GSA SmartPay Fleet Training for Program Coordinators (A/OPCs)

Welcome to the GSA SmartPay online training for fleet Agency/Organization Program Coordinators (A/OPC). As a program coordinator, you play a critical role in your agency's/organization's fleet program. You work with account holders, the bank, and other key stakeholders to ensure that all fleet accounts are effectively managed.

This training module is intended to teach you the basics about your roles and responsibilities as an A/OPC and can be used as refresher training as required by your agency. We encourage you to learn about your agency's specific fleet program requirements and policies, since they will be the foundation of your day-to-day duties.

In addition to this training, the contractor or your agency's bank, also provides an Electronic Access System (EAS) and an A/OPC Guide – these will be invaluable tools for you in performing your duties.

To print or save this training, please follow the following steps:

1. Click below on the "Download Travel Training for A/OPCs PDF" link.
2. Select "Ctrl P" or Print from the menu on your web browser.
3. Select a printer name to print OR select "Adobe PDF" from the dropdown menu to save a copy to your computer.

Download Fleet Training for A/OPCs PDF

- Fleet Program Overview ›

Fleet Program Overview

What is the GSA SmartPay Program?

The GSA SmartPay Program is the largest government charge card and related payment solutions program in the world. The Program has more than three million Purchase, Travel, Fleet, and Integrated accounts and supports more than 560 agencies/organizations. Since the award of the inaugural GSA SmartPay Master Contract in 1998, the GSA SmartPay Program has provided convenient, efficient, and effective payment solutions for the Federal Government, Tribes and Tribal Organizations with a comprehensive portfolio of payment solutions including Purchase, Travel, Fleet, and Integrated charge card services.

In October of 1996, GSA issued a solicitation for commercial fleet payment solution services. The GSA SmartPay Fleet Card Program was included in the GSA SmartPay Master Contract, awarded in 1998. Since then, both the GSA SmartPay 2 and GSA SmartPay 3 Programs include the Fleet business line.

Specific to fleet, the GSA SmartPay program:

- Provides solutions supporting fleet transactions, including Fleet card and non-carded solutions;
- Provides fuel/ maintenance solutions for vehicles, equipment, aviation, small marine vessels and large marine vessels.
- Streamlines ordering, payment and procurement procedures;
- Reduces administrative costs under the simplified acquisition threshold;
- Improves government operations by simplifying the financial process; and
- Allows a platform to improve government operations and accountability.

Through contracts with multiple banks, the GSA SmartPay program enables agencies/ organizations across the Federal Government to obtain payment solutions to support mission needs. The GSA SmartPay Master Contracts, administered by GSA, are fixed price, indefinite delivery/ indefinite quantity (ID/IQ) type contract. The maximum base period for the initial order is four years with three, three-year options.

To participate in the program, Agencies/ Organizations must be eligible to issue a task order against the GSA SmartPay Master Contract. For fleet card accounts, each of the GSA SmartPay contractor banks have contractual relationships with fleet card issuing banks and brands. Your agency awards a task order to one of the GSA SmartPay contractor banks and then selects a specific fleet card issuer such as Wright Express (WEX) or Voyager. Another option is to award to one of the GSA SmartPay contractor banks and use Visa or MasterCard branded cards. Whichever award path your agency has taken, it is through the task order, that card accounts are set-up and managed by A/OPCs. The A/OPC has access to the banks' Electronic Access System (EAS) and also works with the banks to resolve issues and answer questions.

Most fleet accounts are assigned to a vehicle and not a specific account holder, therefore, a creditworthiness assessment is not required for receiving a fleet account. In addition, use of the fleet account will not affect your personal credit history. Any government employee authorized to use the GSA SmartPay program who has a responsibility to make fleet purchases and completes the necessary training is eligible to use a GSA SmartPay fleet charge card.

What are the Benefits to using the GSA SmartPay Master Contract for obtaining payment services?

The GSA SmartPay Program has continued to grow through increased adoption as agencies/organizations realize benefits afforded under the program.

Utilizing the GSA SmartPay 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
- Awards to contractor banks based on a competitive bidding process
- Established relationships with contract banks
- A broad range of flexible products and services for agencies/organizations as well as, the flexibility to add products and services
- Ongoing support for your agency/organizations

Other Benefits include:

- **Universal Acceptance:** Because GSA SmartPay fleet accounts are either WEX, Voyager, MasterCard or VISA brands, they can be used at any merchant that already accepts these types of payment.
- **Refunds:** Agencies receive monetary payments provided by the contractor based on the dollar or spend volume during a specified time period, which result in millions of dollars back per year for the agency.
- **Electronic Access to Data:** The GSA SmartPay contractor banks all provide an Electronic Access Systems (EAS), which provides account access and a variety of reports for A/OPCs to assist in the effective management of the program.

