

Managing Your SmartPay Purchase Program





Managing Your GSA SmartPay Purchase Program

Introduction	2
Chapter 1: Overview of the Purchase Program	3
Chapter 2: Account Holder Fraud	21
Chapter 3: Non-Account Holder Fraud	26
Chapter 4: Liability	29
Chapter 5: The Review Process	30
Chapter 6: Indicators of Account Holder Misuse/Fraud	33
Chapter 7: Electronic Access System/Reporting	38
Chapter 8: Preventative Measures	40
Chapter 9: Taking Action	45
Appendixes	47



Introduction

When paying for purchases of supplies or services, the GSA SmartPay solution provides your agency with numerous benefits including cost savings, discount programs, and refunds. As an agency/organization program coordinator (A/OPC), you serve as the liaison between your agency, the contractor bank, the account holder and GSA. Your role is essential to efficiently and effectively manage your agency's GSA SmartPay purchase program.

In addition to the traditional card services, GSA SmartPay offers a variety of other payment solutions to assist with improving security, control, and oversight, as well as reducing paper and administrative costs. These innovative solutions can help your agency better leverage government spending while increasing transparency and accountability.

For more information, please visit <https://smartpay.gsa.gov>.

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



Chapter 1: Overview of the Purchase Program

GSA SmartPay - Supporting Your Mission

The General Services Administration (GSA) Office of Charge Card Management (OCCM) administers the GSA SmartPay Program, the world's largest government payment solutions program, with approximately \$28 billion in annual spend and 3 million account holders. OCCM provides GSA SmartPay services to more than 350 customer agencies and organizations, each with unique missions and needs. In addition to providing effective and efficient payment solutions, customer agencies have the opportunity to earn refunds for their agency.

OCCM is dedicated to providing customers with best-in-class and innovative payment solutions. OCCM's commitment to customers includes:

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

Customer Service

OCCM 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 A/OPC
- > Facilitating customer meetings and working groups
- > Providing ad hoc executive customer support

Relationship Management

OCCM collaborates and coordinates with customers to help manage critical relationships, which include GSA SmartPay contractor banks, Congress, the Office of Management and Budget, 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
- > Building a community of program coordinators to share best practices and lessons learned

Data Management, Security, & Monitoring

OCCM 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. OCCM 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 contract 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 Government-wide Metrics Dashboards to update customer agencies on individual card program performance
- > Providing customers with ad hoc reporting, by request

Contract and Task Order Management

OCCM provides contract and task order management support, which includes:

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

Master Contract

What is the scope of the GSA SmartPay Master Contract?

The scope of the GSA SmartPay Master Contract is to provide a worldwide procurement, payment, and functional data-storage mechanism to support authorized purchases, expenses, and streamline purchase and payment systems for the fleet, travel and purchase programs. All financial, management and administrative products and services (current and emerging), which assist in the support of authorized purchases, expenses, and streamline purchase and payment systems, fall within the scope of this contract. Additional requirements may be included in the task order issued to your contractor bank.

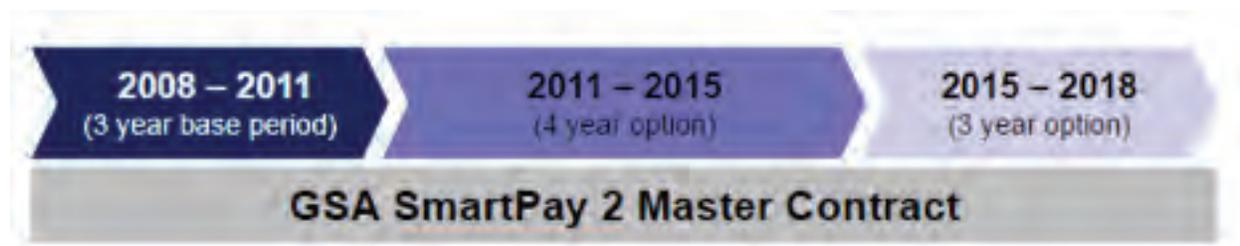
What is the purpose of the GSA SmartPay purchase program?

The purpose of the purchase program is to:

- > Provide commercial payment solutions and associated services in support of official government purchases;
- > Streamline ordering, payment and procurement procedures;
- > Reduce administrative costs under the simplified acquisition threshold;
- > Improve government operations by simplifying the financial process; and
- > Allow a platform to improve government operations and accountability.

What type of contract vehicle is used for the purchase program?

The GSA SmartPay 2 Master Contract is a fixed price, indefinite delivery, indefinite quantity (IDIQ) task order contract. The contract period for GSA SmartPay includes a transitional period and a transactional period. The transitional period began on the date of award and ends November 29, 2008. The transactional period (when actual transactions began to be processed through systems belonging to/ associated with successful offerors) began as early as November 30, 2007, and has a four-year base period, with one four-year option period, and one three-year option period.



Task Order Types:

There are four task order types under the GSA SmartPay 2 Master Contract, and these include:

- > Standard: Contains the same requirements as the master contract
- > Tailored: Includes agency/organization-specific requirements
- > Tag-along: Uses another agency's/organization's task order
- > Pool: Occurs when two or more agencies/organizations collaborate to develop and issue one task order which will meet the multiple agency/organization needs

Benefits to using the GSA SmartPay 2 Master Contract for obtaining payment services:

- > Utilizing the master contract means a faster contract acquisition process and reduced risk of protest, as compared with a full and open competitive procurement
- > Favorable negotiating platform and contract terms
- > GSA SmartPay contracts are awarded to banks based on a competitive bidding process
- > OCCM has established relationships with contract banks
- > The GSA SmartPay 2 Master Contract offers a broad range of flexible products and services for agencies/organizations as well as, the flexibility to add products and services
- > OCCM is available to support customer agency/organizations

Teaming Partnership Opportunities: GSA SmartPay 2 Master Contract offers contractor banks the flexibility to partner with subcontractors (as needed) to provide specific services to agencies/ organizations.

GSA SmartPay Program Refunds

The GSA SmartPay program generates performance-based refunds for agencies/organizations. Types of refunds include:

- > Productivity refunds: based on the timeliness and/or frequency of payments to the bank (faster payments = higher refunds)
- > Sales refunds: based on the dollar or spend volume during a specified time period

Refunds under the GSA SmartPay program are discounts offered by the banks, which 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 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 Treasury general fund.

What is a GSA SmartPay Purchase Account?

A purchase account is a type of payment solution issued by a GSA SmartPay contractor that is used to pay for supplies or services procured at the direction of a Federal agency/organization under official purchase authority. The agency is invoiced for the purchases and makes payment directly to the bank.

All purchase accounts are considered Centrally Billed Accounts (CBAs). They are established by the contractor bank at the request of the agency where payment is made directly by the Federal Government. Purchase accounts may be established through any payment solution listed in the master contract.

