GSA SmartPay®
Supporting your mission

U.S. General Services Administration

Managing GSA SmartPay® Purchase Card Use

A Plan for Success

Table of Contents

Overview 1

Chapter 1: Understanding Cardholder Misuse and Fraud 2

Chapter 2: Understanding Non-Cardholder Fraud 5

Chapter 3: Liability for Purchase Card Transactions 7

Chapter 4: The Review Process 8

Chapter 5: Indicators of Cardholder Misuse or Fraud 10

Chapter 6: Using Reporting Tools to Find Misuse and Fraud 14

Chapter 7: Preventative Measures 16

Chapter 8: Taking Action 20

Chapter 9: Web site Index 21

Chapter 10: Definitions and Acronyms 22

Quick Reference Guide 23

Appendix 1: Sample Annual Review Process 34

Appendix 2: Sample Questionable Purchases Form 44

Overview

The GSA SmartPay® purchase card program provides cards to federal employees to make official government purchases. As the Agency/Organization Program Coordinator (A/OPC) assigned by your agency to oversee the use of the card, detection of misuse/fraud by government employees is your responsibility.

This manual is not a governmentwide policy handbook. Rather, it is intended to serve as an information source for assisting in the oversight role. Use of the card should be in accordance with agency-specific policy.

As used in this guide, the terms "bank" and "contractor" are interchangeable: they represent the three banks awarded contracts under the GSA SmartPay® 2 Master Contract.

Chapter 1: Understanding Cardholder Misuse and Fraud

If an employee in an agency becomes aware of possible misuse of a purchase card, the cardholder 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 cardholder information and would be the first point of contact in most situations.

What is cardholder misuse and fraud?

As a general matter, fraud is the intentional misrepresentation of facts, deceitful practice, or willful device with intent to deprive another of his or her right or to do injury or damage to him or her.

In the case of government purchase cards, intentional use of the purchase card for other than official government transactions constitutes misuse. And depending on the facts, it may involve fraud. The employing agency of a cardholder employee who misuses the card or who participates in fraud may cancel the purchase card and take disciplinary action against the employee, as appropriate. In the case of card misuse, the employee will be held personally liable to the government for the amount of any unauthorized (non-government) transaction.

Additionally, depending on the facts involved, an employee may be subject to fine or imprisonment for action relating to purchase card misuse and fraud. For example, 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. Also, 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 a card have a responsibility to use the card to procure supplies and services at the direction of the agency under official purchase authorization. Examples of misuse include: (1) purchases that exceed the cardholder's limit; (2) purchases not authorized by the agency; (3) purchases for which no funding exists; (4) purchases for personal consumption; (5) purchases that do not comply with the Federal Acquisition Regulation (FAR) and/or other applicable procurement statutes and regulations; and (6) purchases billed by the merchant but not received by the agency.

Consequences

Agencies should establish guidelines and procedures for disciplinary action to be taken against individuals for the improper, fraudulent or abusive use of the purchase card. Purchase card misuse or fraud may have the following potential consequences:

- *Counseling;*
- *Cancellation of purchase card;*
- *Notation in employee performance evaluation;*
- *Reprimand;*
- *Suspension of employment;*
- *Termination of employment; and*
- *Criminal prosecution.*

The purchase card shall be used to purchase supplies and services in accordance with the FAR and agency policy. Purchase card use as the procurement and payment tool for micro-purchases is defined in FAR 13.2. "Micro-purchase" means an acquisition of supplies or services in which the aggregate amount does not exceed $3,000, except that the limit is $2,000 in the case of construction. GSA cardholder training on use of the purchase card may be found on the GSA SmartPay® Web site.

For purchases above the micro-purchase threshold, the purchase card may be used as an ordering and payment mechanism, not a contracting mechanism. When used as an ordering and payment mechanism, contractors may bill against the card. For example, an order has been placed with a contractor on a GSA Federal Supply Schedule for $15,000. The award was made using the ordering procedures in accordance with FAR 8.4. The contractor agrees to accept the purchase card as payment. When the order is delivered, the contractor bills the purchase card 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 card as the ordering and payment mechanism.

