool for larger transactions, consistent with agency policy.
- The government saves money by making only one payment to the contractor bank rather than thousands of payments to individual merchants.

- The government improves the use of its resources by freeing up contracting personnel, so they are able to focus on more complex activities that derive greater benefit from their expertise.
- Merchants throughout the world accept the GSA SmartPay purchase account because it is a commercial product.

As an A/OPC, you are responsible for the overall management and oversight of the accounts under your span of control. Your role is essential to efficiently and effectively managing your agency's/organization's GSA SmartPay purchase program. Generally speaking, your responsibilities include:

- Setting up accounts and designating authorization controls;
- Serving as a liaison between account holders and the contractor bank;
- Providing ongoing advice and assistance to account holders;
- Maintaining account information;
- Developing agency policies and procedures, as needed;
- Auditing purchase accounts as required by your agency policy; and
- Using the contractor bank's EAS to perform account management and oversight.

This manual is intended to serve as a source of information for assisting in the oversight role. Use of the GSA SmartPay purchase payment solutions should be in accordance with agency/organization-specific policy.

Chapter 1: Overview



The Center for Charge Card Management

The Center for Charge Card Management (CCCM) administers the GSA SmartPay program and is committed to supporting the missions of its customer agencies. CCCM's commitment to customers includes:

- Providing excellent customer service to both program coordinators and account holders;
- Serving as customer advocates for both GSA SmartPay contractor banks and oversight bodies;
- Providing and supporting the availability of clean, valid, and reliable account data;
- Helping to ensure security of customer data through information and personnel security; and
- Supporting customer contract and task order management.

Customer Service

CCCM is committed to providing high-quality direct support to program coordinators and their stakeholders. These efforts include, but are not limited to:

- Dedicated customer-service phone line ([703] 605-2808) and email (gsa_smartpay@gsa.gov);
- GSA SmartPay website and other [online resources](#);
- [Free online training](#);
- Hosting in-person and virtual training forums for card program managers (e.g., A/OPCs, AOs);
- Managing the Charge Card Manager Certification (CCMC) Program for A/OPCs;
- Facilitating customer meetings and working groups; and
- Providing ad hoc executive customer support.

Relationship Management

CCCM collaborates and coordinates with customers to help manage critical relationships, which include GSA SmartPay contractor banks, Congress, the Office of Management and Budget (OMB), and other executive branch entities. Activities include:

- Monitoring legislative and policy trends and developments;
- Working with customers to provide input to, plan for, and execute requirements;
- Facilitating agency working groups;
- Serving as customer advocates for contractor banks and resolving identified issues; and
- Building a community of program coordinators to share best practices and lessons learned.



Chapter 1 (continued)

Data Management, Security, and Monitoring

CCCM works closely with GSA SmartPay contractor banks and networks to help ensure that customer data, access to data, and spend information is clean and secure. CCCM also provides tools and reports that support program coordinators to more effectively enhance program performance. Activities include:

- Developing, maintaining, and enhancing the GSA SmartPay Data Warehouse;
- Consolidating, cleaning, and validating contractor bank data;
- Supporting agency and executive reporting;
- Facilitating agency refund reviews;
- Supporting security through information systems and background clearances;
- Developing monthly reports such as the Stats Tool, Program Spend Report, and Convenience Check Report;
- Maintaining Quarterly Governmentwide Metrics Dashboards to update customer agencies on individual card-program performance; and
- Providing customers with ad hoc reporting, by request.



Contract and Task Order Management

CCCM provides contract management support, which includes:

- GSA SmartPay Master Contract development, enhancement, and maintenance
- Enforce terms of the GSA SmartPay Master Contract

CCCM also provides assistance with task order management by:

- Serving as subject matter experts on the GSA SmartPay Master Contract to assist agencies/organizations in understanding products and services available
- Reviewing and assisting with the resolution of complaints between agency/organization and contractor banks
- Providing task order management for a limited number of agencies and organizations

The GSA SmartPay Purchase Program

A purchase account is a type of payment solution issued by a GSA SmartPay contractor bank and used to pay for supplies or services procured at the direction of a federal agency/organization under official purchase authority. Purchase accounts may be established through any payment solution listed in the GSA SmartPay Master Contract.

The GSA SmartPay purchase program is the preferred method of payment for federal employees to make official government purchases for supplies, goods, and services under the micro-purchase threshold.

- The GSA SmartPay purchase accounts are procurement (“open market”), ordering, and payment mechanisms for micro-purchases. When used as an ordering mechanism for micro-purchases, orders can only be placed against existing contracts if authorized in the basic contract, Basic Ordering Agreement (BOA), or Blanket Purchase Agreement (BPA). Funds must be available prior to making the purchase.



- For purchases above the micro-purchase threshold, the GSA SmartPay purchase account may only be used as an ordering and payment mechanism, but not as a procurement (“open market”) mechanism. When used as an ordering mechanism over the micro-purchase threshold, orders may only be placed against existing contracts by a Contracting Officer or authorized Ordering Officer within the limits of their authority and only if authorized in the basic contract, Basic Ordering Agreement (BOA), or Blanket Purchase Agreement (BPA). Funds certification is required prior to placing the order.

Example of an Order Placed Above the Micro-Purchase Threshold: A Contracting Officer needs to place an order with a merchant against an existing GSA Schedule contract for \$55,000. The type and amount of the purchase falls within the Contracting Officer’s warrant authority. The Contracting Officer awards the order using the ordering procedures in the Federal Acquisition Regulation (FAR) Subpart 8.4, to include any applicable agency FAR supplements and any specific terms and conditions in the contract, BOA, or BPA for the use of government purchase card accounts as an ordering mechanism. The merchant agrees to accept the GSA SmartPay purchase account as payment. When the order is delivered, the merchant bills the purchase account and provides a “paid in full” invoice directly to the agency. All applicable requirements of the Competition in Contracting Act (CICA), other statutes, and executive orders also apply to the use of purchase accounts as an ordering and payment mechanism.

Account holders can purchase any commercially available supply or service within their spending limits that is authorized by the appropriate agency official (i.e., Approving Official or other authority) for official government use and not prohibited by either federal or agency-specific procurement regulations, other statute, or policy.



Purchases that are **strictly prohibited** include:

- Long-term rental or lease of land or buildings;
- Travel or travel-related expenses for individuals or groups (does not include conference rooms, meeting spaces, and local transportation services);
- Fleet-related expenses such as fuel, oil, routine maintenance, and repair services;
- Purchases for personal use;
- Purchase not for official government use; and
- Cash advances (unless permitted by your agency/ organization).



GSA SmartPay Master Contract

The scope of the GSA SmartPay Master Contract is to provide the government with access to cutting edge payment products and services, as well as streamlined EASs that help agencies/organizations achieve their missions on a daily basis. The GSA SmartPay Master Contract provides agencies/organizations with a set of core (i.e., Tier 1) and optional value-added (i.e., Tier 2) products and services. Optional value-added products and services available to an agency/organization are determined by the Level 1 A/OPC or other appropriate agency/organization program official.

The GSA SmartPay 3 Master Contract is a fixed price, IDIQ contract. The contract period for GSA SmartPay 3 includes transitional and transactional periods of performance.

- The transitional period of performance began on the date of award of the GSA SmartPay 3 Master Contract and continues for a period not to exceed 18 months. During the transitional period of performance, agencies/organizations solicit, select, and award task orders, tag or pool with other agencies, and work with their new contractor bank to transition to the new contract.
- The transactional period of performance begins the day immediately following expiration of the GSA SmartPay 2 Master Contracts and is the period when actual transactions begin to be processed through systems belonging to/associated with contractor banks. The transactional period of performance continues for a period of 13 calendar years that is broken into a four-year base period and three three-year option periods.

Task Order Types:

Agencies/organizations award task orders under the GSA SmartPay 3 Master Contract to obtain products and services. There are four types of task orders under the GSA SmartPay 3 Master Contract:

- **Standard:** Agency solicits all contractor banks for desired Tier 1 “core” and Tier 2 “value-added” products and services as described in the contractor’s presentation package. Requests to contractor banks include a Statement of Work (SOW) and instructions for submission of a price proposal; technical proposals are not utilized. Pricing is evaluated by the agency/organization and award of a Standard Task Order initiates contractor performance.
- **Tailored:** Agency solicits all contractor banks for desired Tier 1 “core” and Tier 2 “value-added” products and services “tailored” to meet agency-specific requirements. Requests to contractor banks include a comprehensive Statement of Work (SOW) and instructions for submission of technical and price proposals. Proposals are evaluated by the agency/organization following established evaluation criteria and award of a Tailored Task Order initiates contractor performance.
- **Tag Along:** Agency joins with another agency/organization’s task order. The lead agency’s/organization’s requirements must meet the tag along’s needs.
- **Pool:** Two or more agencies/organizations collaborate to develop one set of requirements that will meet the multiple agency/organization needs. A single task order is issued and administered by a lead agency, as determined by the pool.