Best Practice: In accordance with the [Federal Acquisition Regulation \(FAR\)](#), the GSA SmartPay purchase account is the preferred method of payment for supplies and services that are below the micro-purchase threshold:

- The Purchase Account is a procurement and payment mechanism for micro-purchases,
- For purchases above the micro-purchase threshold, the purchase account may be used as a payment mechanism under a contract. The purchase account is NOT a contracting mechanism.

How can my agency utilize purchase payment solutions?

The agency's chief financial officer, chief administrative officer, and procurement executive decide which bank will be issued a task order to provide payment solutions to the agency. The task order will designate who has authority within the agency to administer the program (set up accounts, receive reports, etc.). The agency may also choose to tag along with another agency's task order to obtain more favorable terms.

OMB Circular A-123, Appendix B

OMB Circular A-123, Appendix B – provides guidance for all GSA SmartPay payment solutions including the GSA SmartPay purchase solutions.

- > The Circular consolidated into one document program requirements and guidance from OMB, GSA, Treasury and other federal agencies
- > Establishes standard minimum requirements and best practices for improving the management of the GSA SmartPay program
- > Provides a single source document to incorporate updates, new guidance, or amendments to existing guidance

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

- > Developing and maintaining a management plan
- > Provide training to all account holders and account managers (including A/OPCs and AOs)
- > Implement Risk Management controls, policies, and practices
- > Maintain and report data and performance metrics
- > Manage refunds
- > Implement strategic sourcing for certain commodities & analyze purchase spending data
- > Adhere to Section 508 of the Rehabilitation Act
- > Account for environmental quality of products procured with purchase accounts
- > Recover state and local taxes levied on purchases
- > Develop and maintain written policies and procedures for appropriate use of convenience checks
- > Issue policies and procedures to ensure effective management of federal property

Federal Acquisition Regulation (FAR)

The [Federal Acquisition Regulation \(FAR\)](#) is the principal set of rules in the Federal Acquisition Regulation 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 customer’s 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

OMB Memorandum M-13-21 is a response to Public Law (P.L.) 112-194, the Government Charge Card Abuse Prevention Act of 2012. OMB Memorandum M-13-21 provides supplemental guidance to the OMB Circular A-123, Appendix B in the following areas:

- > Requires all Federal agencies to establish certain safeguards and internal controls for the government payment solutions program;



- > Reports on purchase and integrated violations, and establishes penalties for violators, including dismissal when circumstances warrant (purchase transactions only); and
- > Increases 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.

Compliance Summary Matrix

OMB Memorandum M-13-21 directs agencies to use the “Compliance Summary Matrix” to help ensure the required safeguards and internal controls are in place. 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 existing internal controls within their implementation payment solutions program in order to document the operational effectiveness of current control activities. Instances of non-compliance should be documented as well as a summary of corrective actions to be taken to address shortcomings.

Executive agencies should maintain this compliance summary on-file along with related supporting documentation, as evidence of adequate control assurances. This compliance summary should also be available for IG reviews. Agencies should summarize the overall results in their completed compliance summary and internal 3 control assurance assessments in their annual payment solutions management plans, beginning with their January 31, 2014 submission to OMB.

Note that the compliance matrix is designed to assist agencies in employing an effective internal control program which is in balance with the need to maintain flexibility and ease of use in support of agency mission activities. As a result, compliance with individual matrix criteria in and of itself is not as important as the effectiveness of an agency's internal control program overall.

[Appendix 1-1: Compliance Summary Matrix](#)



Implementation of the Charge Card Prevention Act

The chart in Appendix 1-2 provides information on all reporting requirements for agencies under OMB Circular A-123, Appendix B and the new Public Law 112-194, Charge Card Abuse Prevention Act.

Note: OMB is requiring the submission of the Statistical Report (see OMB Circular A-123, Appendix B 5.3.1). CFO Act Agencies and DHS should continue to submit these reports quarterly. All other agencies are required to submit the report annually on January 31.

Note: OMB is requiring the submission of the Periodic Narrative Report (see OMB Circular A-123, Appendix B 5.3.2) on January 31, 2014.

[Appendix 1-2: Implementation of the Charge Card Prevention Act](#)

Charge Card Violations Report: Reports of Purchase Account Violations

Beginning with fiscal year 2013, each agency with more than \$10 million in purchase spending the prior fiscal year is required to submit semi-annual reports of employee purchase or integrated account violations and the disposition of these violations, including disciplinary actions taken. Consistent with Section 6 of the Charge Card Act, the semi-annual reports shall not disclose personally-identifying information protected from disclosure under the Privacy Act of 1974 (5 U.S.C. 552a).

At a minimum, the report shall provide the following:

- > A summary description of confirmed violations involving misuse of a purchase or integrated solution, following the completion of agency or IG review.
- > A summary description of all adverse personnel actions, punishment, or other actions taken in response to each reportable violation involving misuse of a purchase or integrated solution.
- > An administrative or internal control process inconsistency that does not result in fraud, loss to the Government, or misappropriation of funds or assets (whether or not recouped) is not a reportable violation for purposes of the semi-annual report.

The semi-annual Joint Purchase and Integrated Card Violation Report is to be prepared by the agency head and the IG for submission to OMB 120 days after the end of the reporting periods (i.e., April 1 to September 30 and October 1 to March 30), beginning with the January 31, 2014 submission. The submission should be incorporated into the existing Charge Card Management Plans, which are also due to OMB on January 31, 2014. The second semiannual report is due on July 31, 2014.

[Appendix 1-3: Semi-Annual Report on Purchase Card Violations](#)

Charge Card Narrative Report

Agencies listed in the original Chief Financial Officers Act of 1990 and the Department of Homeland Security are required to report on the following narrative information on an annual basis at the same time the first quarter statistical reports are submitted. All other agencies are required to report on these items on a bi-annual basis:

- > The date(s) of most recent and next scheduled independent review (e.g., Office of the Inspector General) for all agency charge card programs;
- > A description of the current process for monitoring delinquency, including what reports the agency reviews and what actions are taken when a problem is discovered;
- > A description of the steps the agency takes to address turnaround time (> than 15 working days) following voucher submission for travel voucher reimbursement, if applicable;
- > A description of the method the agency utilizes to identify and detect possible card misuse, including the use of any specialized information technology solutions as well as any requests to charge card vendors for data reports;
- > Agency future plans (within the next 12 months) to enhance charge card systems by automating reviews to detect instances of abuse, misuse, and fraud;
- > A description of any best practices the agency employs in charge card management;
- > Any plans for implementing paperless statements; and
- > Any additional useful information regarding charge card programs.

[Appendix 1-4: OMB Circular A-123, Appendix B, Chapter 5.3.2 Narrative Reporting Template](#)

Public Law

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

American Recovery and Reinvestment Act of 2009 (P.L. 111-5)

- > A section on the Tax Increase Prevention and Reconciliation Act of 2005 (TIPRA)
- > Delays the withholding of tax on government contractors until December 31, 2011 (one-year delay from the original date)

Government Charge Card Abuse Prevention Act of 2012 (P.L 112-194)

- > 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
- > Increases oversight by providing that each agency Inspector General periodically conduct risk assessments and audits to identify fraud and improper use of government charge cards
- > Appendix 2: [S.300 Enrolled OMB Crosswalk document](#)

Sources of Public Law:

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

Roles and Responsibilities within the Program

Agency – Each agency must designate an Agency/Organization Program Coordinator (A/OPC) who shall function as the agency's primary liaison to the purchase contractor bank and to GSA. The agency must also identify account holders and designate a billing and disputes office.