Limits on Use

To allow agencies the maximum latitude, the GSA SmartPay® 2 Master Contract excludes only a few categories of purchases, such as long-term rental or lease of land or buildings, travel or travel related expenses (except it may be used for meeting spaces and local transportation services such as Metro fare cards, subway tokens, etc.), and cash advances. Agencies may impose other restrictions on use of the card as well as any exception procedures. The GSA SmartPay 2 Master Contract does not specifically address the maximum transaction amount that may be charged when using the card.

Centrally billed GSA SmartPay accounts cannot be used for private gain. Many GSA SmartPay cardholders have asked whether they can register their GSA SmartPay purchase cards in benefit programs such as Upromise®. The answer is *no*.

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." The purchase card is used to acquire products and services intended for the government's use, and charges made on the card are paid for with government funds. Government purchase cardholders who register their GSA SmartPay purchase cards with these networks are using their public office for private gain and are therefore in violation of ethics rules. If you or your cardholders have questions about ethics rules, please contact your agency Ethics Official (usually, an attorney in your Office of General Counsel).

Chapter 2: Understanding Non-Cardholder Fraud

Non-cardholder fraud involves the use of the purchase card or cardholder data by an unauthorized person. The risk of non-cardholder fraud is higher in certain situations including:

Card never received – A new or replacement card has been mailed to the cardholder but was not received. Due to the possibility that the card could have been intercepted by a third party, the account will be cancelled by the bank upon notification from the cardholder. A new card with a new account number will be issued. Each cardholder will be required to activate his or her card by phone once they receive it.

Lost card –The cardholder reports that the card as misplaced or lost. 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 cardholder prior to reporting it lost. The cardholder may be required to sign an affidavit confirming the card was lost. If transactions not made by the cardholder appear on the statement, the cardholder 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). A Cardholder may forfeit his or her rights to dispute if the form is not sent in within 90 days.

Stolen card – The cardholder reports the card as stolen. The account will be closed, and a new card will be issued. Reporting the card as stolen does not relieve the government of payment for any transactions that were made by the cardholder prior to reporting it stolen. The cardholder may be required to sign an affidavit confirming the card was stolen. If the cardholder did not make the transactions appearing on the cardholder statement, the cardholder must submit a dispute form to the bank within 90 days from the date the transaction was processed. Failure to submit the dispute form and/or affidavit could result in liability to
the government.

Altered or counterfeit cards – These types of cards are normally identified by the bank's authorization process or by the cardholder when he or she receives his or her statement. Third parties obtained account information and used that information to make purchases with an altered or counterfeit card. If the banks recognize a fraudulent pattern of use at the time of authorization, the bank will validate the use of the card with the cardholder and/or suspend the card. The cardholder may be asked to sign an affidavit verifying that the transactions were fraudulent. If the cardholder did not make transactions appearing on the cardholder statement, the cardholder must submit a dispute form to the bank within 90 days from the date the transaction was processed. Failure to submit the dispute form and/or affidavit could result in liability to the government.

Account takeover – This may be known as identity theft. In this case, the cardholder's identity has been compromised, and a third party requested a new card by providing confidential information about the cardholder. Any cardholder who believes that he or she may have been subject to identity theft should contact the bank's customer-service department.

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-cardholder 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-cardholder fraud should be reported to your bank. Cardholders should contact customer service at the toll-free number provided on the back of the card to report any suspected fraud.

Chapter 3: Liability for Purchase Card Transactions

The GSA SmartPay® 2 Master Contract clearly defines liability for purchase card transactions. Liability for transactions made by authorized cardholders rests with the government. If the card is used by an authorized cardholder to make an unauthorized purchase, the government is liable for payment and the agency is responsible for taking appropriate action against the cardholder. Use of the card by a person other than the cardholder, who does not have actual, implied, or apparent authority for such use and for which the cardholder receives no benefit, is not the liability of the government. If it is discovered that someone other than the cardholder has used the card, it should be reported immediately to the A/OPC and the bank's customer service representative.