GSA awards and administers a GSA Pool task order under which all GSA SmartPay Master Contract products and services are available for all business lines. Agencies/organizations that are unable to tag or pool with other lead agencies may be eligible to join the GSA Pool task order after completing an application and GSA review.

GSA SmartPay Program Refunds

What is a refund? A refund is a payment made by the contractor bank to the agency/organization based on the dollar amount or spend volume during a specified time period. Refunds received under the GSA SmartPay program are the part of the interchange fee that the GSA SmartPay 3 contractor bank charges and then provides back to the agency/organization, much like corporate and personal credit card cash-back, rewards, and “points” programs. Agencies/organizations determine at what level refunds are paid and how they can be used, to include refunds against specific appropriations (see below). Refunds can and are used to directly fund and support efforts critical to agency mission delivery and support.

In the GSA SmartPay 3 Master Contract, refunds are expressed in terms of basis points (bps) or cents per transaction, depending on the Contract Line Item Number (CLIN). A basis point is 1/100th of 1 percent (expressed as .0001).

Refunds under GSA SmartPay 3 are a single rate that takes into consideration both spend volume and speed of pay. This guarantees a consistent refund within the payment-performance assumptions set forth by the agency in their task order requests for proposal.

Refunds may be deposited to the credit of the appropriation against which the initial cost was charged. If that appropriation has expired, but not yet closed, the refund may be credited to the expired account, where available. If the appropriation has expired and the expired account has been closed, the refund would be properly credited to the appropriate U.S. Treasury general fund. The exception permitting the deposit of refunds to the appropriation initially charged is permissive in nature. If an agency declines the refund, it should be deposited to the U.S. Treasury general fund.

Chapter 2: Policies



Office of Management and Budget (OMB) Circular A-123, Appendix B

OMB Circular A-123, Appendix B, provides guidance for all GSA SmartPay payment solutions. The circular:

- Consolidates into one document program requirements and guidance from OMB, GSA, U.S. Treasury, and other federal agencies;
- Establishes standard minimum requirements and best practices for improving the management of the GSA SmartPay program; and
- Provides a single source document to incorporate updates, new guidance, and/or amendments to existing guidance.

Policies from the OMB Circular A-123, Appendix B, related to the purchase program include:

- Developing and maintaining a charge card management plan;
- Providing training to all account holders and account managers (including A/OPCs, AOs, and Certifying Officials);
- Implementing risk-management controls, policies, and practices;
- Maintaining and reporting data and performance metrics;
- Managing refunds based on prompt payment, sales volume, or taking other actions by the agency for verifying accuracy and proper recording as a receipt to the agency;
- Implementing category management techniques and strategic sourcing and analyzing purchase spending data to better leverage purchasing power, reduce total costs, and improve overall performance;
- Adhering to Section 508 of the Rehabilitation Act;
- Accounting for the environmental sustainability of products and services procured with purchase accounts;
- Recovering state and local taxes levied on purchases;

- Developing and maintaining written policies and procedures for appropriate use of convenience checks;
- Issuing policies and procedures to ensure effective management of federal property acquired by a purchase card; and
- Developing and maintaining written policies and procedures for appropriate use of grants funding cards and cardless solutions, for grant-making agencies.

Federal Acquisition Regulation (FAR)

The **Federal Acquisition Regulation (FAR)** is the principal set of rules in the FAR System. This system consists of sets of regulations issued by federal agencies to govern the acquisition process. That process consists of three phases: (1) need, recognition, and acquisition planning, (2) contract formation, and (3) contract administration.





The purpose of the FAR is to provide uniform policies and procedures for acquisition. Among its guiding principles is to have an acquisition system that (1) satisfies customers' needs in terms of cost, quality, and timeliness; (2) minimizes administrative operating costs; (3) conducts business with integrity, fairness, and openness; and (4) fulfills other public policy objectives.

OMB Memorandum M-13-21 and M-17-26

OMB Memorandums M-13-21 and M-17-26 were developed to further define the requirements contained in Public Law 112-194, the Government Charge Card Abuse Prevention Act of 2012. The memorandums provide agencies/organizations with guidance and reporting requirements and frequencies. The memorandums provide guidance in the following areas:

- Requires all federal agencies to establish certain safeguards and internal controls for the government payment-solutions program;
- Establish and outline reporting requirements for business lines such as reports on purchase and integrated violations;
- Establishes penalties for violators, including dismissal when circumstances warrant (purchase transactions only); and
- Increase oversight by requiring that each agency Inspector General (IG) periodically conduct risk assessments and audits to identify fraud and improper use of the government payment solutions.

In response to the OMB memorandums, GSA developed and maintains a Charge Card Prevention Act Reporting Requirements Matrix to assist agencies/organizations with understanding required reports, frequency of the reports, and where to send the reports. This matrix can be accessed on the [GSA SmartPay website](#).

Public Laws

Below are public laws and sources for public laws related to the GSA SmartPay purchase program:

Government Charge Card Abuse Prevention Act of 2012 (Public Law 112-194)

The Government Charge Card Abuse Prevention Act of 2012 requires all federal agencies to establish certain safeguards and internal controls for government charge card programs and to establish penalties for violations, including dismissal when circumstances warrant. The law increases oversight by requiring that each agency Inspector General (IG) periodically conducts risk assessments and audits to identify fraud and improper use of government charge cards.

GSA developed and maintains a Compliance Summary Matrix to assist agencies/organizations with employing an effective charge card internal control program that is in balance with the need to maintain card flexibility and ease of use in support of agency mission activities. The matrix details the internal control requirements stated in P.L. 112-194. Agencies are not required to submit the matrix to OMB. Agencies/organizations should review these requirements and compare them to their existing internal controls in order to document the operational effectiveness of current controls and processes. Instances of non-compliance should be documented, as well as a summary of corrective actions to be taken to address shortcomings. The Compliance Summary Matrix can be located on the [GSA SmartPay website](#).

Sources of Public Law:

- [National Archives and Records Administration, Code of Federal Regulations](#)
- [Legislation information from the Library of Congress](#)

Chapter 3:

Roles and Responsibilities within the Program



Numerous individuals and offices are involved in the administration of the GSA SmartPay program. Each program participant has unique roles and responsibilities within the program.

Who are the key program participants in the GSA SmartPay program within my agency/organization?

Agency/Organization Program Coordinator (A/OPC): As an A/OPC, you are responsible for the overall management and oversight of the accounts under your span of control. Generally, your responsibilities include:

- Setting up accounts and designating authorization controls;
- Serving as a liaison between account holders and the contractor bank;



- Providing ongoing advice and assistance to account holders;
- Maintaining account information;
- Developing agency policies and procedures, as needed;
- Auditing purchase accounts as required by your agency policy;
- Using the bank's EAS to perform account management and oversight; and
- Ensure account holders are aware of their recordkeeping responsibilities.

Approving Official (AO): The individual (typically a supervisor) responsible for ensuring an account is used properly by the agency/organization. The AO authorizes account holder purchases (for official use only) and ensures that the statements are reconciled and submitted to the Designated Billing Office (DBO) in a timely manner.

Account Holder: The account holder is the individual or agency/organization component designated by an agency/organization to receive an account. The account holder is responsible for:

- Securing the account;
- Maintaining records relating to all purchase transactions-related documentation, including, but not limited to, pre-approval documentation, if and when such pre-approval is required by the cardholder's agency/organization policy; and
- Using the account ethically and appropriately.



Designated Billing Office (DBO): The DBO generally serves as the focal point for receipt of official centrally billed invoices. The DBO also serves as the liaison between the agency/organization, the A/OPC and the Centrally Billed Account (CBA) holder. The DBO oversees the proper processing of invoices and ensures invoices are paid within the Prompt Payment Act time frames. Responsibilities include:

- Reconciling invoices;
- Providing feedback to the A/OPC on contractor bank performance;
- Providing timely payment to the contractor bank;
- Providing proper interest penalties for payments that exceed Prompt Payment Act time frames; and
- Making certain that the agency/organization's task order is adequately funded.

Transaction Dispute Officer (TDO): The TDO is an individual or office that may be designated by the ordering agency/organization to assist the agency/organization and the contractor bank in tracking and resolving disputed transactions. The TDO oversees the proper processing of transaction disputes and works with the contractor bank to ensure a resolution.