Agency/Organization Program Coordinators (A/OPCs) are responsible for the overall management and oversight of the accounts under their span of control. Generally speaking, these 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;
- > Auditing accounts as required by your agency policy;
- > Monitoring fraud and misuse within the program;
- > Establishing guidelines for the agency/account holder;
- > Administering training; and
- > Using the bank's Electronic Access System to perform account management and oversight.

Approving Official (AO) is typically the account holder's supervisor and assures proper use of the purchase account. The AO is responsible for:

- > Conducting an independent review of account holder transactions;
- > Ensuring all charges are proper, meet agency needs, and are reconciled in a timely manner; and
- > Approving monthly billing statement.

Account Holders are individuals or agency/organization components designated by an agency/organization to receive an account. The account holder is responsible for:

- > Securing the payment solution;
- > Maintaining records relating to all transactions;
- > Using the account ethically for official government purchases only;
- > Understanding their respective agency's policies and procedures regarding the use of a purchase account;

- > Using the account for authorized purchases;
- > Reporting lost or stolen account;
- > Reconciling account; and
- > Disputing transactions in accordance with the bank's policy.

How are invoices issued and processed?

Invoicing will occur on a monthly basis, unless otherwise specified by the agency. The agency policy shall include a process for a thorough manual or electronic reconciliation of all transactions, debits and charges posted to the account during the billing cycle.

Settlements for centrally billed accounts are made directly by the agency designee. The contractor bank shall accept payment from multiple sources electronically and post such payments within two business days of receipt of payment to the agency's specified account.

Designated Billing Office (DBO) serves as the focal point for receipt of official centrally billed invoices. The DBO oversees the proper processing of invoices and ensures invoices are paid within the Prompt Payment Act timeframes. Responsibilities typically include:

- > Reconciling invoices;
- > Providing feedback to the A/OPC on bank performance;
- > Determining whether to pursue faster payment of official invoices in order to take advantage of productivity refunds, if in the best interest of the Government;
- > Providing timely payment to the bank;
- > Providing proper interest penalties for payments that exceed Prompt Payment Act timeframes; and
- > Making certain that the agency/organization's task order is adequately funded.

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

EC/EDI Office (EO) is the focal point for electronic commerce/electronic data interchange (EC/EDI) for the agency/organization. The EO oversees the proper implementation of the agency/organization EC/EDI capabilities and processes.

Purchase Contractor/Issuing Bank:

- > Enables merchant payments for purchase transactions;
- > Establishes accounts;
- > Issues cards, if required;
- > Prepares the monthly statement for each account holder;
- > Issues invoices to the DBO;
- > Provides 24-hour customer service; and
- > Prepares reports that assist your agency in effectively utilizing the program.

Can the bank suspend or cancel an account?

Suspension of an account: The bank shall notify the A/OPC and the Designated Billing Office (DBO) requesting payment of undisputed past due accounts (45 days from billing date). The bank shall provide a pre-suspension report to the A/OPC to identify the undisputed overdue amounts. After 55 calendar days from the billing date, the bank shall notify the A/OPC and the DBO electronically, or in writing, of suspension if the payment for the principal amount is not received by the close of business on the fifth calendar day after notification. The bank is required to reinstate, automatically suspended accounts, upon payment of the undisputed principal amount and Prompt Payment Act interest.

Cancellation of an account: The bank has the discretion to initiate cancellation procedures on accounts. Cancellation must be initiated within 180 calendar days of the billing cycle in which the charge appeared. If the bank initiates cancellation, it shall provide a pre-suspension/pre-cancellation report to the A/OPC to identify the undisputed amount that is overdue. There are two reasons in which a bank may initiate cancellation:

1. The account has been suspended two times during a 12 month period for undisputed amounts; or
2. The account is 120 calendar days past the billing date and suspension procedures have been met. After 120 calendar days past the billing date, the bank shall send a letter to the A/OPC and the DBO requesting payment of the undisputed principal amount. If payment is not received by the close of business on the fifth calendar day after notification (126 days from the billing date), the bank may cancel the account.

The bank may, but is not required to, reinstate cancelled accounts upon payment of the undisputed principal amount and Prompt Payment Act interest. A/OPCs have the discretion to initiate suspension and/or cancellation procedures. They must document the reason for cancellation or suspension.

Merchant is the source for your supplies or services. Merchants may be a required source inside or outside the Government, another government agency, or a private sector merchant of supplies or services.

GSA SmartPay Payment Solutions

Through the GSA SmartPay program you will have access to many payment options to support agency mission delivery, such as improving security, control and oversight, reducing paper and administrative costs, as well as other innovative ways to better leverage government spending while increasing transparency and accountability.

The products and services offered under the GSA SmartPay master contract allow agencies to customize payment solutions and achieve their goals. Each agency awards a unique task order to one of the three GSA SmartPay contractor banks: Citibank, J.P. Morgan, and U.S. Bank. All products and services described here are available for your agency under the GSA SmartPay program, but may not be specified at the task order level. Therefore, it is important to review your agency's task order to find out how you can take advantage of these offerings.



Contactless and Contact Chip Cards

Contact Chip Card – Ever evolving needs and new demands on the card industry have led to new, improved and innovative card technologies. Pursuant to section 1(b) of the Presidential Executive Order (EO) on “Improving the Security of Consumer Financial Transactions,” also known as the “Buy Secure” initiative, the United States General Services Administration’s (GSA), Office of Charge Card Management (OCCM), has transitioned the federal government’s GSA SmartPay commercial charge card program to higher security EuroPay MasterCard Visa (EMV) standard “chip” type charge cards.

The EO requires the Federal Government to adopt “enhanced security features” on its commercial payment programs. This transition was undertaken to reduce program exposure to external fraud, as well as to show federal leadership in moving to this technology. Among other issues, actions to enhance charge card transaction security involve both charge cards issued to federal government agencies and other authorized organizations as well as merchant terminals used by these organizations to process charge card payments.

How Chip Technology Works: Chip or EMV charge card products contain a microprocessor which is embedded into the card. The chip creates a code known as a “cryptogram” for each transaction when inserted into a payment terminal while making a purchase. As a result, it is much harder to counterfeit these cards compared to traditional magnetic stripe cards, since a unique cryptogram is generated for each transaction and fraudsters have yet to be successful in counterfeiting the chip technology. These cards therefore offer significant protection against “card present” fraud, where the card is physically inserted into a payment terminal.