Under the terms of the GSA SmartPay 2 Master Contract, liability of the government for lost or stolen cards shall not exceed the lesser of $50 or the amount of money, property, labor, or services obtained before notification to the contractor. The contractor and the Agency/Organization Program Coordinator (A/OPC) are to be notified when it becomes evident that a card has been lost or stolen. Cards that have been reported lost or stolen are blocked immediately. The contractor will issue the cardholder a new card with a new account number. After the cardholder reports a lost or stolen card, the contractor will send the cardholder a letter explaining the steps that need to be taken. The cardholder should follow the instructions in that letter to mitigate liability for any unauthorized transactions. Unauthorized transactions may appear on the cardholder statement even though the card has been reported lost or stolen. If unauthorized transactions appear on a cardholder statement, the cardholder should contact the bank's customer-service department.

Chapter 4: The Review Process

Given that the agency is liable for unauthorized purchases by an authorized cardholder, agency purchase card 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. Level 1 review by the AO and/or A/OPC, including first hand knowledge of the type of products and services authorized by the organization, is the first line of defense.

Cardholder

At the end of each billing cycle, the cardholder shall reconcile the transactions appearing on his/her monthly statement by verifying their accuracy against cardholder records. The cardholder shall review all information on the monthly statement, verifying charges, credits, outstanding disputes, and refunds.

Approving Official (AO)

The AO is responsible for ensuring that all purchases made by the cardholder(s) within his/her responsibility were appropriate and the charges are accurate. He/she must resolve all questionable purchases with the cardholder. In the event an unauthorized purchase is detected, the AO must notify the A/OPC and other appropriate personnel in accordance with agency policy After review, the AO will sign the account statement and maintain the documentation in accordance with agency procedures. As designated by the agency, the AO may also be responsible for certifying the monthly invoice resulting from the purchases/transactions of the cardholders within his/her account structure.

The number of cardholders and the volume of transactions for which an approving official is responsible need to be reasonable, so that the official may conduct reviews in a timely manner. Timely reviews of transactions are necessary to ensure detection of possible cases of card misuse and fraud.

The number of cardholders assigned to an AO should be reasonable, considering the volume of cardholder activity and the organizational structure. The AO should have direct knowledge of the cardholder's role in the agency and the ability to verify receipt of the purchase. In situations where cardholder use is infrequent, more cardholders could be assigned to the AO.

Agency/Organization Program Coordinator (A/OPC)

A/OPC reviews of the purchase card program must be accomplished to ensure adequate local internal controls are in place. The review should consist of an evaluation of local operating procedures to ensure that cardholders 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 on a random basis. A sample checklist for an annual review is included in Appendix 1.

Best Practice: Cardholders should use a standardized form to provide additional information to A/OPCs on questionable transactions (see Appendix 2).

Who Should Have Cards?

There is no right number of cardholders for your agency. In certain circumstances, a large number of cardholders may be required to accomplish the mission of the agency. The risk of issuing more cards must be weighed against the need for more cardholders. A regular review of account activity will identify accounts with little or no activity. You should review use and close accounts that are no longer needed.

Best Practice: A/OPCs are encouraged to review the number of cardholders as part of the Annual Review Process. Cards with little or no activity should be considered for cancellation.

Separation of Duties

Agency policy should include direction regarding separation of duties to minimize the risk of fraud and/or loss of property. In particular, responsibilities of cardholders, 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 cardholder statements, making payments, certifying funding, and reviewing or 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, training, etc., to ensure they can successfully perform their duties.

Chapter 5: Indicators of Cardholder Misuse or Fraud

Some simple things to keep in mind when looking at transactions:

- *Card misuse and cases of fraud often start small and may not stop after only one action. No matter how small the misuse or fraud, it should be addressed immediately to prevent any future occurrences.*
- *Cards must only be used by the cardholder. If the cardholder is not directly involved in the transaction, there is greater risk that fraud will be committed.*
- *Cardholders should be able to provide documentation of purchases, such as invoices, receipts, etc. when requested by the Approving Official (AO), Agency/Organization Program Coordinator (A/OPC), or auditors.*
- *Ensure that cardholders certify transactions promptly. Prompt certification allows for prompt remedial action in the event of misuse or fraud.*
- *Random reviews of cardholder records by the A/OPC will discourage misuse and fraud since cardholders, 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.*

The checklist on page 11 is provided to highlight indicators that may point to cardholder fraud. It is important to understand that these are indicators only. As such, they must be investigated further with the cardholder or other individuals.