EC/EDI Office (EO): The EO is the focal point for Electronic Commerce/Electronic Data Interchange (EC/EDI) for the agency/organization. This office also serves as the liaison between the A/OPC, EC/EDI systems staff, and the contractor bank. The EO oversees the proper implementation of the agency/organization EC/EDI capabilities and processes.

Who are the key program participants in the program that are outside of my agency/organization?

There are five key program participants in the GSA SmartPay program that exist outside of your agency/organization: (1) the contractor bank, (2) the brand, (3) the merchant community, (4) the Center for Charge Card Management (CCCM), and (5) the GSA SmartPay Contracting Officer.

Contractor bank major duties are:

- Paying merchants for account transactions;
- Establishing accounts;
- Issuing accounts;
- Creating and maintaining an EAS for agencies/organizations to utilize in managing the program;
- Preparing monthly statements for each account holder;
- Issuing invoices to the DBO for CBAs;
- Providing customer service 24/7;
- Preparing reports;
- Participating in an annual training forum, sponsored by GSA, that provides hands-on training on the EAS, sharing best practices and addressing any issues and concerns; and
- Complying with all other terms and conditions of the GSA SmartPay Master Contract and agency/organization task order.

Brands are financial institutions that dictate where payments can be processed and facilitate the payment process between account holders, cardholders, merchants, and issuing financial institutions (e.g., Visa and Mastercard).

Merchants are the source of the supplies and services that the account holder obtains to fulfill agency/organization's mission using the GSA SmartPay purchase account.

The GSA CCCM provides a variety of customer service functions to assist agencies/organizations with program related needs. Services include helpdesk support, program inquiries, maintaining a government-wide data warehouse, facilitating government-wide customer meetings, training and oversees the Charge Charge Management Certification Program for GSA SmartPay customers. In addition, CCCM provides technical expertise and support, housing the Contracting Officer Representative (COR) for the GSA SmartPay Master Contracts.

The **GSA Contracting Officer** administers the GSA SmartPay Master Contract on behalf of all authorized users, including your agency/organization. The GSA Contracting Officer is the only person authorized to:

- Make any changes to or add any requirements of the GSA SmartPay Master Contract;
- Legally commit or obligate the government to the expenditure of public funds for the GSA SmartPay Master Contract; and
- Render a final decision on a dispute pertaining to the GSA SmartPay Master Contract.

Is there anyone else who will be involved with the GSA SmartPay Program?

The GSA SmartPay program is a highly visible program and receives a lot of interest both within and outside your agency/organization; therefore, your agency/organization's management, the IG staff, and other investigators/auditors will likely be interested in the performance of the purchase program. Many agencies/organizations will have periodic audits of the purchase program, and you will likely be a key player in those audits. Additionally, you may find that OMB and Congress take an interest in the performance of your program. Your agency/organization management and policy office will provide you with more information on handling audits, investigations, and external inquiries.

What are my responsibilities as a Program Coordinator?

As an A/OPC for your agency/organization, you serve as the liaison between your agency/organization, the contractor bank, the account holder, CCCM, and the GSA Contracting Office.

Your role is essential to efficiently and effectively managing the purchase program.

The following list identifies specific A/OPC responsibilities. You may be required to assume some or all of the following responsibilities:

- Maintain an up-to-date list of account names, account numbers, addresses, email addresses, telephone numbers, etc., of all current account holders and accounts.
- Provide to the contractor bank any changes in your agency's organizational structure that may affect invoice/report distribution.
- Review and evaluate the contractor's technical and administrative task order performance and compliance.



- Resolve technical and operational problems between the contractor and account holders as required.
- Take appropriate action regarding delinquent accounts and report to internal investigative units and the GSA Contracting Officer any observed violations of applicable executive orders, laws, and regulations.
- Participate in the annual GSA SmartPay Training Forum and train account holders.
- Ensure account holders use their account correctly.
- Monitor account activity and manage delinquencies.
- Ensure that appropriate steps are taken to mitigate suspension or cancellation actions.
- Develop agency program procedures and policies as necessary.

- Keep the lines of communication open with all key program participants.
- Periodically remind (at least once a year) account holders under your purview of their responsibility to obtain, maintain, and retain complete documentation of all purchases in accordance with agency procedures, OMB (OMB Circular A-123, Appendix B, "Improving the Management of Government Charge Cards [as revised]"), NARA requirements, as well as the GSA SmartPay Master Contract and relevant GSA CCCM operational guidance (such as [Smart Bulletin No. 028](#), Re-emphasizing Record Keeping Requirements).

Communication is key to an effective purchase program to ensure that all program participants, including senior management/leadership, are aware of what is going on in the program. Keep in touch with your agency/organization's purchase program participants by networking, asking questions, and sharing or distributing agency/organization policy changes, program information, and/or other purchase-account information.

As an A/OPC, you should try to establish relationships with the account holders and the AOs within your span of control. The better you understand why and how the purchase account will be used, the more effective you can be in managing the program.

Chapter 4: Strategic Payment Solutions



What are some of the strategic solutions offered under GSA SmartPay 3?

Strategic payment solutions provide agencies/organizations with increased payment flexibilities. There are several strategic payment solutions offered under the [GSA SmartPay 3 Master Contract](#) including:

- **EPayables:** A solution that augments or replaces the accounts-payables process such that electronic transactions take place directly between the government and the supplier. EPayables solutions are typically used with merchants who are either:
 - Traditionally paid by convenience check or EFT or
 - Merchants who do not accept charge card payments (e.g., utility companies).

EPayables do not include virtual cards, single use accounts (SUAs), ghost accounts, or other products/services defined within the GSA SmartPay Master Contract. Types of

ePayables vary and may include an additional fee for use. Your contractor bank can provide more information on the ePayables solutions available for your program needs.

- **Mobile Applications:** The ability to access EAS, pay invoices, receive text/email alerts, and view statement and payment information over a mobile device. Your contractor bank provides mobile application capabilities, upon request, at no additional cost.
- **Mobile Payments:** The ability to make payments via mobile device at the point of sale. For example, a federal employee could pay for a purchase at a store utilizing a mobile wallet on their government-issued phone without the physical card present. Your agency/organization should develop policies and procedures regarding utilization of contractor bank mobile payment applications to ensure proper use (e.g., types of devices allowed for use, procedures for lost/stolen devices)





- **Net Billing:** The process of ensuring that merchant discounts or refunds offered are deducted at the point of sale and guaranteeing such discount arrangements. For example, the contractor bank ensures that discount information is identified on the invoice and passed to the agency/organization, when available. If a federal agency/organization purchases a toner cartridge for \$100 and the merchant offers a government discount of \$4.00 to the agency/organization based on existing agreements, the contractor bank shall net bill only \$96 for the transaction.
- **Single Use Account (SUAs):** SUA payment solutions leverage a single virtual account number for each payment. The limit on each account is set to the specific payment amount. Internal controls such as Merchant Category Code (MCC) blocks, spend limits, time frames, and account expiration dates can be used for increased control. Agencies also have the ability to append accounting data for seamless reconciliation. Examples of use include payment invoice and contract payments, which help to ensure that merchants are not able to charge more than approved amounts. Benefits of SUAs include:
 - Accounts can be activated in real time;
 - Controls can be placed on account allowing for increased oversight of spend;
 - Disposable; one-time use account numbers reduce the risk of fraud;
 - Seamless reconciliation; and
 - Reduces the necessity for using convenience checks.
- **Tokenization:** Tokenization is the use of a secure, unique token in place of a 16-digit account number to provide extra security for transactions.
- **Virtual Accounts:** Virtual accounts provide a one-time-use account number that may be used for a limited amount, certain time frame, and/or for a specific vendor. There are multiple types of and uses for virtual accounts that often do not involve the issuance of a plastic charge card. Ghost cards and SUAs are two examples of this type of account. A virtual account can be used for single or multiple transactions, depending on how it is set up. These accounts offer a solution to various business challenges, such as:
 - Large-ticket transactions;
 - Payment to vendors who do not typically accept card-based payments;
 - One-time supplier payments; and
 - Recurring transactions with a specific vendor.
- **Declining Balance Solutions:** Declining balance solutions can be applied for a specific purpose, with a finite balance, for a specified time period. Credit limits can either be reset as needed or the card becomes inactive once the balance is used. These accounts can be easily loaded and distributed to employees in case of emergency or disaster situations. Benefits may include:
 - Financial flexibility and security;
 - Reduction of agency/organization administrative fees;
 - A flexible option for applicants who cannot be issued a traditional account; and
 - Safe and excellent alternative to cash and paper checks.

Chapter 4 (continued)

- **Ghost Accounts:** Ghost accounts are for agencies/ organizations that frequently do business with one vendor and have recurring payments. An account number can be assigned to the vendor and authorized agency-personnel transactions occur without having to use multiple cards or accounts. Many agencies use this product for purchases such as airline tickets. Benefits may include:
 - Reduced number of open accounts (making payment processing and oversight easier);
 - Allows for multiple users;
 - Allows for a high level of control; and
 - Reduces the risk of lost or stolen cards.