Best Practice: Card data from the face of the card or from the magstripe (which will also be present on chip cards as a back-up capability for the foreseeable future), can still be captured and used in online fraud, so it is important to remind account holders to continue to monitor their transactions and monthly statements. As an added layer of security and to facilitate overseas acceptance, OCCM is requiring the issuance of Personal Identification Numbers (PINs) as one of the account holder verification methods for every GSA SmartPay purchase and travel charge card. Within the U.S., PIN prompting may be very limited, however there are countries where PIN use is more prevalent, particularly at unattended kiosks such as those often located within public transit stations. We hope to encourage the payment industry in the United States to move towards further use of PIN-preferring corporate charge cards over time.

Contactless Chip Cards – A contactless chip card is a card product that has a chip and antenna integrated within the plastic, in addition to a traditional magnetic strip which is found on the back of the card. As an alternative to swiping a card through a card reader, a contactless chip card needs merely to be placed over a RFID (Radio-Frequency Identification) reader in order for the transaction data to be captured and a purchase to be completed. Contactless chip cards use highly secure data transmission standards, and are considered difficult to compromise. Typically, the contactless chip within the card creates a unique transaction number for every transaction that is included with the card number details, which makes it very difficult for any data to be copied and reused by those wishing to commit fraud.

Tokenization may be available for corporate accounts in the near future. Card-related payment systems which use tokenization include: Apple Pay, Google Wallet and Samsung Pay (formerly Loop Pay). These systems provide a higher level of security and can generally be used for both card present and card not present transactions. Note: This form of payment require employees to use a smartphone to complete a transaction.

Stored Value and Declining Balance

Stored value and declining balance solutions are innovative products where a set amount can be placed onto the account and the account holder cannot spend more than the amount that has been pre-loaded or more than the credit limit that has been set to the account. Both types of solutions will reduce administrative costs and inefficiencies associated with paper work and support the government's green initiative by reducing paper-based methodology. These products also provide financial flexibility and security, as well as offering a safe and excellent alternative to cash, paper checks (eliminating the risk of lost or stolen checks) and electronic fund transfers. Each bank's Electronic Access System (EAS) has the ability to provide maximum flexibility to program coordinators, allowing them to use the stored value and declining balance accounts alternatives to solve various business needs.

Benefits:

- Provides financial flexibility and security
- Reduces agency/organization administrative fees
- Offers a flexible option for applicants who cannot be issued a traditional account
- Presents an opportunity to increase savings and refunds for the agency/organization
- An alternative to convenience checks, which also provide the opportunity to move towards green practices, including the government's initiative to lessen convenience check usage

Stored Value Solutions – A stored value account has a specific dollar amount that is paid in advance from agency funds onto the account. Stored value accounts can have a single value load (e.g. rebate cards) or can be reloaded with a specified amount that is funded to the account on a recurring basis (e.g. payroll cards). There are many levels of control that can be granted to program coordinators through the bank's EAS in order to solve unique business functions or expenses.

Benefits include:

- > Immediate fund availability and flexibility on activation procedures
- > PIN number can be provided for ATM withdrawals
- > MasterCard/Visa branded for Point of Sale (POS) transactions
- > Purchase restrictions such as Merchant Category Codes (MCC) controls
- > No credit check, spending limits are not determined by credit history
- > High levels of control (i.e. more spending limit options)
- > Option to issue as a non-personalized account
- > Account holder can access bank's website to view balance and transaction history
- > A variety of other benefits and flexible options

Declining Balance Solution – Declining balance accounts have the same functionality as a basic charge card, but the limits on the declining balance accounts do not have to refresh each month. Declining balance accounts are a central liability and thus are paid for by the agency much like the Purchase, Travel, or Fleet Centrally Billed Accounts (CBAs). This type of account can be set up for a specific purpose or for a specified time period where the account is set with a pre-determined credit limit. The credit limit can either be reset as needed (or at a specified time) or the account becomes inactive once the balance is used. With a declining balance card, an agency does not have to pay the amount on the account in advance since it works like a traditional centrally billed account, allowing for greater oversight and control versus a stored value account where all funds loaded to the account are available for spend. Similar authorization controls, such as MCC blocks, can be used on these types of accounts in the same way that they are used to control the traditional GSA SmartPay accounts. Declining balance accounts do not require credit checks and spending limits are not determined by credit history if used in place of an Individually Billed Account (IBA) travel card. There is also a high level of potential control as well as one-time use options or low frequency refreshes.

Declining Balance Accounts can be provided to employees who cannot or should not have a regular account, to infrequent travelers in lieu of a travel card, and/or to non-agency personnel for invitational travel. They can also be used in emergency situations or for grants funding, reimbursement to employees for out-of-pocket expenses, uniform allowances and relocation payments.

Grant Funding Challenge – Many grant-making agencies face the challenges of distributing federal funds to grantees in an efficient manner, as well as coordinating with grantees to maintain a level of transparency and accountability for how dollars are spent. Stored value or declining balance solutions can be used to issue grant funds. Using these types of solutions for grants funding will allow greater transparency in the award and distribution process (once the grant-making agencies receive the funds by allowing agencies to track, monitor and administer grant programs through the bank's EAS). Agencies will also earn refunds on grants funding spend.



Virtual Accounts

Virtual accounts are a popular alternative to handling large dollar transactions. There are multiple types and uses for virtual accounts and they often do not involve the issuance of a plastic charge card. Virtual accounts can be used for single or multiple transactions.

Ghost cards and single use accounts (SUA) are two types of virtual accounts. Although traditionally used within the Federal Government for the purchase of airline tickets, centrally billed virtual accounts can be set up or used as a payment method under existing contracts with a high volume of ordering activities. It may be an organizational account used within a specific department, or as an account that sits within an accounts payable or finance office.

Benefits: Virtual accounts offer solutions to various business challenges, such as large ticket transactions, payment to vendors who do not typically accept card-based payments, one-time supplier payments or recurring transactions with a specific vendor. Virtual accounts also help your agency increase refunds and achieve its sustainability goals, since the virtual card authorization and transaction posting process is completely electronic.

Ghost Accounts – A ghost account is a centrally billed cardless account designated for a supplier who is frequently used by an agency, where the account number is typically assigned to the vendor, allowing for any authorized agency personnel to purchase from this vendor without having to use multiple accounts. This type of account is typically managed in a central location by one office/department within an agency. Today, many agencies use ghost accounts, whether it is through a purchase card account or a centrally billed travel account used to procure airline tickets.

Best Practice: To aid in ghost account reconciliation, it is a recommended best practice that the agency employee responsible for the ghost account works closely with the vendor to determine if the vendor is at least capable of passing level 2 information to capture each agency employee making purchases. For central travel airline accounts, the passenger name is typically captured by the travel agency and passed back in the transaction information to aid in reconciliation. Note that accounts issued in a department name instead of an agency employee name do have different chargeback and dispute rights, so check with your GSA SmartPay contractor bank about this for details.