Merchant Category Codes (MCCs) are often used to highlight transactions requiring further investigation. While a transaction with a merchant in a questionable MCC (see the Quick Reference Guide) may initially raise questions, further investigation may reveal that the transaction was a legitimate purchase or that the merchant was misclassified.

	Issue	Yes	No	Comments
1.	Does the transaction fall within a bolded merchant category code in the MCC table?			
2.	Does the merchant name appear to be outside the cardholder's general area of responsibility?			
3.	Does the cardholder have several transactions with the same merchant within a short time frame, and does the amount of the transactions total more than $3,000?			Possible split transactions
4.	Has the account been closed due to fraud and a new card issued?			
5.	Has the cardholder disputed transactions on a frequent basis?			
6.	Has the cardholder had multiple declined authorizations?			Cardholder traning recommended
7.	Does the cardholder have transactions (authorizations) occurring on non-working days (e.g., weekends)?			
8.	Does the cardholder have higher-than-normal expenditures during the billing cycle?			
9.	Has the dollar limit on the account been raised during the billing cycle?			A/OPC review recommended
10.	Has the contractor been debarred (see https://www.epls.gov/ for listing) by the federal government?			
11.	Is the cardholder unable to provide proofs-of-purchase such as receipts?			
12.	Does the cardholder have multiple transactions of even dollar amounts (e.g., $20, $100)?			
13.	Has the cardholder allowed others in the office to use his/her card for making purchases?			
14.	Does the cardholder have recurring purchases of a high dollar value?			
15.	Does the cardholder have transactions with two merchants with two different names but same address and owner?			
16.	Does the cardholder repeatedly do business with the same merchants (minimal rotation)?			
17.	Does the cardholder make repeated purchases close to his/her single purchase limit?			
18.	Does the cardholder consistently hit his/her monthly limit?			
19.	Does the merchant address appear to be a home address?			

Convenience Checks

Some agencies allow for the use of convenience checks. Convenience checks are a payment and/or procurement tool intended only for the use with merchants that do not accept purchase cards and for other authorized purposes where charge cards are not accepted. Convenience checks should be used as a payment method of last resort, only when no reasonable alternative merchant is available who accepts the charge card.

If your agency/organization determines a need for convenience checks, your purchase charge card contractor bank will provide a supply of checks to the designated cardholder drawn on the cardholder's purchase charge card account. The checks will be processed as they are presented for payment. Convenience checks are multi-copied (one copy for the cardholder'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 card 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 micropurchase limits as defined in FAR Section 2.1. In addition, convenience checks may NOT be written to:

- *Vendors who accept the purchase card;*
- *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 he 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 should be limited to reduce risk.*
- *The number of checks on hand should be limited to reduce risk.*
- *Before a check is issued, every reasonable effort should be made to use the purchase card. Maximum efforts should be made to find and use vendors who accept the purchase card. Due to the cost associated with convenience checks, the number of checks written should be kept to a minimum.*

The GSA SmartPay® 2 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, as well as input 1099 information, such as merchant TIN, address, etc. The bank will: (1) provide a supply of checks to the designated convenience check account holder, (2) process and pay 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, and (3) provide a listing of the checks cleared on the monthly cardholder statement.

Hard copies of checks are generally available 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 cardholder should record in his/her files the date, check number, payee, and amount of each check.

Chapter 6: Using Reporting Tools to Find Misuse and Fraud

An Agency/Organization Program Coordinator (A/OPC) can use the servicing bank's electronic access system in order to generate agency reports as a means of detecting 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. 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, including transaction date, transaction type (credit, debit, convenience check, etc.), merchant name, and dollar amount. This report allows an A/OPC to sort transactions by dollar size, merchant, date, or type. 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 cardholders who have attempted to use a card 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).*

If a cardholder consistently has declined authorizations, the A/OPC should take action by providing additional training or making a change to the cardholder authorization controls or dollar limits.

Disputes Report – The disputes report identifies date, merchant, reason code, dollar amount, and status of each dispute filed by a cardholder. Reviewing the report would identify cardholders with excessive disputes. These cardholders 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. Cardholders should attempt to resolve disputes directly with merchants prior to filing a disputes report. If a merchant is consistently appearing on the disputes report, the A/OPC should 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 banks offer various reports identifying transactions that may warrant further review. These reports vary by bank.