What are Convenience Checks?

Some agencies allow the use of convenience checks, which are a contractor provided instrument that is written, dated, and signed against an account within established dollar limits. Convenience checks are intended only for the use with merchants who do not accept the GSA SmartPay purchase account. Convenience checks should be used as a payment method of last resort, only when no reasonable alternative merchant who accepts the GSA SmartPay purchase account is available.

If your agency/organization determines a need for convenience checks, your contractor bank will provide a supply of checks to the designated account holder drawn on the account holder's purchase account. The checks will be processed as they are presented for payment.

Convenience checks are multi-copied (one copy for the account holder's records; the original for the merchant). Because of the increased potential of fraud and abuse, specialized training on convenience checks is required prior to being authorized to write checks. If any misuse or



abuse is discovered, your agency will revoke the employee's convenience check and purchase account privileges. That employee will then be referred for disciplinary action in accordance with agency procedure.

Convenience checks may **not** be written for purchases above the maximum dollar limit established by your agency/organization. In addition, convenience checks may not be written to:

- Vendors who accept the GSA SmartPay purchase account;
- Vendor transactions already under another method of acquisition (e.g., purchase orders, contracts, etc.);
- Employee reimbursements;
- Cash advances;
- Salary payments, cash awards, or any transaction processed through the payroll system;
- Travel-related transportation tickets;
- Meals or lodging related to employee travel except as related to emergency incident response; and
- Other restrictions as determined by agency policy.



Checks must be used in sequential order. Each convenience check must be entered into a check register or log for tracking purposes. The following information must be written on each check:

- Date the check is being issued;
- The name of the payee;
- Amount of the check; and
- An original signature.

As an A/OPC, you are responsible for the implementation of the appropriate internal controls and oversight of convenience check activity, including ensuring that all checks issued are for official government business only and are stored in a secured location. You must verify that each check issued was both necessary and in compliance with the agency's convenience check policy.

The Internal Revenue Service (IRS) requires that information be collected for reporting income to the IRS when a convenience check is used for purchases of services. If a person is "engaged in a trade or business and, in the course of that trade or business, pays any person an aggregated \$600 or more of rent, salaries, wages, premiums, annuities, compensations, remunerations, emoluments, or other fixed or determinable gains, profits and income during a calendar year, IRS Code Section 6041 generally requires them to file an information return with the IRS and to furnish an information statement to the payee."

The IRS states that agencies may rely on the MCC in determining whether a transaction is subject to Form 1099 reporting. Failure to file a correct information return (Form 1099) by the due date may result in a penalty imposed by the IRS.

Why should I work toward eliminating convenience checks?

Convenience checks are actually not as convenient as one may think. They provide thieves with an easy way to commit fraud, and they don't offer the same kinds of consumer protections as other GSA SmartPay solutions. Convenience checks have:

- **Less refund opportunities for agencies:** Convenience checks don't offer federal agencies refunds; you are assessed a fee for each check. As a result, using convenience checks decreases the refund your agency will receive through the GSA SmartPay program.
- **Greater fraud risk:** Convenience checks often don't require signature verification, which could lead to fraudulent transactions. In addition, they don't carry the same "paper trail" as other electronic payment methods, which may lead to misuse.
- **Less streamlined processes:** Electronic payments, like charge cards, help facilitate smoother transactions, enhance transparency, save time, and lead to improved data-monitoring capabilities.
- **No support for green initiatives:** Electronic payments help reduce paper usage and aid agencies in meeting their sustainability goals. Records also reside in a central location, which will make it easier to locate and verify information.
- **Decreased consumer protection:** Other solutions provide the opportunity for a much quicker reimbursement to a customer who may be unsatisfied with a product or service or who is charged incorrectly.



- **More hassle:** Convenience check transactions must be reported to the IRS using a 1099 form. Alternatively, in accordance with Section 6050W of the Housing Assistance Tax Act (Public Law 110-289), agencies are no longer required to report other GSA SmartPay payment solution transactions to the IRS using the 1099 form. Utilizing another option instead of a convenience check delivers tremendous time and cost savings, leaving more time for mission-critical activities.
- **Weakened merchant-client relationship:** When an alternative is used, merchants are paid within three days of the transaction. They receive a guaranteed payment and as a result, are able to provide greater security, reports, and data to the customer. This increases satisfaction on both sides of the transaction.
- **Potential to adversely affect mission:** There are many examples of agencies decreasing convenience check usage and still being able to successfully meet their mission.
- **More restrictions:** Convenience checks have several restrictions, including those on purchases above the micro-purchase threshold and vendor transactions already under another method of acquisition, thereby making other payment methods more preferable.

Before a check is issued, every reasonable effort should be made to use another payment option. Maximum efforts should be made to find and use vendors who accept other GSA SmartPay solutions. Because of the cost associated with convenience checks, the number of checks written should be kept to a minimum.

Before writing a convenience check, ask yourself these questions:

- **Does this vendor accept the GSA SmartPay purchase charge cards?**
 - If yes, please use one. If no, determine what other payment options are available.
- **Are there other vendors who accept charge cards and offer the same product or service?**
 - Conduct a price analysis among various vendors. Review a vendor's performance history.
- **Is a similar product a possibility?**
 - Which features are mandatory, and which can be substituted?
 - What specific requirements must be met?
- **What other avenues for purchasing can be considered?**
 - What alternative methods has your agency used in the past?
 - How did those purchases turn out?
- **What are your bank's preferred methods?**
 - Which options provide the banks with the best opportunity to record data, pay merchants faster, and provide the best service to you?
- **Which options lead to the best recording and tracking?**

Chapter 5: Misuse/Abuse/Fraud



How can you minimize the risk of misuse or fraud in your GSA SmartPay purchase program?

The most important thing you can do is to be aware of what activity is occurring on the accounts under your purview. Do not be afraid to ask account holders questions if you identify unusual or suspicious transactions or behavior.

GSA SmartPay purchase account misuse/abuse can take many different forms. Here are some of the most-common examples:

- **Purchases exceed the account holder's authorized limit:** Account holders may be limited to a specific spending limit per transaction, per day, and/or per monthly billing cycle.
 - **Purchases for which no funding is available:** Federal law requires that funds must be available before any government purchase is made. It is up to the account holder to ensure that the funds are available prior to making any transaction. Funds must be certified available for transactions over the micro-purchase threshold.
 - **The account holder allows other people to use their purchase account:** Account holders must take steps to ensure the security of their account. This means the purchase account must be used only by the account holder and only for official government business. If the account holder allows others to use the purchase account, the account holder will be held personally liable to the government for any unauthorized transactions.
 - **Split transactions:** The FAR limits the dollar threshold for micro-purchases. Any purchase that, as a whole, would exceed the micro-purchase limit, but is separated into smaller transactions in order to avoid the micro-purchase limit, is considered to be a split transaction.
- 
- **Products or services that do not meet the government's requirements:** Account holders must use discretion when making purchases to ensure that they meet the government's requirements. Because of the wide array of products and services available, there may be occasions when account holders may be requested or tempted to buy luxury or deluxe versions of products and services that exceed the government's actual requirements. For instance, it would be questionable for an account holder to buy a \$500 designer fountain pen when there are many quality fountain pens available for \$50 or less.
 - **Purchases for personal consumption:** All purchases must be for official government use only. Thus, any purchase made that is for the account holder's personal use rather than for official government purposes is considered to be misuse. For example, an account holder who uses the purchase account to buy lunch because they have no cash available on that day is misusing the purchase account.
 - **Purchases that are not authorized by the agency/organization:** Your agency/organization may have additional limits on the use of the purchase account, such as limiting certain categories or types of products or services.

Examples of Account Holder Misuse and Abuse:

Case #1: An account holder conspired with a local business owner to make purchases not authorized by the account holder's agency. The merchant circumvented the authorization process to allow the account holder to make purchases for their personal consumption. The AO approved the transactions.

Case #2: An account holder conspired with a company to make unauthorized purchases. No receipts were found to support the purchase and the amount of purchases from this company exceeded the normal expenditures of other account holders. The goods or services purchased were never delivered to the government.

Case #3: A business owner approached an account holder and offered to provide kickbacks to the account holder if the account holder made supply purchases from the owner's business. The account holder was authorized to make purchases of these supplies, and the supplies were delivered. The company provided false receipts for the supplies. The account holder repeatedly made transactions with this company. The company paid the account holder a percentage of sales.