Specific to the GSA SmartPay Fleet Account

Benefits of using the GSA SmartPay fleet account include:

- **Fuel and Maintenance Acceptance**
    - 135,000 fuel providers have account acceptance
    - 45,000 maintenance locations can accept payment under $100 with total acceptance of 500,000 when taking into account MasterCard backup
- **Fraud Monitoring Using Level 3 Data**
    - Program data allows us to monitor and ensure that any fraud or misuse is billed to the responsible party resulting in overall savings to our customer agencies
- **Replacement Card Orders Direct Shipped to Agencies**
    - Decreased potential vehicle downtime by having replacement for lost, stolen, or broken cards shipped directly to the agency
- **Real Time Authorization Data**
    - If there is a problem with the account, the contractor can determine immediately what the problem is and how to complete the transaction
- **Refunds**
    - Receive refunds that result in savings for our customer agencies
- **Tax Recovery**

What is a GSA SmartPay Fleet Account?

A fleet account is a type of payment solution, issued by a GSA SmartPay contractor bank, and used to pay for the purchase of fuel, maintenance and repair of government owned/operated motor equipment, aviation (including airports, airbuses, and associated services), small marine vessels and large marine vessels (including ocean going ships, barges, tugs, dredges, and other marine conveyances that are not required to utilize DLA Energy as the required integrated material manager for bunker fuel and associated services).

Program coordinators/ fleet managers assign fleet accounts to vehicles, which may be used by the Federal Government or other authorized employees to make authorized purchases as determined by the agency/ organization.

Examples of authorized purchases include:

1. Regular unleaded self service fuel
2. Immediately consumable items for vehicles (quart of oil, washer fluid, etc.)
3. Required preventative maintenance
4. Car washes (not to exceed $25 per month or as determined by your agency)
5. Mechanical repairs

Examples of unauthorized purchases include:

- Premium or full service fueling
- Maps, air fresheners, food, etc.
- Buying services in excess of required repairs
- Excessive car washes or details
- Upgrading tires or accessories (may vary depending on specific agency policy)

What is a Centrally Billed Account vs an Individually Billed Account? Why is it important to know the difference?

Because the agency is invoiced for purchases and payments are made directly to the contractor banks by the Federal Government, all fleet accounts are considered **Centrally Billed Accounts (CBAs)**. In contrast, travel cards/accounts and integrated cards/accounts can be either CBAs or IBAs as determined by the agency/organization. **Individually Billed Accounts (IBAs)** are invoiced directly to the account holder and payment is the responsibility of the account holder, who is then reimbursed by the agency/ organization.

The distinction between CBA and IBA is important when determining state tax exemption. **All GSA SmartPay CBAs should be exempt from state taxes.** In addition, with a CBA, the Federal Government accepts liability for charges made by an authorized account holder, but is not liable for any unauthorized use. Unauthorized use means the use of an account by a person, other than the account holder, who does not have actual, implied or apparent authority for such use and from which the account

holder receives no benefit. When the CBA has been used by an authorized account holder to make an unauthorized purchase, the Government is liable for the charge and the agency is responsible for taking appropriate action against the account holder.

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

Be sure to instruct your account holders to report a lost or stolen fleet account promptly to:

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

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

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

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

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

Innovative payment solutions provide agencies/organizations with increased payment

flexibilities and strategies for making payments. Under the GSA SmartPay 3 Master Contract and your agency task order, there are several innovative solutions offered including:

- **Additional Authorization Controls** add value to the GSA SmartPay Program:.
  - Product code dollar limits: Restricting the dollars per designated cycle (e.g., daily, weekly, biweekly, monthly) per product code (e.g., fuel, non-fuel, general merchandise, oil and fluids, parts and service, quicklube, roadside) on each card/account as set by the A/OPC; and
  - Product code daily transaction limit: Restricting the number of transactions designated cycle (e.g., daily, weekly, biweekly, monthly) per product code (e.g., fuel, non-fuel, general merchandise, oil and fluids, parts and service, quick lube, roadside) on each card/account as set by the A/OPC.
- **Additional Data Mining Tools** include being capable of accepting rules-based parameters to indicate specific rules for the data analysis.
- **Additional International Customer Service** provides customer service in other languages.
- **After-Hours Roadside Assistance:** Customer support/service during after hours and holidays

as well as provide after-hours roadside assistance support as required to ensure coordination of the driver's call to the appropriate roadside assistance program.