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

Master File – The master file should be reviewed periodically to eliminate cardholders who are no longer employed in the agency, correct addresses, and verify whether card limits and authorization controls are appropriate.

Ad Hoc Reports – The banks offer a wide range of ad hoc reporting tools. Check with your bank to determine what is available.

Best Practice: Place ad hoc reports in a shared folder so all A/OPCs can access them. This saves A/OPCs from developing reports and ensures consistency across the organization.

Chapter 7: Preventative Measures

Credit Limits

Credit limits can be set up to restrict single-purchase or daily/weekly/monthly expenditures by the cardholder. 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 cardholder misuse. By reviewing cardholder 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 Level 1 A/OPCs may raise limits according to agency policy.

Merchant Category Code (MCC) Blocks

MCCs are established by the bankcard associations or banks to identify different types of business*. Merchants 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 cardholder. The bank has established sample templates that may assist in determining which MCCs should be restricted. In the event that a cardholder needs to make a purchase outside of his/her 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 cardholder to determine the nature of the purchase. What may appear to be an inappropriate use of the card 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 his or her acquiring bank and request that it be corrected.

**A sample list of MCCs is located on page 30 in the Quick Reference Guide.*

Agency Policies

Policy will vary from agency to agency, based on mission considerations. It is recommended that agency policies address the following areas to ensure that clear guidance is provided to A/OPCs, AOs and cardholders:

- *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

Each agency should include a list of A/OPC duties and responsibilities in its written policy and A/OPC training materials to ensure that all parties understand their role. This is particularly important in situations where there is frequent turnover of A/OPCs. Contractor provided A/OPC guides can assist agencies in training their A/OPCs.

The A/OPC generally serves as the focal point for answering questions, contract administration, coordination of the applications, issuance and destruction of cards, 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, e-mail addresses, and telephone numbers of all current cardholders and accounts.*
- *Providing to the contractor(s) any changes in their respective organizational structures that may affect invoice/report distribution.*
- *Reviewing and evaluating the contractor's technical and administrative task order performance and compliance.*
- *Resolving technical and operational problems between the contractor and cardholders.*
- *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 conferences and training cardholders.*
- *Ensuring cardholders use the card program correctly.*
- *Monitoring account activity and managing delinquencies.*
- *Ensuring that appropriate steps are taken to mitigate suspension or cancellation actions.*

The A/OPC is the eyes and ears of the organization. The A/OPC's role is of extreme importance to the agency.

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.*

A strong bond between the purchase card program office and the IG's office is the key to successful management of your card 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 purchase card office should work with the IG to gather data on completed investigations so that preventive measures can be addressed in agency purchase card policy.

Joint Agency Coordination

Joint agency coordination is important because fraud and abuse found through investigations in one agency could uncover and/or prevent similar situations occurring in another agency. The types of criminal acts involved in purchase card 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 card investigations, but also to conduct proactive analysis of purchase card activity. The FBI provided space with computers in order to download and compile purchase card 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 card program; however, some agencies may require supplemental training to address agency specific issues. Following is a list of free tools that GSA and/or the contractors offer to agencies:

Managing GSA SmartPay Purchase Card Use –The guide addresses issues of concern to the A/OPC, including responsibilities of program participants, account setup and maintenance, account suspension/cancellation, disputes, reports, and invoicing procedures. The guide is available from your contractor as a hard copy or electronically.

A/OPC Online Training – GSA designed this online training for purchase charge card A/OPCs. Online training can be found on the the GSA SmartPay training website https://training.smartpay.gsa.gov.

Annual GSA SmartPay® Training Conference – GSA sponsors an annual conference to train A/OPCs on account administration, program management, reports, and electronic access systems. In addition to A/OPCs, the conference is beneficial for approving and billing officials, inspectors and auditors. Information regarding the conference may be found at http://www.gsasmartpayconference.org.

Cardholder Guide –The cardholder guide addresses authorized uses of the card, disputes, and billing. This guide can be requested through your bank.

Purchase Cardholder Online Training – GSA designed this course to provide cardholders basic information needed to make official purchases. It is available online by going to the GSA SmartPay training website: https://training.smartpay.gsa.gov.