How ghost accounts can benefit your agency:

- > Reduces number of open accounts, making payment processing and oversight easier
- > Allows for multiple users
- > Creates strong, ongoing relationship with merchants
- > Allows for a high level of control
- > Reduces the risk of lost or stolen accounts

Best Practice: The Department of Commerce (DOC) utilizes “Department Virtual Payment Cards” which allows DOC to pay UPS orders via GSA’s Federal Strategic Sourcing Initiative (FSSI) Document Delivery Service BPA. This innovative solution improves operational efficiencies, reduces administrative costs and allows DOC to earn additional refunds.

Single Use Accounts (SUA) – A single use account does not require a physical card in order to function like one. A single use account is a virtual account number that may be used during a limited time period, for a limited dollar amount, and/or for a specific vendor. A single use account product can offer a pre-established account that is available for instantaneous issue, where a randomly generated account number can be activated in real time through the bank’s Electronic Access System (EAS). In addition, an expansive selection of payment controls – such as Merchant Category Code (MCC) blocks, spending limits, timeframes, and account expiration dates – can be established prior to or at the time of the account number’s activation, allowing for increased control over spend on the account. Finally, the agency can append accounting data to the order to ensure seamless reconciliation.

Examples include using a SUA to pay for expenses related to a specified meeting or conference. Invoices relating to the event would be paid with the account number. This provides control over the availability of funds, by limiting what can be spent on the account. Single use accounts can also be used to pay approved invoices or make contract payments, which will ensure that the merchant cannot charge more than the approved amount.

Benefits of Single Use Accounts:

- > 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
- > Reduces the usage of convenience checks
- > Offer significant protection against merchant misuse and fraud

As an example, the Department of Energy (DOE) has expanded its GSA SmartPay program implementation to allow one of its major cost reimbursable contractors, CH2M-WG, LLC (CWI), to participate in the purchase card program. The approach has been a win-win situation for both DOE and CWI, with a net result of increased card program spend and both entities receiving the benefits of refunds. DOE, through CWI, discovered that SUA is an easy-to-adopt alternative to checks, ACH, and WIRE. Similarly, SUA is helping CWI expand its GSA SmartPay program to include large-dollar purchases that would normally not be allowed under the traditional purchase card program. In addition to boosting spend, CWI has found SUA to be a cost effective alternative to other payment methods.

Electronic Invoice Presentment and Payment (EIPP) – The Electronic Invoice Presentment and Payment (EIPP) solution allows agencies and merchants to manage the entire invoice and payment cycle online, eliminating the steps and procedures typically associated with a paper-based system. EIPP capability supports invoice tracking and management through an online portal, directly connecting buyers with suppliers. As a result, the length of time that sales are outstanding is shortened and costs traditionally associated with paper-based payment systems are eliminated.

The EIPP solution allows agency personnel to use electronic payments to pay merchants who traditionally do not accept card based payments on high dollar transactions. When a normal charge card transaction is processed, merchants pay a discount rate on every transaction in order to accept a charge card. Merchants are willing to pay the rate for small dollar transactions but when the size of the transaction grows, the associated discount rate may become untenable for them. EIPP gives the merchant the ability to receive early payment at a discount rate that is much lower than what would normally be associated with a purchase card transaction.

Benefits of EIPP:

- > Improved cash-flow visibility – the status of each invoice can be viewed online
- > Early payment options frees up vendor credit lines to capture additional funding with lenders
- > Accelerated payment settlement, due to the elimination of mail time and float typically associated with paper-based processes
- > Increased visibility and control over invoice tracking and history for buyers and suppliers
- > Ability to pay merchants who traditionally do not accept card-based payments on high dollar transactions
- > Efficient payment process reduces the number of late payments and therefore the need to pay Prompt Payment Act penalty interest.

Foreign Currency Accounts

A foreign currency account is a product that is both issued and billed within a specific local currency other than U.S. dollars. This type of account is designed to coordinate and align with the common business practices of a specific country or area in the world. Account related issues such as customer service inquiries, billing statements, and merchant issues occur in the language and currency of the country in which the card is issued.

For agencies and organizations with globally based employees, or that deploy personnel to international zones for long periods of time, the issuance of a foreign currency account is a flexible option that takes advantage of the new technology and opportunities offered through the GSA SmartPay program, and which can improve your overall program.

Benefits of a Foreign Currency Account:

- > The greatest financial benefit of foreign currency accounts is the elimination of foreign currency exchange fees as long as the account is used in-country
- > Availability to issue accounts in predefined global locations
- > Authorization and settlement of transactions occur in local currency, eliminating exchange fees for in-country transactions
- > Foreign currency accounts allow for customer support in the local language
- > Alignment with local business practices improves relationship with merchants

Best Practice: The Department of State: Foreign Currency Card Program The Department of State began to utilize Centrally Billed Account (CBA) travel foreign currency cards in the summer of 2008. They are currently being used in as many as seven countries, predominately throughout Europe. This card solution was implemented in an effort to reduce exchange rate fees and increase overall cost savings when making local purchases abroad. These CBA travel accounts are issued with country/region specific BINs and in the local currency. The card statements are provided in the country currency instead of in U.S. dollars. This is beneficial to the overseas program office as well as to international vendors. Additionally, customer service for account holders and vendors is offered in the local language, making customer service issues easier to resolve.

Other Offerings

Other offerings under the GSA SmartPay program include:

- > **Data Mining** – Data mining is available for agencies that wish to analyze spending trends and patterns.
- > **Net Billing** – This process ensures that merchant discounts or rebates offered are deducted at the point of sale, guaranteeing discount arrangements.
- > **Email Alert Service** – This option provides automatic email alerts for account transactions to program coordinators, approving officials and/or supervisors.



Chapter 2: Account Holder Fraud

If an employee in an agency becomes aware of possible misuse of a payment solution, the account holder activity should be examined by the designated Agency/Organization Program Coordinator (A/OPC) to determine if further action is required. Some activity may appear suspect upon initial review, but with further investigation may be determined to be legitimate government business that can include a broad range of activities. A/OPCs have access to account holder information and would be the first point of contact in most situations.

What is account holder fraud/misuse?

Fraud is a deception deliberately practiced with the motive of securing unfair or unlawful gain. Examples include intentional misrepresentation of facts, deceitful practice, or willful device with intent to do injury or damage to another. Specific to our topic here, fraud can be an attempt to cheat the Federal Government and corrupt its agents by using GSA SmartPay accounts for transactions not part of official government business. Fraud can come in many disguises, such as false emails, mail, or phone calls. Intentional misuse of a GSA SmartPay account by the account holder can result in fraud.

The employing agency of an account holder who misuses the account or who participates in fraudulent activity may cancel the purchase account and take appropriate disciplinary action against the employee. In the case of account misuse, the employee will be held personally liable to the Federal Government for the amount of any unauthorized transaction. Additionally, depending on the facts involved, an employee may be subject to fines or imprisonment for action relating to the misuse/fraud.