- **Combined Charge Card and Identification Card Technology** combines payment solutions and personnel identity cards into a single card, such as programming government issued identification cards with payment solution functionality.
- **Commercially Offered Convenience Services** such as extended warranty programs, guaranteed return programs, and merchant discount programs.
- **Chip Cards:** Implementation of chip card for Fleet transactions is not yet available. Upon availability, Contractors must offer chip cards or equivalent enhanced security technology for the Fleet business line at no additional cost.
- **ePayables:** A solution that replaces the accounts payables process such that electronic transactions take place directly between the Government and the supplier. ePayables solutions are typically used with merchants who are either:
    - Traditionally paid by convenience check or EFT or
    - Merchants who do not accept charge card payments (e.g., utility companies)
- **International Fleet Solution:** Products and solutions designed for use outside of the continental United States, Alaska, and Hawaii. Solutions can either utilize a closed loop network that provides Level III data or an open loop network that does not guarantee Level III data.
- **Mobile Application** : The ability to access EAS, pay invoices, receive text/email alerts, and view statement and payment information over a mobile device. Your contractor bank provides mobile application capabilities, upon request, at no additional cost. Mobile application capabilities include:
    - the ability to access EAS,
    - pay invoices,
    - receive text/email alerts and
    - view statement and payment information over a mobile device.
- **Mobile Payments:** The ability to make payments via mobile device at the point-of-sale. Your contractor bank provides the ability for account holders to make secure payments using a mobile device at the point-of-sale.
- **Net Billing:** The process of ensuring that merchant discounts or refunds offered are deducted at the point-of-sale and guaranteeing such discount arrangements. For example, the contractor bank ensures that discount information is identified on the invoice and passed to the agency/organization, when available.
- **Single-Use Account (SUAs):** SUA payment solutions leverage a single virtual account number for each payment. The limit on each account is set to the specific payment amount. Internal controls such as MCC blocks, spend limits, timeframes, and account expiration dates can be used for increased control. Agencies also have the ability to append accounting data for seamless reconciliation. Examples of use include payment invoice and contract payments, which help to ensure that merchants are not able to charge more than approved amounts. Benefits to SUAs include:
    - Accounts can be activated in real time
    - Controls can be placed on account allowing for increased oversight of spend
    - Disposable; one-time use account numbers reduce the risk of fraud
    - Seamless reconciliation, and
    - Reduces the necessity for using convenience checks
- **Software** support other commercial off-the-shelf or customized software that assists the management of GSA and agency/organization level GSA SmartPay Programs including

streamlining government backroom processes (e.g., vouchering, accounts payable), integration with on-site fuel systems (e.g., military bases, national parks, ports) and integration with private alternative fuel systems (e.g., State governments, utilities).

- **Telematics:** Fleet vehicle tracking technology solutions to assist fleet managers in identifying misuse and abuse faster, track drivers and vehicles with factors such as speed as well as global positioning satellite (GPS) location, and reduce fuel consumption and find the lowest gas prices based on GPS location.
- **Tokenization:** Tokenization is the use of a secure, unique "token" in place of a 16-digit account number to provide extra security for transactions.
- **Virtual Cards:** The Contractor shall provide virtual accounts that may be used during a limited time, for a limited amount and possibly for a specific vendor.
- **Ghost Cards:** Ghost Cards are for agencies who frequently do business with one vendor and have recurring payments. An account number can be assigned to the vendor and authorized agency personnel transactions occur without having to use multiple cards or accounts. Many agencies use this product for purchases such as airline tickets. Benefits may include:
    - Reduced number of open accounts (payment processing and oversight easier)
    - Allows for multiple users
    - Allows for a high level of control
    - Reduces the risk of lost or stolen cards

What are Convenience Checks?

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

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

Convenience checks are multi-copied (one copy for the account holder's records; the original for the merchant). 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. That employee will then be referred for disciplinary action in accordance with agency procedure.

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

- Vendors who accept the GSA SmartPay fleet account;
- 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
- The name of the payee
- Amount of the check
- An original signature

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

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

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

- ‹ GSA SmartPay Fleet Training for Program Coordinators (A/OPCs)
- Key Program Participants ›

Key Program Participants

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

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

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

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

1. Setting up accounts and designating authorization controls;
2. Serving as a liaison between account holders and the contractor bank;
3. Providing ongoing advice and assistance to account holders;
4. Maintaining account information;
5. Developing agency policies and procedures, as needed;
6. Auditing fleet accounts as required by your agency policy; and
7. Using the bank's Electronic Access System to perform account management and oversight.

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

- Securing the account;
- Maintaining records relating to all fleet transactions; and
- Using the account ethically and appropriately.

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

- Reconciling invoices;
- Providing feedback to the A/OPC on contractor bank performance;
- Determining whether to pursue faster payment of official invoices in order to take advantage of productivity refunds;
- Providing timely payment to the contractor 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) - The TDO is an individual or office that may be designated by the ordering agency/organization to assist the agency/organization and the contractor bank in tracking and resolving disputed transactions. The TDO oversees the proper processing of transaction disputes and works with the contractor bank to assure a resolution.