Case #4: An account holder obtained goods and services for personal use. The ship-to address was the employee's home. A third party did not confirm receipt of the materials. The account holder advised the merchant to split transactions to ensure they would not exceed the account holder's single-purchase limit.

Case #5: An account holder made an unauthorized purchase. When questioned, the account holder requested a credit from the merchant. The merchant issued a credit but later re-billed the account. The account holder was hoping that the transaction would pass review at a later date.

Case #6: An account holder established front companies to receive payment for merchandise never received. The account holder then conspired with either other contractors or other employees to utilize business to obtain larger profit margins and to show some legitimate business was being conducted.

Consequences

Consequences for misuse/abuse may include:

- Reprimand;
- Purchase account cancellation;
- Counseling;
- Suspension of employment;
- Termination of employment; and
- Criminal prosecution.

Your agency may have agency-specific penalties and consequences for misuse/abuse of the purchase account.

What is fraud?

Fraud is a deception deliberately practiced with the motive of securing unfair or unlawful gain. Fraud can be an attempt to cheat the federal government and corrupt its agents by using GSA SmartPay payment solutions for transactions not part of official government business. Like any deception, fraud has its fair share of victims.

Some of the different types of fraud include:

- **Counterfeit Accounts:** 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 Accounts:** Often physical 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 card verification code (CVC), which is 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 new or replacement cards are mailed and then stolen while in transit.
- **Identity Theft Fraud:** Whenever a criminal applies for an account using another person's identity and information.

As a program coordinator, you must inform your account holders to:

- Be alert to the indicators of fraud (including false charges/ transactions, mischarging, bribes, gratuities, and kickbacks); and
- Report suspected fraud immediately through the proper channels at your agency (AO, A/OPC, Financial Officer, Office of the Inspector General, or Office of Special Investigations).

Any intentional use of the GSA SmartPay purchase account for other than official government business is considered an attempt to commit fraud against the U.S. government and may be cause for disciplinary actions. The account holder is held personally liable to the government for the amount of any non-government transaction. Under 18 U.S.C. 287, misuse of the purchase account could result in fines or imprisonment or both. Military members who misuse the purchase account may be subject to court martial under 10 U.S.C. 932, UCMJ Art. 132.

What happens if a GSA SmartPay purchase account is lost or stolen?

Instruct your account holders to report a lost or stolen purchase account promptly to:

1. The contractor bank;
2. You, the program coordinator (A/OPC); and
3. Their supervisor.

Once an account has been reported as lost or stolen, the contractor bank immediately will block that account from further usage, and a new account number will be issued to the account holder.

Reporting the account as stolen does not relieve the account holder or the government of payment for any transactions that were made by the account holder prior to reporting it stolen. If the account holder does not recognize a transaction appearing on their statement, they are responsible for notifying the contractor bank within 90 calendar days from the transaction date to initiate a dispute, unless otherwise specified by the agency/organization. This notification of transaction dispute may occur via the EAS, telephone, or other electronic means (e.g., email).



The account holder relinquishes their right to recover a disputed amount after 90 calendar days from the date of the transaction. It is their responsibility to dispute questionable charges. If they don't, they will be held personally liable for the amount of the questionable charge.

There are various reasons other than fraud for disputing transactions, including:

- Unauthorized or incorrect charges;
- Charges for merchandise that has not been received;
- Charges for returned merchandise; and
- Statement does not include credits for which the account holder has been issued.

In most cases, the account holder should contact the merchant directly to resolve any disputed charges and request a credit from the merchant. Sales tax and shipping charges are not disputable items and must be resolved between the account holder and the merchant.

The A/OPC should monitor disputes filed by account holders. Merchants with a high number of disputes should be watched to determine whether they are acting improperly.

What should I do if I suspect misuse or fraud?

A key responsibility for most program coordinators is to detect and report suspected misuse. If a situation occurs where you must report suspected misuse, make sure you have all the information necessary to assist with a formal inquiry or investigation. Contact the account holder to obtain any information that could explain questionable charges. If the account holder provides documentation or an explanation regarding the charges and you still have questions or

concerns about it, compile all the information (e.g., statement, exception report, documented contacts between you and the account holder, copies of receipts, etc.) before you report it. Your agency/organization may ask you to report suspected misuse to one or more of the following personnel:

- The AO
- The Finance Officer
- The Office of Inspector General (via the hotline) or the Office of Special Investigations (for Defense agencies)

Always follow your agency's policies and procedures when handling cases of suspected misuse.

When reviewing transactions, please keep in mind:

- Cases of misuse/fraud often start small and may not stop after only one action. No matter how small the misuse/fraud, it should be addressed immediately to prevent any future occurrences.
- Accounts must only be used by the account holder. If the account holder is not directly involved in the transaction, there is greater risk that fraud will occur.
- Account holders should be able to provide documentation of purchases (such as invoices or receipts) when requested by the AO, A/OPC, or auditors.
- Ensure that account holders certify transactions promptly. Prompt certification allows for prompt remedial action in the event of misuse/fraud.
- Random reviews of account holder records by the A/OPC will discourage misuse and fraud, because account holders and AOs know their actions are being monitored.
- Government investigators indicate that, in many instances, the AO and/or A/OPC would have detected fraud earlier with proper review.



Appendix 2: Account Holder Fraud Checklist provides a downloadable Microsoft® Excel® checklist that highlights indicators that may point to account-holder fraud. Indicators do not necessarily mean that fraud has occurred, but that the situation must be investigated further with the account holder or other individuals involved.

The GSA SmartPay purchase card program includes many tools to assist you in the proper management of your agencies purchase card program. Program management tools include:



1. **Credit limits:** Credit limits restrict single, daily, weekly, or monthly expenditures by the account holder. In accordance with agency/organization policy, an A/OPC may set the limits that best meet the agency's needs. Setting limits that are realistic, but not excessive, will deter account holder misuse. By reviewing account holder spending patterns, you may be able to lower limits without disrupting the agency's mission. A/OPCs also have the authority to raise limits at any time in response to emergency or unforeseen situations.
2. **Merchant Category Code (MCC) Blocks:** MCCs are established by the associations or contractor banks to identify different types of businesses. Merchants select the codes best describing their business. You may limit the types of businesses where the account will be accepted by limiting the MCCs available to the account holder. The contractor bank has established sample templates that may assist you in determining which MCCs should be restricted. In the event that an account holder needs to make a purchase outside of their restricted MCCs, the A/OPC is authorized to override the restriction for a transaction by contacting the contractor bank's customer-service representative. Agency/organization policy should specify who is authorized to perform overrides.
3. **Online Reports:** A/OPCs have access to many standard and ad hoc reports online through the contractor bank's EAS.
4. **Account Deactivation:** In those instances when the purchase account is not needed on a continuous basis, deactivation of the account may serve as a deterrent to fraud and/or misuse. You may deactivate the account when an account holder is not using or is not planning to use the purchase account. By understanding the account holder's need and use of the account, you can work with the account holder to establish deactivation guidelines. Deactivation and reactivation can be completed through the bank's EAS or by calling the contractor bank's customer-service phone number.
5. **Guides:** The contractor banks have developed written guides for A/OPCs and account holders, as follows:
 - o **A/OPC Guide:** This guide addresses issues of concern to the A/OPC, including responsibilities of program participants, account setup and maintenance, account suspension/cancellation, disputes, reports, and invoicing procedures. The guide is available from the banks in hard copy and/or electronically.
 - o **Account Holder Guide:** This guide addresses authorized uses of the purchase account, disputes, and billing.

6. **Fraud Analytics Tools:** The GSA SmartPay contractor banks provide, internally or via the associations (i.e., brands), fraud analytic capabilities/tools that use real-time data and random data signatures that are tracked within all data repositories to monitor data packets. If an unauthorized packet is detected, it will trigger an auto-severing program to prevent data breach. These tools also analyze transactions and test each transaction against specific rules established by agencies/organizations. The system identifies and reports all non-compliant transactions. At an aggregate level, an analysis of all completed transactions against all new transactions can be made to detect patterns of potential fraud and then flag non-compliant transactions when potential fraud is detected.
7. **Case Management Tools:** The GSA SmartPay contractor banks provide, internally or via the associations (i.e., brands), case management capabilities/tools integrated with the contractor bank's EAS that enables high-volume automated processing of cases leveraging data mining, fraud analytics, and risk determination. Data is seamlessly integrated from the contractor bank's data mining and fraud analytics solutions, including, but not limited to, the following data requirements: transaction date, account holder, merchant name and location, MCC, transaction amount, account number, and transaction type. Automated notifications to account holders can be triggered through a variety of platforms (e.g., email, phone, text) as determined by the agency/organization.