If convicted under 18 USC 287, a person is subject to fines and/or imprisonment for not more than five years. Military members may be subject to court martial under 10 USC 932, UCMJ Art.132. Depending on the circumstances, other sections of the USC may apply and may carry additional penalties or fines:

- **Frauds and Swindles (Mail Fraud) – 18 USC 1341;**
- **Fraud by Wire, Radio, or Television – 18 USC 1343;**
- **Conspiracy to Commit Offense or Defraud United States – 18 USC 371;**
- **Bribery of Public Officials and Witnesses – 18 USC 201;**
- **Laundering of Monetary Instruments – 18 USC 1956;**
- **Public Money, Property, or Records – 18 USC 641;**
- **Statements or Entries Generally – 18 USC 1001;**
- **Extortion by Officers or Employees of the United States – 18 USC 872;**
- **Conspiracy to Defraud the Government with Respect to Claims – 18 USC 286; and**
- **Persons in a Position of Trust – Normally used during sentencing. This statement is usually introduced by the assistant U.S. attorney to obtain additional points from the Federal Sentencing Guidelines.**

Employees issued an account are responsible and accountable for each transaction made with their purchase account and they must ensure that supplies and services are procured at the direction of the agency under official purchase authorizations.

Intentional use of a government account for other than official government business constitutes misuse, and depending on the situation, may constitute fraud. Each agency develops and implements policies related to employee misuse.

Examples of misuse include:

- > Purchases that exceed the account holder's limit;
- > Purchases that are not authorized by the agency;
- > Purchases for which there is no funding;
- > Purchases for personal consumption;
- > Purchases that do not comply with the Federal Acquisition Regulations (FAR) and other applicable procurement statutes and regulations; and
- > Purchases billed by the merchant but not received by the agency.

Examples of Cardholder Misuse and Fraud

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 his personal consumption. The account holder 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 his 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 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 – Account holders would establish front companies to receive payment for merchandise never received. The account holders would then conspire 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

Best Practice: Establish clear guidelines and procedures for disciplinary action to be taken against individuals for the improper, fraudulent or abusive use of the purchase account.

Potential consequences for the account holder may include:

- > Counseling,
- > Cancellation of the account,
- > A written warning,
- > Notation in employee performance evaluation,
- > Reprimand,
- > Suspension or termination of employment, and
- > Criminal prosecution.

In the case of a centrally billed account (CBA), either purchase or CBA travel account misuse, the employee may be held personally liable to the Federal Government for the amount of any unauthorized transactions. Depending on the agency and the circumstances, there are a number of applicable laws that can result in fines or imprisonment.



Additionally, in certain cases, contractor banks are authorized to take certain actions against account holders whose accounts are cancelled for delinquency, such as:

- > Assessing late fees;
- > Utilizing collection agencies to recover the delinquent balance;
- > Reporting the delinquency to national credit bureaus, and
- > Salary offset.

Limits on Use

Micro-purchases:

The GSA SmartPay payment solution may be used to purchase supplies and services in accordance with and agency policy. The purchase account acts as both an ordering/contracting mechanism and a payment tool for micro-purchases. “Micro-purchase” means an acquisition of supplies or services in which the aggregate amount does not exceed the micro-purchase threshold, except in the case of construction.

References:

- FAR Subpart 13.2 Actions At or Below the Micro-Purchase Threshold
- FAR Subpart 13.3 Simplified Acquisition Methods
- FAR Subpart 8.4 Federal Supply Schedules

Purchases Above the Micro-Purchase Threshold:

For purchases above the micro-purchase threshold, the purchase account may be used as an ordering and payment tool, but not a contracting mechanism. When used as an ordering and payment tool, merchants may bill against the account.

Example of a Purchase Above the Micro-Purchase Threshold: An order has been placed with a merchant on a GSA Federal Supply Schedule for \$15,000. The award was made using the ordering procedures in accordance with FAR 8.4. The merchant agrees to accept the purchase account as payment. When the order is delivered, the merchant bills the purchase account instead of issuing an invoice directly to the agency. All applicable requirements of the Competition in Contracting Act, other statutes and Executive Orders, the Federal Acquisition Regulations, as well as agency supplements, apply to purchases made with the purchase account as the ordering and payment tool.

To allow agencies the maximum latitude, the GSA SmartPay Master Contract excludes only a few categories of purchases. However, agencies may choose to impose other restrictions on use or any exception procedure, such as maximum transaction dollar amount for a purchase.

Purchases that are STRICTLY PROHIBITED include:

- > Long-term rental or lease of land or buildings
- > Travel or travel-related expenses (not including conference rooms, meeting spaces, and local transportation services)
- > Cash advances (unless permitted by your agency/organization)

Centrally billed GSA SmartPay accounts cannot be used for private gain. For example, a GSA SmartPay account holder can not register for any benefit program linked to their their GSA SmartPay purchase account. The purchase account is used to acquire products and services intended for Government use paid for with Government funds. Account holders who register their accounts with these benefit programs are violating the Standards of Ethical Conduct because they are using their public office for private gain. Please contact your agency Ethics Official for any questions on this issue (Usually, an attorney in the Office of General Counsel).

The Standards of Ethical Conduct for Employees of the Executive Branch (Title 5, Chapter XVI, Section 2635 of the Code of Federal Regulations) states: "An employee shall not use his public office for his own private gain".

<https://www.oge.gov/>

The Office of Government Ethics (OGE) website provides the Standards of Ethical Conduct for employees of the executive branch.



Chapter 3: Non-Account Holder Fraud

Non-cardholder fraud involves the use of a payment solution or account holder data by an unauthorized person.

Fraud involving a physical card:

- > **Card Never Received** – A new or replacement card has been mailed to the account holder but was not received. Due to the possibility the card could have been intercepted by a third party, the account will be cancelled by the bank upon notification from the account holder. A new card with a new account number will be issued. Each account holder will be required to activate his or her card by phone once they receive it.
- > **Lost/Stolen Card** – The account holder reports the card lost or stolen. The account will be closed, and a new card will be issued. Reporting the card as lost does not relieve the Government for payment of any transactions that were made by the account holder prior to reporting it lost. The account holder may be required to sign an affidavit confirming the card was lost/stolen.
- > **Altered or Counterfeit Cards** – These types of cards are normally identified by the bank's authorization process or by the account holder when they receive their statement. Third parties obtained account information and used that information to make purchases with an altered or counterfeit card. If the bank recognizes a fraudulent pattern of use at the time of authorization, the bank will validate the use of the card with the account holder and/or suspend the card. The account holder may be asked to sign an affidavit verifying that the transactions were fraudulent.

For any transactions NOT made by the account holder on the statement, the account holder must submit a dispute form to the bank within 90 days from the date that the transaction was processed. Failure to submit the dispute form and/or affidavit could result in liability of the Government for the transaction charge(s). An account holder may forfeit his or her rights to dispute if the form is not submitted within 90 days.

Fraud involving Identity theft:

- > **Account Takeover** – In this case, the account holder's identity has been compromised, and a third party requested a new card by providing confidential information about the account holder. Any account holder who believes that they may have been subject to identity theft should contact the bank's customer service department.