EC/EDI Office (EO) - The EO is the focal point for electronic commerce/electronic data interchange (EC/EDI) for the agency/organization. This office also serves as the liaison between the A/OPC, EC/EDI systems staff and the contractor bank. The EO oversees the proper implementation of the agency/organization EC/EDI capabilities and processes.

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

There are four key program participants in the GSA SmartPay program that exist outside of your agency/ organization: (1) the contractor bank, (2) the brand, (3) the merchant community, and (4) the GSA Contracting Officer.

The Contractor Bank's major duties are:

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

The GSA SmartPay Brands are financial institutions that dictate where payments can be processed and facilitate the payment process between account holders, merchants, and issuing financial institutions (for example WEX and Voyager).

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

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

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

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

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

- [‹ Fleet Program Overview](#)
- [Program Coordinator Responsibilities ›](#)

[Program Coordinator Responsibilities](#)

What are my responsibilities as a Program Coordinator?

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

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

Roles may differ with each organization, but could include:

- Managing all agency/ organization GSA SmartPay Fleet Account programs
- Promoting appropriate use of the GSA SmartPay Fleet Accounts
- Monitoring and taking appropriate action for fraud, waste or abuse
- Resolving technical and operational problems between the contractor bank and the fleet account
- Developing agency/ organization fleet-specific program policies and procedures
- Maintaining open lines of communication

Some best practices for fleet managers in effectively managing their GSA SmartPay Fleet Program include:

- Monitor appropriate reports and ensure fleet accounts are paid in a timely manner, to avoid becoming delinquent
- Publish Frequently Asked Questions (FAQs) on the agency/ organization's internal website
- Create a monthly newsletter for agency/ organization fleet policies and procedures

- Develop automated reports to eliminate manually performing data analysis

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

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

How are new accounts set up?

Accounts are established by using information required for each account. As an A/OPC, you are responsible for setting up and maintaining all accounts. Information is supplied by each agency/organization to the contractor bank.

What is the process for renewing fleet accounts?

At least 180 calendar days prior to the expiration of each account, the contractor bank will submit a report to the A/OPC listing each expiring account, containing all information necessary for the agency/organization to renew the account. Fleet Cards used within the past 90 calendar days will automatically renew unless otherwise directed from the A/OPC. If the fleet account has not been used within the past 90 calendar days, the Contractor shall close the account unless a renewal request is received by the A/OPC. Renewed cards will be sent between 20-40 days before the expiration date.

How are accounts closed/terminated and what are the recommended exit procedures?

There are four steps to closing or terminating an account, as follows:

1. Immediately notify the contractor bank when an account is no longer required.
2. Follow the account close out procedures from your contractor bank.
3. Instruct the account holder to destroy/dispose of the card by cutting it into pieces.
4. Review the master file/ account holder listing to ensure the account is closed.

What is my responsibility in the suspension/ cancellation of a fleet account?

As the A/OPC you have the discretion to initiate suspension and/or cancellation procedures for any account; however, you must document the reason for cancellation and/or suspension.

Suspension is the process by which an account is deactivated due to delinquency or multiple pre-suspension actions. An account is considered past due if payment for undisputed principal amounts has

not been received within 45 calendar days from the billing date.

The contractor bank may suspend an account when the account becomes delinquent. Once payment of the undisputed principal amount and Prompt Payment Act Interest is received, the bank is required to reinstate suspended account.

An account can be canceled if an undisputed balance remains unpaid for the prescribed number of calendar days after the date of the statement of account on which the charge first appeared. An account may also be canceled for numerous suspensions.

Can I, as an A/OPC, suspend or cancel an account? Yes. A reason must be documented for suspension or cancellation. Accounts may be cancelled through your bank's electronic access system or through the bank's customer service office.

The following chart may be used as a guide for determining the status of an account.

Calendar Days Past the Payment Due Date	Account Status/Action
45 Days Past Due	Pre-Suspension
61 Days Past Due	Suspension/Pre-Cancellation
126 Days Past Due	Cancellation
180 Days Past Due	Charge Off/Write Off

Please refer to your agency policy for specific delinquency stages.

(For more details on Suspension/ Cancellation Procedures, see the GSA SmartPay 3 Master Contract, Section C.3.3.11 Suspension Procedures and Section C.3.3.12 Cancellation Procedures)

The bank is required to automatically reinstate suspended accounts upon payment of the undisputed principal amount unless otherwise specified by you. You may also notify the bank of any mission-related, extenuating circumstances for which the account should not be suspended within the notification timeframes mentioned previously. Once an account has been cancelled, the contractor bank is under no obligation to reinstate the account.