Best Practice: MCCs are often used to highlight transactions requiring further investigation. While a transaction with a merchant in a questionable MCC may initially raise questions, further investigation may reveal that the transaction was a legitimate purchase or that the merchant was misclassified (you can view a full listing of MCCs in Appendix 1: Merchant Category Codes).

How do these tools make it easier to audit and manage the use of purchase accounts?

By providing electronic reports and transaction files, auditors and agency/organization program managers have immediate access to information such as merchant name, type of merchant, dollar amount of transaction, and date of transaction. These tools make it easier to identify questionable transactions and follow through to ensure that the transactions were proper. In some instances, merchants also provide line-item detail of transactions, including quantities, prices, and product descriptions. GSA continues to work with the associations to increase availability of line-item detail.

What tools does GSA provide to assist agencies/ organizations with preventative measures/ program management for the purchase program?

- GSA hosts an online training course for account holders and A/OPCs that discusses the proper use of purchase account
- The annual GSA SmartPay Training Forum for A/OPCs provides training on the bank's EAS, best practices, and program management.
- Free online resources from the GSA SmartPay website to assist purchase A/OPCs in detecting and preventing misuse and fraud.
- Helpful Hints for Purchase Account Use, one of our printable resources, is a card-sized brochure that provides information on the purchase account. This brochure can be ordered online (free of charge!) and can be passed out to account holders when they receive their purchase accounts.
- Sample log and pre-approval and approval templates can be found on the GSA SmartPay website under Resources For Approving Officials/Tools .

Chapter 6: Liability



What is a Centrally Billed Account, and why is it important to know?

All purchase accounts are considered Centrally Billed Accounts (CBAs), because the agency directly receives the invoices and pays the contractor bank. The distinction is important when determining state tax exemption. **All GSA SmartPay CBAs should be exempt from state taxes. This includes all cards under the purchase card program.**

With a CBA, the federal government accepts liability for charges made by an authorized account holder, but is not liable for any unauthorized use. Unauthorized use means the use of an account by a person other than the account holder who does not have actual, implied, or apparent authority for such use and from which the account holder receives no benefit.

When the CBA has been used by an authorized account holder to make an unauthorized purchase, the government is liable for the charge and the agency is responsible for taking appropriate action against the account holder.

The agency/organization is not liable for any unauthorized use, including unauthorized transactions on lost or stolen accounts. If it is discovered that someone other than the account holder has used the account, it should be reported immediately to the A/OPC and the contractor bank. The contractor bank will then issue the account holder a new account number. Unauthorized transactions may appear on the account holder statement, even though the account has been reported lost or stolen. If unauthorized transactions appear on a billing statement, the account holder should contact the bank's customer service department immediately.



Chapter 7: The Review Process



Given that the agency is liable for unauthorized purchases by an authorized account holder, agency purchase account policy should address reviews to be undertaken by the AO and A/OPC to mitigate risk to the agency. Top-level A/OPC and AO review, including first-hand knowledge of the type of products and services authorized by the organization, is the first line of defense.

Responsibilities During the Review Process

Account Holder

At the end of each billing cycle, the account holder should reconcile the transactions appearing on their monthly statement by verifying their accuracy against account holder records. The account holder should review all information on the monthly statement, verifying charges, credits, outstanding disputes, and refunds.

Best Practice: Account holders should use a standardized form to provide additional information to A/OPCs on questionable transactions (Appendix 3-4: Sample Questionable Purchases Form).

Approving Official (AO)

The AO, typically a supervisor, is responsible for ensuring that all purchases made by the account holder are authorized, allowable, and accurate. In addition to authorizing purchases, the AO must:

- Ensure that the statements are reconciled and submitted to the DBO in a timely manner;
- Sign account statements on a monthly basis (e.g., CBA);
- Certify the monthly invoices resulting from account holder transactions;

- Conduct informal compliance reviews;
- Resolve all questionable purchases with the account holder; and
- Notify the account holder, A/OPC, and other appropriate personnel in accordance with agency policy if an unauthorized purchase is detected.

The contractor bank's EAS allows AOs to review an account holder's transactions online. In addition, account holders can maintain electronic purchase logs through the EAS. There are many other functions of the EAS that are beneficial for AOs, including electronic reconciliation and certification, editing account allocation, multi-account allocation and assignment of account codes.

As with all roles, one must know what is expected of them to be successful, and training for an AO is no exception. Before becoming an AO, it is important to take the online training for GSA SmartPay purchase account holders and remain familiar with the rules and regulations governing the use of a purchase program, including specific agency policy. AOs must also take refresher training at least once every three years and should familiarize themselves with their agency's approval and tracking systems.

Best Practice: The number of account holders and the volume of transactions for which an AO is responsible needs to be reasonable, considering the volume of account holder activity and the organizational structure. This will allow reviews to be conducted in a timely manner and ensure detection of possible cases of misuse and fraud. The AO should have direct knowledge of the account holder's role in the agency and the ability to verify receipt of the purchase. AOs should also keep a log to track pre-approval and/or approval requests and responses to aid in their recording keeping. This will assist in the annual review process.



Agency/Organization Program Coordinator (A/OPC)

The A/OPC must ensure that adequate internal controls are in place. The annual review should consist of an evaluation of local operating procedures to check that account holders and AOs are operating within the prescribed policies and maintaining complete records of the transaction process, including pre-approval/approval documentation.

A review should encompass the following areas:

- Compliance with agency policies;
- Applicable training requirements;
- Appropriate delegation of authority;
- Integrity of the purchase process;
- Compliance with procurement regulations;
- Receipt and acceptance procedures; and
- Records retention and completeness.

Agency policy may require an annual review by each A/OPC. Depending on the number of accounts, the annual review may be performed on each account or at random. See Appendix 3 for sample annual review process information.

Appendix 3: Sample Annual Review Process

- Appendix 3-1: Sample Annual Review Checklist
- Appendix 3-2: Sample Summary of Findings
- Appendix 3-3: Sample Certification of Completion of the Annual Review
- Appendix 3-4: Sample Questionable Purchases Form

Who Should Be Given Accounts?

There is no correct number of account holders for your agency. In certain circumstances, a large number of account holders may be required to accomplish the agency's mission. The risk of issuing more accounts must be weighed against the need for more account holders.

Best Practice: A/OPCs are encouraged to review account activity and the number of account holders as part of their annual review process. Accounts with little or no activity should be closed if they are no longer needed. It is also recommended that the A/OPC completes the annual review around the same time each year.

Separation of Duties

Agency policy should include direction regarding separation of duties to minimize the risk of fraud and/or loss of property. Responsibilities of account holders, AOs, and A/OPCs should not overlap, to ensure that management controls are not circumvented. Assignment of duties (such as authorizing, approving, and recording transactions), receiving assets, approving account-holder statements, making payments, certifying funding, and reviewing/auditing should be assigned to separate individuals to the greatest extent possible.

Best Practice: When appointing A/OPCs or AOs, consider factors such as grade, position, experience, and training to ensure they can successfully perform their responsibilities.

Chapter 8: Electronic Access System (EAS)/Reporting



The GSA SmartPay contractor banks all provide an Electronic Access System (EAS), which provides account access and a variety of reports for A/OPCs to assist in the effective management of the program. An A/OPC can use the contractor bank's EAS in order to implement, manage, receive, and complete all reporting requirements. The EAS will allow the A/OPC to view statements, send in program forms, set up accounts, maintain accounts, activate/deactivate accounts, update authorizations, and download reports.

Agency reports can be generated as a means of detecting misuse/fraud. There are several essential reports that can provide transaction data with different levels of detail. Each report can be made available at every level of the hierarchy.

Each bank has a slightly different suite of reports available, so review the contractor bank's A/OPC Guide or view information online to learn about the specific reports offered. Most electronic reports are updated within two to three days after a transaction. However, some reports are only updated at the end of the billing cycle.

The following reports may be utilized to detect misuse and fraud within your program:

The **Account Activity Report** consists of summary totals for the reporting period and the fiscal year to date, categorized by account and agency/organization. This report is used by the A/OPCs to obtain and manipulate program data. It includes:

- Complete account activity, both active and inactive;
- An agency/organization hierarchy roll-up section;
- Current and past fiscal year account activity;

- Segregated charges and credits by individual or agency/organization accounts with current period totals of the data elements identified; and
- Merchant information, such as name, address, and MCC (as applicable).

The Account Activity Report can be useful for identifying:

- Suspicious merchants;
- Unusually high spending patterns;
- Excessive convenience-check usage; and/or
- Untimely purchases.

The **Declined Transaction Report** includes a list of declined transactions and the reasons for the declines. It will identify account holders who have attempted to use an account to buy an item:

- For which they are not authorized;
- That exceeds their single purchase limit;
- That exceeds their monthly purchase limit; or
- From a merchant that falls under a blocked MCC.