To report any suspected fraud, account holders should immediately contact the bank's customer service:

Citibank:

- (800) 790-7206 (within United States)
- (904) 954-7850 (collect calls from outside United States)

JP Morgan Chase:

- (888) 297-0781 (within United States)
- (847) 488-4441 (collect calls from outside United States)

U.S. Bank:

- (888) 994-6722 (within United States)
- (701) 461-2232 (collect calls from outside United States)

Once a determination is made that an account has been compromised, investigation of the activity on the account is the responsibility of the bank. Unless a government employee is determined to be involved in the fraud, the agency generally does not participate in the investigation. The account will be closed, and a replacement account opened. Non-account holder fraud is investigated by special units within the banks responsible for initiating civil actions and communicating with government law enforcement organizations. Any information that you may acquire related to non-account holder fraud should be reported to your bank.

Disputing Transactions

There are various reasons 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. In the case of a lost or stolen account, the account holder should contact the A/OPC and the bank's customer service representative instead of the merchant. If the account holder and merchant are unable to resolve the dispute, the account holder can dispute a charge by visiting the contractor bank's website, contacting the bank's customer service number, or through the bank's electronic access system (EAS). The account holder will have to provide information including the account number, transaction date, merchant name, transaction amount, account holder signature, and a detailed explanation of the dispute.

All disputes must be reported to the agency's customer service representative within 90 days from the date the transaction was processed. The bank will suspend the disputed charge and immediately provide temporary credit to the account, while investigating the disputed charge by contacting the merchant and requesting a response. A merchant is required to respond to a disputed charge within 21 to 45 days after receipt of the request. If the merchant does not respond within 45 days, the disputed charge will be resolved in favor of the account holder and the merchant will be charged back for the particular goods or services. If the disputed charge is resolved in favor of the merchant, a letter will be sent to the account holder explaining that the charge will appear on their next billing statement.

The A/OPC should monitor disputes filed by account holders. If a transaction is disputed, the AO would not be required to review and approve it. If the bank determines that the account holder did make the purchase legitimately by providing a signed receipt or other evidence of a valid transaction, the charge will appear on the next statement. If the bank determines that the transaction was not proper, the charge will not appear on the next statement. Merchants with a high number of disputes should be watched to determine if they are acting improperly.



Chapter 5: 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 Approving Official (AO) and Agency/Organization Program Coordinator (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 shall reconcile the transactions appearing on his/her monthly statement by verifying their accuracy against account holder records. The account holder shall 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 5-4: 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 designated billing office in a timely manner;
- > Sign account statements on a monthly basis (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 Electronic Access System (EAS) allows AOs to review a 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 as an AO is no exception. Before becoming an AO, one must take the GSA SmartPay Purchase Training 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 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 approving official 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.

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 approving officials are operating within the prescribed policies.

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.

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.

[Appendix 5: Sample Annual Review Process](#)

- [Appendix 5-1: Sample Annual Review Checklist](#)
- [Appendix 5-2: Sample Summary of Findings](#)
- [Appendix 5-3: Sample Certification of Completion of the Annual Review](#)
- [Appendix 5-4: 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 complete 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 6: Indicators of Account Holder Misuse/Fraud

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 Approving Official (AO), Agency/Organization Program Coordinator (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 since 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 4: 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.

Best Practice: Merchant Category Codes (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 3: Merchant Category Codes)

Convenience Checks

Convenience checks are a payment and/or procurement tool intended only for the use of authorized purchases with merchants that do not accept other forms of payment, such as a GSA SmartPay purchase cards. Convenience checks should be used as a payment method of last resort, only when no reasonable alternative merchant is available who accepts a GSA SmartPay purchase account.

If your agency/organization determines a need for convenience checks, your contractor bank will provide a supply of paper 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 and the original for the merchant).

Due to 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, the employee will lose convenience check and purchase account privileges and referred for disciplinary action in accordance with agency procedure.

Convenience checks may not be written for purchases above the micro-purchase threshold as defined in FAR Section 2.1 unless the account holder is a warranted Contracting Officer. In addition, convenience checks may NOT be written to:

- > Vendors who accept another form of payment;
- > Vendor transactions already under another method of acquisition (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 in a check register or log for tracking purposes. The following information must be written on each check:

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

Due to the nature of this product, additional care should be taken in managing accounts with the convenience check feature:

- > Checks should be secured at all times to ensure against physical theft. Checks are negotiable instruments and are to be stored in a locked container, such as a safe or metal filing cabinet. Checks should be accounted for appropriately to prevent loss, theft or potential forgery.
- > The number of accounts and checks on hand should be limited to reduce risk.

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. Due to the cost associated with convenience checks, the number of checks written should be kept to a minimum.

The GSA SmartPay Master Contract requires online access or contractor provided software to enable agencies/organizations to automate their convenience check system. The system shall, at a minimum, provide:

- > The ability to track, add, tally, report and reorder convenience checks,
- > View cleared checks, and
- > Input 1099 information (such as merchant TIN, address).

The **contractor bank** is responsible for:

- > providing a supply of checks to the designated convenience check account holder;
- > processing and paying the checks as they are presented through the bank check-clearing system for payment within established single-purchase limits established by the A/OPC for each individual;
- > Providing a listing of the checks cleared on the monthly billing statement; and
- > Providing hard copies of checks upon request.

The **A/OPC** is 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. The A/OPC must verify that each check issued was both necessary and in compliance with the agency's convenience check policy.

The **account holder** is responsible for recording the date, check number, payee, and amount of each check in their file.

Best Practice: 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?

Convenience Check Alternatives

Convenience checks are actually not convenient after all. They provide thieves with an easy way to commit fraud and they don't offer you the same kinds of consumer protections that other GSA SmartPay solutions do.

Why should I eliminate convenience checks?

- > **Greater refund opportunities for agencies** – Convenience checks don't offer federal agencies refunds, so using them decreases the amount of money your agency will receive through the GSA SmartPay program.
- > **Minimized fraud** – 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.
- > **More streamlined processes** – Electronic payments, like charge cards, help facilitate smoother transactions, enhance transparency, save time and lead to improved data monitoring capabilities.
- > **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.
- > **Increased 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.
- > **Less hassle** – Convenience check transactions must be reported to the Internal Revenue Service 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 Internal Revenue Service 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.

- > **Improved 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.
- > **No adverse effect on mission** – There are many examples of agencies decreasing convenience check usage and still being able to successfully meet their mission.
- > **Fewer 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.

What are some useful alternatives to replace convenience checks?