- ‹ Key Program Participants
- Reporting Tools ›

Reporting Tools

How do I access reports related to the GSA SmartPay fleet program?

Program Coordinators have a number of reporting tools that enable you to manage your fleet program effectively through your contractor bank's Electronic Access System (EAS). To access reports, contact your bank representative to obtain a User ID and password.

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

Program coordinators will also have access through the EAS to monitor account holder transactions at any time. By searching by account number, you can track transactions, as well as view monthly statements. You may also contact the bank's customer service at any time to request information on a specific account.

Note: See the GSA SmartPay 3 Master Contract, Section C.7.1 Electronic Access System for a full list of the EAS requirements.

Best reporting practices for Program Coordinators/ Fleet Managers include:

- Monitoring bank reports regularly, which allows you to oversee the fleet program's financial condition and watch for fraud, waste, and abuse
- Use bank reports proactively, not reactively, for activities such as invoice and payment data and meeting OMB requirements
- Research and understand all reports available to you
- Develop automated reports, specific to the agency/ organization

Which reports provide general account information?

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

- Complete account activity, both active and inactive,
- An agency/organization hierarchy roll-up section,
- Current and past FY account activity,
- Segregates charges and credits by individual or agency/organization accounts with current period totals of the data elements identified, and
- Merchant information such as name, address, and MCC (as applicable).

Specific to fleet, data elements required are:

- Total transactions;
- Total units for the reporting period for each fuel type by unit type;
- Total taxes for each state by tax category;
- Total gross fuel charges for each fuel type;

- Total gross non-fuel charges for non-fuel category;
- Total net fuel charges for each fuel type;
- Total net non-fuel charges for non-fuel category;
- Grand total gross fuel charges;
- Grand total gross non-fuel charges;
- Grand total taxes deducted;
- Grand total net fuel charges; and
- Grand total net non-fuel charges.

The Account Change Report lists any changes made to the master file information and identifies what and when elements were changed. This report is generally used by A/OPCs to manage programmatic data as well as to flag/verify changes.

The Current Accounts Report shows all accounts in alphabetical order and includes all information necessary to identify and contact the account holder. This report is generally used by A/OPCs as an easy reference for account holder identification.

The Exception Report identifies high risk transactions such as lost, stolen, invalid or cancelled accounts, declined transactions and unusual spending activity, and details such transaction activity. This report includes current and past due balances. It is generally used by A/OPCs and the Designated Billing Office (DBO) to monitor account holder activity, track misuse and/or identify training needs of an account holder.

The Master File Report contains master file information on all accounts (e.g., account number, cardholder information, account expiration date, etc.).

The Renewal Report lists accounts due to expire and identifies account name, account number, expiration date, and any other information required to determine renewal status. This report is generally used by the A/OPC to flag expiring accounts.

Which reports are available on transactions, payments, and disputes?

The Detailed Electronic Transaction File lists each account holder's detailed transactions for the reporting period and contains all transaction data. This file is used by the agency/ organization in processing transactions through their financial systems and for reporting purposes.

The Invoice Status Report identifies payment status on each outstanding invoice and includes all transaction data, including the original invoice number and other references required to identify the charge. This report is generally used by the DBO to manage payments and disputes.

The Transaction Dispute Report lists all outstanding and resolved transaction disputes and includes all information necessary to identify, track, balance, and obtain status on the dispute from the original charge through resolution. It is generally used by the Transaction Dispute Office (TDO) to manage disputes.

Which reports provide information on account delinquency?

The Pre-suspension/Pre-cancellation Report lists accounts eligible for suspension or cancellation as defined in the Master Contract, Section C.3.3.11 Suspension Procedures and C.3.3.12 Cancellation Procedures. It identifies account name, account number, status, balance past due, number of days past due, and interest penalty for CBAs.

The Suspension/Cancellation Report lists accounts that have been suspended or canceled as defined in the Master Contract, Section C.3.3.11 Suspension Procedures and C.3.3.12 Cancellation Procedures. It identifies account name, account number, status (suspended or canceled), date of status, balance past due, number of days past due, and interest penalty.

The Delinquency Report lists account status for each 30-120+ day time frame (e.g., 30, 60, 90, 120 or more days).

The Write-off report lists the amount of the write-off and date written off. This report is used by the agency/organization to identify problem areas to better manage delinquencies, to analyze and project programmatic data for the future, and to verify and balance delinquent data in contract reports.

Exception Reports identifies high risk transactions, as defined by the agency/organization, such as declined authorizations, Merchant Category Code (MCC) reports for questionable expenditures, ATM withdrawals, high volume accounts, etc.

Which reports provide statistical or summary information?