Best Practice: If an account holder consistently has declined transactions, the A/OPC should take action by providing additional training or making a change to the authorization controls or dollar limits.

The **Transaction Dispute Report** lists all outstanding and resolved transaction disputes and includes all information necessary to identify, track, balance, and obtain status on the dispute from the original charge through resolution. This report shall include all attributes of the original charge. Reviewing the report would identify account holders with excessive disputes. The account holders identified in this report either may require training or may be trying to disguise misuse or fraudulent activity. AOs and A/OPCs should track and follow up on disputes to determine their outcomes. Account holders should attempt to resolve disputes directly with merchants prior to filing a disputes report.

Best Practice: If a merchant is consistently appearing on the disputes report, the A/OPC should investigate to determine whether the merchant may have billing issues, have quality issues, or is attempting to commit fraud by submitting false transactions.

The **Fraud Analytics Report** is a series of reports that identifies lost, stolen, invalid, or canceled accounts, declined transactions and unusual spending activity, and details such as unusual transaction activity. It includes current and past-due balances.

The **Master File Report** contains master-file information on all accounts (e.g., account number, account-holder information, account expiration date, etc.). The Master File Report should be reviewed periodically to eliminate account holders who are no longer employed in the agency, correct addresses, and verify whether account limits and authorization controls are appropriate.

Ad Hoc Reports provide the ability for GSA and the agency/organization community to access all data elements of the AO, account holder, and transaction records at any time by allowing GSA and/or agencies/organizations to create reports in HTML, Excel, text (ASCII) formats, and/or others, as defined by the agency/organization at the task order level. The contractor bank provides the capability for GSA to utilize the ad hoc reporting functionality of the EASs for any additional future reporting needs that are not listed.

Best Practice: After building an ad hoc report, share the report with other A/OPCs at your agency. This saves other A/OPCs time from recreating similar reports and ensures consistency across the organization.

What are my responsibilities for printing and storing reports?

You should save copies of all electronic reports you generate, particularly statistical or summary reports. Because of the volume of information available, the bank will furnish information for a limited period of time (generally 18 months or less) before archiving the data. Reports containing sensitive information (e.g., account numbers, account holder information, etc.) should be maintained in a secure location. Review and follow your agency/organization's policy for instructions on printing and safeguarding reports.

Chapter 9: Preventative Measures



Some program management tools for preventing fraud/misuse and abuse within your program include:

- Credit limits
- MCC blocks
- Online reports
- Account deactivation



Credit Limits

Credit limits can be set up to restrict single-purchase or daily/weekly/monthly expenditures by the account holder. In accordance with agency policy, an A/OPC sets credit limits that best meet the agency's needs. Setting limits that are realistic but not excessive will deter account holder misuse. By reviewing account holder spending patterns, you may be able to lower limits without jeopardizing the employee's mission. A/OPCs have the authority to raise limits at any time in response to emergency or unforeseen situations.

Best Practice: Only allow top-level (Level 1 A/OPCs) to raise limits according to agency policy.

Merchant Category Code (MCC) Blocks

MCCs are established by the banks or associations to identify different types of businesses. Merchants work with their acquiring banks to select the codes best describing their businesses. An A/OPC may limit the types of businesses where the card will be accepted by limiting the MCCs available to the account holder. Your contractor bank has already established sample templates that may assist in determining which MCCs should be restricted. In the event that an account holder needs to make a purchase outside of their restricted MCCs, an A/OPC is authorized to override the restriction for a transaction by contacting the bank's customer service representative. Agency policy should specify who is authorized to perform overrides.

Appendix 1: Merchant Category Codes

Agency Policy

Agency policy will vary among agencies, based on mission considerations. It is recommended that agency policies address the following areas and clear guidance is provided to A/OPCs, AOs, and account holders:

- Delegation of contracting authority;
- Training requirements;
- Account limits;
- Uses of the account;
- Receipt and acceptance of supplies and services;
- Reconciling accounts;
- Review procedures;
- Span of control for AOs and A/OPCs;
- Criteria for establishing accounts;
- Criteria for deactivating or cancelling accounts with minimal activity; and
- Pre-approval procedures, if required.



Defining the A/OPC Role

To ensure that everyone understands their role, include a list of A/OPC duties and responsibilities in your agency's written policy and A/OPC training materials. This is particularly important in situations where there is frequent turnover of A/OPCs.

Training for A/OPCs is available through:

- **GSA SmartPay online training (available 24/7)**
- In-person training provided by your contractor bank (schedule an appointment with the bank's account manager assigned to your agency)
- GSA SmartPay in-person and virtual training forums

The role of the A/OPC is extremely important to the agency, because they are the eyes and ears of the organization.

Audits and Investigations

The Inspector General Act of 1978 established the Office of Inspector General in departments and agencies to:

- Conduct audits and investigations related to programs and operations;
- Provide leadership;
- Recommend policies that detect and prevent fraud and abuse in programs and operations; and
- Provide a means for informing the head of the department or agency of problems or deficiencies.

Because the GSA SmartPay program is a highly visible program and receives a lot of interest both within and outside your agency/organization, your agency/organization's management, the IG staff, and other investigators/auditors will likely be interested in the performance of the purchase program. Many agencies/organizations will have periodic

audits of the purchase program, and you will likely be a key player in those audits. Additionally, you may find that OMB and Congress take an interest in the performance of your program. Your agency/organization management and policy office will provide you with more information on handling audits, investigations, and external inquiries.

Best Practice: Establishing a good relationship between the GSA SmartPay Program office and the IG's office is the key to successful management of your program.

The two types of functions generally performed by the IG are audits and investigations.

- Audits are performed to ensure compliance with policy and to detect fraud and misuse. They are general in nature and not focused on specific actions or individuals. Audits may review internal or external operations.
- Investigations are more specific in nature, although they may look at several areas or individuals inside and outside the organization. The agency's program management office should work with the IG to gather data on completed investigations, so that preventive measures can be addressed in agency purchasing policy.

The GSA SmartPay Audit Repository can be found on the GSA SmartPay website at <https://smartpay.gsa.gov/content/resources#sa836>.

Joint Agency Coordination

Joint agency coordination is important because fraud and abuse found through investigations in one agency could uncover and prevent similar situations occurring in another agency. The types of criminal acts involved in purchase fraud are often conducted in rings. Further, in the case of contractor involvement, the contractor normally does business with multiple federal agencies and usually continues similar behavioral patterns with other government employees.

An example of joint agency coordination is the Joint Federal Task Force “Sudden Impact,” assembled by the Federal Bureau of Investigations (FBI). This task force was composed of multiple federal agencies, ranging from the U.S. Army Criminal Investigation Command to the Defense Criminal Investigation Service to the Environmental Protection Agency. This task force met on a regular basis, not only to discuss new purchase account investigations, but also to conduct proactive analyses of purchase account activity. The FBI provided space with computers in order to download and compile purchase account activity for task force review. The task force received prosecutorial assistance from attorneys within the Justice Department and the Department of Defense.



Training Materials

Training is a key component of fraud prevention. GSA offers numerous training opportunities to assist A/OPCs in the administration of the purchase program; however, some agencies may require supplemental training to address agency-specific issues.

Managing Your GSA SmartPay Purchase and Travel Program FlipBooks – These interactive guides give program coordinators an overview of the GSA SmartPay program, addressing issues of concern to the A/OPC, including responsibilities of program participants, account setup and maintenance, account suspension/cancellation, disputes, reports, and invoicing procedures.

A/OPC Online Training – GSA SmartPay offers free online training (24/7) to purchase and travel A/OPCs and account holders. Online training can be found on the GSA SmartPay training website: <https://training.smartpay.gsa.gov>.



Annual GSA SmartPay Training Forum – GSA sponsors an annual forum, either physically or virtually, to train A/OPCs on account administration, program management, reports, and EASs. In addition to A/OPCs, the forum is beneficial for approving and billing officials, inspectors and auditors. Information regarding the next forum may be found at <https://smartpay.gsa.gov>.

Onsite Training – As requested by agencies/organizations, your bank provides on-site training at an agency/organization specified location to groups of 20 or more A/OPCs, Designated Billing Office and Transaction Disputes Office points of contact, or any combination thereof. Agencies/organizations may group together to form a group of 20 or more for on-site training. All contractor travel and site related costs associated with on-site training shall be borne by the contractor. In some instances, GSA may provide a site to host this type of training. Contact your account manager at your contractor bank to set up an on-site training session.

Account Holder Guide – The account holder guide can be requested through your contractor bank and addresses authorized uses of the account, disputes, and billing.