- > **GSA SmartPay Purchase Charge Card:** All GSA SmartPay charge cards now contain secure microchip technology including contactless and contact (EMV) chip cards.
- > **Cardless Accounts:** Cardless solutions can be customized for large ticket transactions, payments to vendors not traditionally accepting cards, and one-time supplier payments or recurring transactions with a single vendor. These solutions can be a cost effective alternative for streamlining payment processes and earning refunds. Cardless accounts can also help agencies meet sustainability goals as transactions are 100% electronic.
 - Ghost Card
 - Single Use Cards
 - Virtual Cards
 - Electronic Invoice Presentment and Payment (EIPP)
- > **Declining Balance Card:** These cards function similarly to a traditional charge card, however limits do not refresh each month. These cards can be applied for a specific purpose or for a specified time period. Credit limits can either be reset as needed or the card becomes inactive once the balance is used.
- > **Stored Value Card:** Agencies pay a specific dollar amount in advance. These cards can have a single value load (e.g. rebate cards) or can be reloaded on a recurring basis (e.g. payroll cards).
- > **Supplier Finance**
- > **Third Party Payment Systems:** Third Party Payment processors (e.g., PayPal, iBill, etc.) offer e-commerce/internet payment solutions for commercial transactions.



Chapter 7: Electronic Access System/Reporting

An Agency/Organization Program Coordinator (A/OPC) can use the contractor bank's electronic access system (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.

Can the A/OPC setup an account through an EAS?

Yes. To set up an account, applications must be completed for each account holder and approved by the A/OPC. Completed applications can be sent to the contractor bank by EAS (also fax, mail, or e-mail). In emergency cases, an A/OPC can give verbal directions to the bank to set up an account with electronic confirmation to the bank within three business days.

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

Account Activity Report –This report shows all active accounts and the spending for each account during a billing cycle. It provides details on each transaction and allows an A/OPC to sort transactions by transaction date, transaction type, merchant and dollar amount. The Account Activity Report is particularly useful for identifying:

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

Declined Authorizations Report – The Declined Authorization Report 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 limits;
- > That exceeds their monthly purchase limit; or
- > From a merchant that falls under a blocked Merchant Category Code (MCC).

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

Disputes Report – The disputes report identifies date, merchant, reason code, dollar amount, and status of each dispute filed by an account holder. Reviewing the report would identify account holders with excessive disputes. The account holders identified in this report may either require training or may be trying to disguise misuse or fraudulent activity. Approving officials 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, quality issues, or is attempting to commit fraud by submitting false transactions.

Unusual Spending Activity Report – The contractor banks offer various reports identifying transactions that may warrant further review. Please contact your contractor bank for more information on the Unusual Spending Activity Report.

Lost/Stolen Card Report–The lost/stolen card report identifies accounts that are reported lost or stolen. This report may be reviewed to identify account holders who have repeatedly reported their accounts missing. This may either be an indicator that the account holder needs to secure their account or that the account holder is attempting to disguise misuse or fraudulent activity by denying the charges.

Master File – The master file 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 – In addition to the reports listed above, your contractor bank offer a wide range of ad hoc reporting tools. Check with your bank to determine what is available.

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.



Chapter 8: Preventative Measures

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 Agency/Organization Program Coordinator (A/OPC) sets credit limits which 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.

If an A/OPC has a question about a purchase based on the MCC, the A/OPC should discuss the matter with the account holder to determine the nature of the purchase. What may appear to be an inappropriate use of the account actually may be a matter of an erroneous or misclassified MCC. Some merchants operate multiple types of businesses or change the nature of their businesses over time. If a merchant has an inaccurate MCC, the merchant should notify their acquiring bank and request that it be corrected.

Appendix 3: Merchant Category Codes

Agency Policies

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 card;
- > Receipt and acceptance of supplies and services;
- > Reconciling accounts;
- > Review procedures;
- > Span of control for AOs and A/OPCs;
- > Criteria for establishing accounts; and
- > Criteria for deactivating or cancelling accounts with minimal activity.

Define the A/OPC Role

To ensure that all 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 \(24/7\)](#)
- > 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 A/OPC generally serves as the focal point for answering questions, contract administration, coordination of the applications, issuance and destruction of accounts, setting authorizations, establishment and review of reports, and administrative training. Typically, responsibilities include:

- > Maintaining an up-to-date list of account names, account numbers, addresses, email addresses, and phone numbers of all current account holders and accounts.
- > Providing to the contractor bank any changes in their respective organizational structures that may affect invoice/report distribution.
- > Reviewing and evaluating the contractor bank's technical and administrative task order performance and compliance.
- > Resolving technical and operational problems between the contractor and account holders.
- > Taking appropriate action regarding delinquent accounts and reporting to internal investigative units and the GSA Contracting Officer any observed violations of applicable executive orders, laws, or regulations.
- > Participating in training forums and training account holders.
- > Ensuring account holders use their account correctly.
- > Monitoring account activity and managing delinquencies.
- > Ensuring that appropriate steps are taken to mitigate suspension or cancellation actions.

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 (IG) 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.

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.

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 comprised 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 analysis 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. Following is a list of free tools that GSA and the contractor banks offer to agencies:

Managing Your GSA SmartPay Purchase and Travel Program FlipBooks – These interactive guides gives program coordinators an overview of the GSA SmartPay program, 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.

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 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 electronic access systems. 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 onsite training. All Contractor travel and site related costs associated with onsite training shall be borne by the Contractor. In some instances, GSA may provide a site to host this type of training. Contact your implementation/account manager at the 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

In instances when accounts are not needed on a continuous basis, deactivation of the account may serve as a deterrent to fraud or misuse. A/OPCs may deactivate accounts when account holders are not using them. Deactivation/activation can be completed through the bank electronically or by calling customer service. If someone attempts to use a deactivated account, the authorization will be declined. The account is not cancelled and can easily be reactivated by the A/OPC, either electronically or through customer service. If you intend to use this process, be sure you understand any relevant timeframes for reactivation.

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.



Chapter 9: Taking Action

The Agency/Organization Program Coordinator (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 Inspector General (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 if 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);

- > The Federal Bureau of Investigation (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).

Online 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 (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, LinkedIn, and Google + 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, LinkedIn, and Google + 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 Government 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.

For first time visitors to the Acquisition Gateway, please take a brief moment to [register at OMB Max](#). Click [here](#) for a video on the registration process.



Appendixes

Appendix 1: OMB Memorandum M-13-21

- > [Appendix 1-1: Compliance Summary Matrix](#)
- > [Appendix 1-2: Implementation of the Charge Card Prevention Act](#)
- > [Appendix 1-3: Semi-Annual Report on Purchase Card Violations](#)
- > [Appendix 1-4: OMB Circular A-123, Appendix B, Chapter 5.3.2 Narrative Reporting Template](#)

[Appendix 2: S.300 Enrolled OMB Crosswalk document](#)

Appendix 3: Merchant Category Codes

- > [Appendix 3-2: VISA Supplier Locator](#)
- > [MasterCard Quick Reference Booklet](#)

[Appendix 4: Account Holder Fraud Checklist](#)

[Appendix 5: Sample Annual Review Process](#)

- > [Appendix 5-1: Sample Annual Review Checklist](#)
- > [Appendix 5-2: Sample Summary of Findings](#)
- > [Appendix 5-3: Sample Certification of Completion of the Annual Review](#)
- > [Appendix 5-4: Sample Questionable Purchases Form](#)

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:

Phone: (703) 605-2808

E-mail: gsa_smartpay@gsa.gov