The 1057 Report contains summary merchant demographic information (minority, women-owned business, etc.) on a quarterly and cumulative fiscal year basis. It includes the amount of purchase, merchant name, merchant address, merchant demographic information, North American Industrial Classification System (NAICS) code and size standard. This report is generally used by the agency/organization in fulfilling its small business and small disadvantaged business goals.

The Payment Performance and Refund Report lists the payment performance (average payment time) and any refunds paid to the agency/organization level. It includes total net charge volume, payment performance, refund amount, payment method and transaction type (e.g., ePayables, large ticket items). This report is used by the agency/organization to analyze payment performance and refunds as well as for audit purposes. This report includes daily accrual figures and the percentage of potential refunds earned by the agency/ organization along with an explanation of how this figure was derived.

The Statistical Summary Report provides program summary information such as dollar volume, ATM volume, number of transactions, active account holders, total accounts, new accounts, miscellaneous fees, transaction type (e.g. convenience check, ATM, large ticket) and identification of fees (e.g., fees for customized services, fees for convenience checks, fees for value-added product and service offerings) on a current and FY basis.

Specific to fleet, data elements required are:

- Agency/organization;

- Customer account;
- Task order number;
- Fuel sales (purchases made using card);
- Non-fuel sales (purchases made using card);
- Number of fuel transactions;
- Number of non-fuel transactions;
- Miscellaneous charges (line item description);
- Number of active (recently used) accounts;
- New cards issued;
- Number of replacement cards issued;
- Number of cards cancelled;
- Number of cards reported lost;
- Number of cards reported stolen;
- Total customer units (accounts);
- Total new customer units; and
- Total number of cards in inventory.

The Summary Quarterly Merchant Report lists, by FY Quarter, summary spending information by merchant category codes (MCCs) and Product Number/Code. It reports MCC description, number of transactions per MCC, total dollar amount per MCC, and average dollar amount per MCC. This report is used by the agency/organization to summarize supplier categories where the agency/organization dollars are spent, and trend analysis. This report shall also show which MCCs are listed in each template.

The Summary Quarterly Purchase Report provides a summary of purchases under the micro-purchase threshold as described in FAR Part 2.101 Definitions. It also provides a summary of purchases over the micro-purchase threshold. It includes number of transactions, the dollar volume and comparative percentages for the current reporting period and FY activity.

OMB Report: This report provides transaction data required by Chapter 5 – Performance Metrics and Data Requirements of OMB Circular A-123, Appendix B. This report shall include a program type identifier (e.g., Purchase, Travel, Fleet, Integrated). Examples of this transaction data includes, but is not limited to, number of cards, and number of active accounts.

Summary Quarterly Merchant Analysis Report: This report lists, by FY, a detailed quarterly and cumulative summary of the top 100 merchants, by individual merchant, city, state, and service type, in total dollars and total number of transactions. This report is used by the agency/organization to negotiate better discounts with merchants and trend analysis.

Summary Quarterly Merchant Ranking Report: This report lists, by FY, a quarterly and comparative summary by name and type of merchant, ranking the major merchants and their dollar charges, along with a percentage breakdown of totals and changes from the previous quarter as well as the same quarter of the previous year, if applicable. This report is used by the agency/organization for market and trend analysis.

What are my responsibilities for printing and storing reports?

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

What are Ad Hoc Reports?

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

- ‹ Program Coordinator Responsibilities
- Risk Mitigation ›

Risk Mitigation

This section will provide you with information on how you can minimize the risk of misuse or fraud in your GSA SmartPay fleet program. The most important thing you can do is to be aware of what activity is occurring on the accounts under your purview. Do not be afraid to ask questions if you identify unusual or suspicious transactions or behavior.

GSA SmartPay Purchase Account **Misuse/ Abuse** can take many different forms, but here are some of the most common examples:

- Purchases exceed the authorized limit. Accounts may be limited to a specific spending limit per transaction, per day, or per monthly billing cycle.
- Purchases for which no funding is available. Federal law requires that funds must be available before any government purchase is made.
- Using the fleet account for an unauthorized vehicle. Account holders must take steps to ensure the security of their account. This means the fleet account must be used only by an authorized vehicle and only for official government business. If the account holder allows others to use the fleet account, the account holder will be held personally liable to the Government for any unauthorized transactions.

- Split Transactions. The FAR limits the dollar threshold for micro-purchases. Any purchase that, as a whole, would exceed the micro-purchase limit but is separated into smaller transactions in order to avoid the micro-purchase limit is considered to be a split transaction.
- Products or services that do not meet the government's requirements. Account holders must use discretion when making purchases to ensure that they meet the government's requirements. Due to the wide array of products and services available, there may be occasions when account holders may be requested or tempted to buy luxury or deluxe versions of products and services that exceed the government's actual requirements. For instance, it would be questionable for an account holder to buy a $200 car wash when there are many quality car washes available for $50 or less.
- Purchases for personal consumption. All purchases must be for official government use only. Thus, any purchase made that is for the account holder's personal use rather than for official government purposes is considered to be misuse. For example, an account holder who uses the fleet account to buy himself lunch at the gas station because he had no cash available that day is misusing the account.
- Purchases that are not authorized by the agency/organization. Your agency/organization may have additional limits on the use of the purchase account, such as limiting certain categories or types of products or services.