Deactivation

As a preventative measure, an A/OPC can deactivate an account in those instances when the purchase account is not needed on a continuous basis. This action may serve as a deterrent to fraud and/or misuse. By understanding the account holder's needs, you can work with the account holder to establish deactivation guidelines that allow you to activate and deactivate the account to meet those needs. Deactivation and reactivation can be completed through the bank's EAS or by calling the bank's customer-service phone number.

Automated Transaction Review

Contractor banks can provide transaction files in an electronic format to agencies. With receipt of electronic transaction data, an agency has the option of reviewing account holder activity through data mining. Data mining is the extraction of useful information from a database using artificial intelligence algorithms and neural networks. Several agencies have developed data-mining tools to highlight potential misuse and fraud. The accuracy of the tools is contingent on models that depict fraud occurrences. In order to develop accurate models, the patterns of account holder misuse and fraud must be documented and understood.

What tools does GSA provide to assist agencies/organizations with preventative measures/program management for the purchase program?

- GSA hosts an online training course for account holders that discusses the proper use of purchase accounts.
- The annual GSA SmartPay Training Forum for A/OPCs provides training on the bank's EAS, best practices, and program management.
- Free online resources from the GSA SmartPay website to assist purchase A/OPCs in detecting and preventing misuse and fraud.
- Helpful Hints for Purchase Account Use, one of GSA's printable resources, is a card-sized brochure that provides information on the purchase account. This brochure can be ordered online (free of charge!) and can be passed out to account holders when they receive their purchase accounts.
- Sample log and pre-approval and approval templates can be found on the GSA SmartPay website under Resources/For Approving Officials/Tools.

Chapter 9 (continued)



Reporting Suspected or Actual Fraud

The A/OPC has the responsibility to report any suspected or actual fraud to the appropriate authorities within the federal government.

If fraud by an account holder, merchant, or other third party is suspected, an A/OPC can file a complaint with their agency's IG. Investigations are initiated upon receipt of a complaint or other information that gives a reasonable account of the wrongful or fraudulent act. Many agencies provide fraud hotline numbers to facilitate reporting of fraud. Make sure that A/OPCs, AOs, and account holders are aware of the hotline number. Be as specific as possible when calling or sending in a complaint. If the complaint relates to an account holder, the A/OPC should provide the following:

- The employee's full name;
- Rank or pay grade;
- Duty station;
- Specific suspected fraudulent act or wrongdoing;
- Specific dates and times;
- Specific location of where the suspected fraudulent act occurred; and
- How the individual completed the alleged fraudulent act.

Inquiries that are informal administrative investigations normally are completed within 180 days. However, the time required to conduct an inquiry may vary depending on the complexity or amount of additional information needed to complete the investigation. Typically, the investigator will be able to tell whether the case is open or closed because of restrictions on disclosure of records covered by the Privacy Act of 1974. If a copy of the report is required, the A/OPC can make a written request to the IG's office.

Based on the findings of the investigation, an A/OPC may be required to notify an employee's supervisor and human resources office for further internal administrative action. Depending on the circumstances, an A/OPC may need to contact other organizations, including:

- The contractor bank's fraud unit;
- The IG;
- The fraud hotline;
- The DoD Criminal Investigative Service (DCIS);
- FBI;
- The Naval Criminal Investigation Service (NCIS);
- The U.S. Army Criminal Investigation Command (USACIDC); and/or
- The Air Force Office of Special Investigations (AFOSI).

Chapter 10: Joining the Community



Discussions with GSA SmartPay

GSA SmartPay online communities offer opportunities for networking and sharing best practices among groups utilizing the GSA Interact platform.

Discussions with GSA SmartPay is a private online community giving program coordinators (i.e., A/OPCs) a central location to share ideas and best practices, as well as discuss all other issues related to the GSA SmartPay program. If you are an A/OPC and would like to register, please go to <https://interact.gsa.gov>. Once registered, email your user ID to gsa_smartpay@gsa.gov, so we can add you to the private group.

Social Media

At GSA SmartPay, we believe that social media is a great way to stay in frequent, real-time contact with our customers and with the public, by highlighting all of the exciting developments, events, and news within our program.

GSA SmartPay maintains a strong online presence on social media, which includes regularly updated Facebook, Twitter, and LinkedIn pages.

To connect with GSA SmartPay on social media, go to <https://smartpay.gsa.gov> and click on the social media icons located on the homepage, which will direct you to GSA SmartPay's Facebook, Twitter, and LinkedIn pages. Feel free to follow or "like" our pages to receive our regular updates.

Acquisition Gateway

The Acquisition Gateway was created to consolidate available product and service information across best-in-class federal providers.

The Acquisition Gateway is categorized into product and service offering "hallways," which include information, tools, and resources to facilitate acquisition and procurement decision-making.

First-time visitors to the Acquisition Gateway should take a brief moment to register at **OMB Max**.

[View a video on the registration process.](#)



Monthly Meetings and Annual GSA SmartPay Training Forum

If you are an A/OPC and interested in participating in our monthly meetings and/or the annual GSA SmartPay Training Forum, please contact the GSA SmartPay program support Team at gsa_smartpay@gsa.gov.

Chapter 10 (continued)

Resources

Bank Contact Information

In order to effectively manage the GSA SmartPay purchase program for your agency/organization, it is important to know your contractor bank's information. It will be helpful to get to know your bank's customer service representatives/account managers. They can provide a wealth of information and are ready and able to answer questions to help you manage your program. Many of your responsibilities as an A/OPC involve a working relationship with the contractor bank.

Here is a listing of the contractor banks' websites and phone numbers. Ask questions and get involved – they are available to give you the technical assistance you need.

Citibank:

- (800) 790-7206 (within United States)
- (904) 954-7850 (collect calls from outside United States)
- [Citibank Online Account Access](#)

U.S. Bank:

- (888) 994-6722 (within United States)
- (701) 461-2232 (collect calls from outside United States)
- [U.S. Bank Online Account Access](#)

GSA SmartPay Program Support

For general information about the program or for escalated issues, please contact a member of the GSA SmartPay program support team:

Email: gsa_smartpay@gsa.gov

Phone: (703) 605-2808

The GSA SmartPay 3 Master Contract

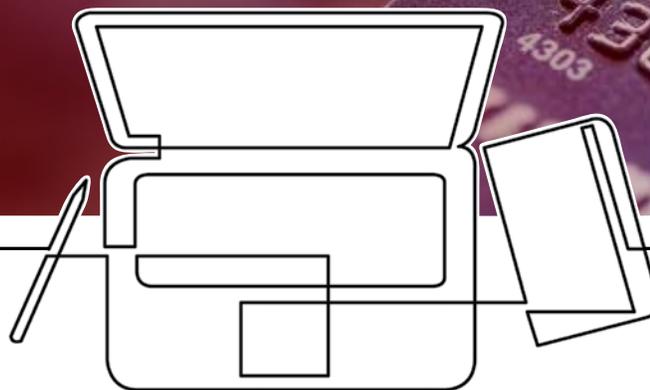
Understanding the terms and conditions of the GSA SmartPay Master Contract is important to performing your role as a program coordinator. The terms and conditions of the Master Contract identify specific contractual requirements that the GSA SmartPay program has with the contracting banks.

The GSA SmartPay Master Contract can be viewed on the [GSA SmartPay website](#). Download a copy and review relevant clauses and sections that pertain to the GSA SmartPay purchase program, as well as the GSA SmartPay program in general.

List of Commonly Used Abbreviations

Acronym	Description
A/OPC	Agency/Organization Program Coordinator
AO	Approving Official
CBA	Centrally Billed Account
CCCM	Center for Charge Card Management
DBO	Designated Billing Office
EAS	Electronic Access System
FAR	Federal Acquisition Regulation
GSA	General Services Administration
IBA	Individually Billed Account
IG	Inspector General
MCC	Merchant Category Code
OMB	Office of Management and Budget
TDO	Transaction Dispute Office/Official
TIN	Taxpayer ID Number

Appendixes



Appendix 1: Merchant Category Codes

- **Appendix 1-1:** Visa Supplier Locator
- **Appendix 1-2:** Mastercard Quick Reference Booklet

Appendix 2: Account Holder Fraud Checklist

Appendix 3: Sample Annual Review Process

- **Appendix 3-1:** Sample Annual Review Checklist
- **Appendix 3-2:** Sample Summary of Findings
- **Appendix 3-3:** Sample Certification of Completion of the Annual Review
- **Appendix 3-4:** Sample Questionable Purchases Form

Notes



Two columns of horizontal dotted lines for writing notes.

GSA SmartPay® Program Support

<https://smartpay.gsa.gov>

(703) 605-2808

gsa_smartpay@gsa.gov

www.gsa.gov
Winter 2018
5-19-00261

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