Consequences for misuse/abuse may include:

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

Note: Some agencies have agency-specific penalties and consequences for misuse/abuse of the fleet account.

What is fraud?

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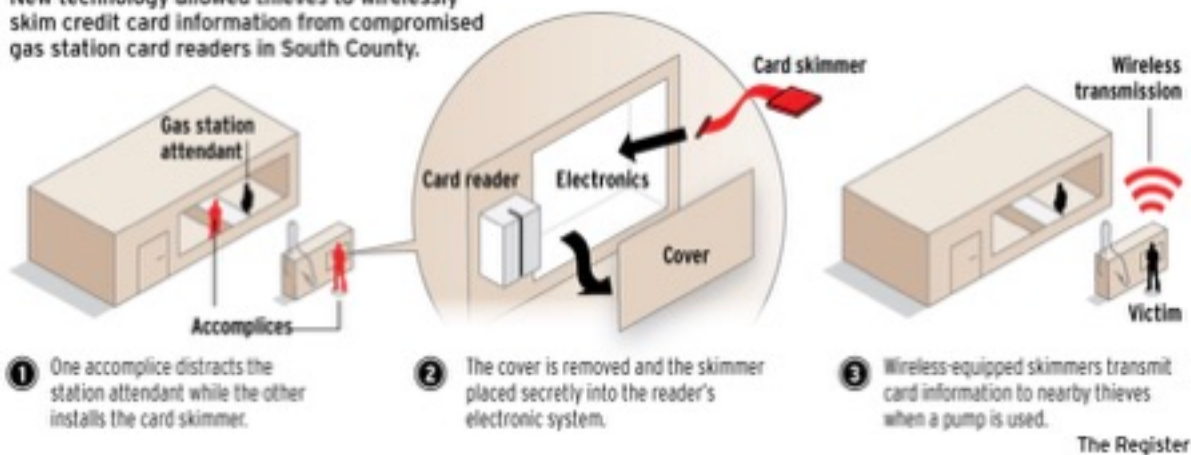
Some of the different types of fraud include:

- Counterfeit Accounts — To make fake cards, criminals use the newest technology to "skim" information contained on magnetic stripes of cards, and also to pass security features (such as holograms).
- Lost or Stolen Accounts — Often physical cards are stolen from an unattended vehicle.
- Non-Receipt Fraud — This occurs whenever new or replacement cards are mailed and then stolen while in transit.
- "Friends and Family" fraud - an employee steals the card and uses it to fuel personal vehicles or

a stranger's vehicle often in return for a discounted cash price

- Phishing — Phishing occurs whenever an account holder receives a fake email directing him or her to enter sensitive personal information on a phony website. The false website enables the criminal to steal information from the account holder.
- Skimming - Account information is stolen at the pump

The next generation of card skimming

New technology allowed thieves to wirelessly skim credit card information from compromised gas station card readers in South County.

Gas station attendant

Card reader **Electronics**

Accomplices

Card skimmer

Cover

Wireless transmission

Victim

❶ One accomplice distracts the station attendant while the other installs the card skimmer.

❷ The cover is removed and the skimmer placed secretly into the reader's electronic system.

❸ Wireless-equipped skimmers transmit card information to nearby thieves when a pump is used.

The Register

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

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

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

What should I do if I suspect misuse or fraud?

A key responsibility for most program coordinators is to detect and report suspected misuse. If a situation occurs where you must report suspected misuse, make sure you have all the information necessary to assist with a formal inquiry or investigation. Contact the driver to obtain any information that could explain questionable charges. If the driver provides documentation or an explanation regarding the charges and you still have questions or concerns about it, compile all the information (e.g., statement, exception report, documented contacts between you and the account holder, copies of receipts, etc.) before you report it. Your agency/organization may ask you to report suspected misuse to one or more of the following personnel:

- The Approving Official

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

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

Program management tools include:

1. **Credit limits -** Credit limits restrict single, daily, weekly, or monthly expenditures per account. In accordance with agency/organization policy, an A/OPC may set the limits which best meet the agency's needs. Setting limits that are realistic, but not excessive, will deter misuse. By reviewing spending patterns, you may be able to lower limits without disrupting the agency's mission. A/OPCs also have the authority to raise limits at any time in response to emergency or unforeseen situations.
2. **Merchant Category Code (MCC) Blocks -** Merchant Category Codes (MCCs) are established by the associations or contractor banks to identify different types of businesses. Merchants select the codes best describing their business. You may limit the types of businesses where the account will be accepted by limiting the MCCs available to the account holder. The contractor bank has established sample templates that may assist you in determining which MCCs should be restricted. In the event that a driver needs to make a purchase outside of his/her restricted MCCs, A/OPCs are authorized to override the restriction for a transaction by contacting the contractor bank's Customer Service Representative. Agency/organization policy should specify who is authorized to perform overrides.
3. **Online Reports -** A/OPCs have access to many standard and ad hoc reports online through the contractor bank's EAS.
4. **Account Deactivation -** In those instances when the fleet account is not needed on a continuous basis, deactivation of the account may serve as a deterrent to fraud and/or misuse. You may deactivate the account when an account is not being used. By understanding the use of the account, you can work establish deactivation guidelines. Deactivation and reactivation can be completed through the bank's EAS or by calling the bank's customer service phone number.

In addition, fleet program coordinators can:

- Establish policies and procedures to detect fraud, waste and abuse
- Emphasise standards of conduct and clearly state consequences for misuse
- Manage delinquency and implement proper training

Drivers can:

- Double check that they are using the correct card before making a purchase
- Keep their Driver ID/ PIN confidential, do not write it on or near the physical card
- Ensure pumps are not compromised or opened
- Use pumps that face the attendant, they are less likely to have skimming devices installed
- Secure the fleet card when stored and don't leave it in the vehicle or in a place accessible to all

How do these tools make it easier to audit and manage the use of fleet

accounts?

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

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

- GSA developed and hosts online training courses
- The annual GSA SmartPay Training Forum for A/OPCs provides training on the bank's EAS, best practices, and program management.
- Free online resources from the [GSA SmartPay website](#) to assist purchase A/OPCs in detecting and preventing misuse and fraud.
- Printable resources such as Helpful Hints for Fleet Account Use is a card-sized brochure that provides information on the fleet account. This brochure can be ordered on online and can be placed in vehicles with the fleet card.

- [‹ Reporting Tools](#)
- [Policies/ Regulations ›](#)

[Policies/ Regulations](#)

What policies apply to Government Owned Vehicles (GOVs)?

Policies and guidance documents that affect the operation and management of federal vehicles come in many forms: advisory bulletins, Government Accountability Office (GAO) Reports, Executive Orders, OMB Circulars, Office of General Counsel guidance, laws, regulations, and agency specific policies.

Listed are a few Federal Regulations to become familiar with:

- **Fleet Management Regulation (§102-34.50)** - Agencies may only obtain the minimum size of motor vehicle necessary to fulfill mission and must obtain motor vehicles that achieve maximum fuel efficiency, limit motor vehicle body size, engine size and optional equipment to what is

essential to meet your agency's mission.

- **Executive Order 13693:** Planning for Sustainability in the Next Decade
    - Reduce federal fleet per-mile greenhouse gas (GHG) emissions by 30% by 2025 from a 2014 baseline
    - By 2020, 20% of new fleet acquisitions must be comprised of zero emissions and plug-in hybrid electric vehicles (Increase to 50% by 2025)
    - Plan for refueling infrastructure that can record vehicle level refueling data
- **Energy Independence and Security Act of 2007 (EISA)**
    - Acquire only low-GHG emitting vehicles with some exceptions
    - MY17 Passenger Cars: 300 g/mile max CO_2 emission (295 for MY18)
    - MY17 Light-Duty Trucks: 375 g/mile max CO_2 emission
- **Energy Policy Act 1992/2005 (EPAct)**
    - 75% of light duty vehicle acquisitions must be alternative fuel vehicles in metropolitan areas

- [‹ Risk Mitigation](#)
- [Resources ›](#)

[Resources](#)

Bank Contact Information

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

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

Wright Express (WEX):

- Customer Service: 1-866-939-4472
- [WEX Online Account Access](#)

Citibank:

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

U.S. Bank:

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

The GSA SmartPay 3 Master Contract

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

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

List of Commonly Used Acronyms

Acronym	Description
AFV	Alternative Fuel Vehicle
A/OPC	Agency/Organization Program Coordinator
AO	Approving Official
DBO	Designated Billing Office
EAS	Electronic Access System
FAR	Federal Acquisition Regulation
GSA	General Services Administration
IG	Inspector General
MCC	Merchant Category Code
OMB	Office of Management and Budget
TDO	Transaction Dispute Office/Official
TIN	Taxpayer ID Number

Acronym	Description
VIN	Vehicle Identification Number

- [‹ Policies/ Regulations](#)
- [Quiz ›](#)