Deactivation

In instances when cards are not needed on a continuous basis, deactivation of the card may serve as a deterrent to fraud or misuse. A/OPCs may deactivate cards when cardholders 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 card, the authorization will be declined. The card 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

The banks can provide transaction files in an electronic format to agencies. With receipt of electronic transaction data, an agency has the option of reviewing cardholder 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 cardholder misuse and fraud must be documented and understood.

Chapter 8: Taking Action

As the Agency/Organization Program Coordinator (A/OPC), you have the responsibility to report any suspected or actual fraud to the appropriate authorities within the government.

If fraud by a cardholder, merchant, or other third party is suspected, an A/OPC can file a complaint with his/her 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 cardholders are aware of the hotline number. Be as specific as possible when calling or sending in a complaint. If the complaint relates to a cardholder, as an A/OPC, you 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 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).*

Chapter 9: Web Site Index

http://www.usoge.gov/

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

https://smartpay.gsa.gov

The GSA SmartPay® Web site provides a copy of the GSA SmartPay® 2 Master Contract, contractor guides, performance summaries, online training, and a list of agency representatives who can answer questions.

https://training.smartpay.gsa.gov

The GSA SmartPay training website provides training to both cardholders and Agency Program Coordinators (purchase and travel).

www.statebuy.state.gov

This Web site provides policy and operational guidance, as well as other related resources for Department of State, USAID, USIA, and the Peace Corps (includes both domestic and overseas activities).

https://www.navsup.navy.mil/ccpmd/purchase_card

This Web site displays policy and related links for the Department of the Navy purchase card program.

http://dodgpc.us.army.mil/

This Web site displays policy and operational guidance for Department of Defense (DOD) purchase card program.

www.dodig.mil

This Web site displays information on the scope of responsibility and leadership offered to prevent and detect fraud and abuse in programs through the Office of the Inspector General.

www.dscc.dla.mil/offices/base

This Web site was developed to provide program participants with access to information that will assist them in complying with all regulatory requirements and instructions received from DoD, DLA and DSCC.

https://www.acquisition.gov/far/

The Federal Acquisition Regulation (FAR) was established to codify uniform policies for acquisition of supplies and services by executive agencies. It is issued and maintained jointly, pursuant to the OFPP Reauthorization Act under the statutory authorities granted to the Secretary of Defense, the administrator of General Services Administration, and the administrator of National Aeronautics and Space Administration.

Chapter 10: Definitions and Acronyms

Definitions

Agency/Organization Program Coordinator (A/OPC) –The A/OPC generally serves as the focal point for answering questions, task order administration, establishing and maintaining accounts, and issuance and destruction of cards. Only the A/OPC is authorized to request the contractor establish new accounts. The A/OPC oversees the card program(s) for his or her agency/organization and establishes guidelines. Changes to authorization controls must be submitted to the contractor by the A/OPC.

Approving Official (AO) – An individual tasked with reviewing the transactions of cardholders to assure proper use of the purchase card. AOs make sure that purchases are necessary for accomplishing the mission of the agency. They may also be known as reviewing or certifying officials.

Cardholder – Any individual or agency/organization component designated by the agency/organization to receive a card.

GSA SmartPay® / GSA SmartPay®2 – Contracts managed by GSA to provide fleet, travel, purchase and integrated charge cards to federal agencies/organizations.

Purchase Card – A type of charge card issued by a GSA SmartPay 2 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.

List of Acronyms

A/OPC: Agency/Organization Program Coordinator

DSCC: Defense Supply Center Columbus

OFPP: Office of Federal Program Procurement Policy

AO: Approving Official

FAR: Federal Acquisition Regulations

UCMJ: United Code of Military Justice

AFOSI: Air Force Office of Special Investigation

FBI: Federal Bureau of Investigation

USACI: U.S. Army Criminal Investigation

DCIS: DOD Criminal Investigative Service

IG: Inspector General

USAID: U.S. Agency for International Development

NCIS: Naval Criminal Investigative Service

USC: U.S. Code

USIA: U.S. Information Agency

Quick Reference Guide

Contract Specific Information

This Quick Reference Guide provides an A/OPC with a consolidated look at the GSA SmartPay® 2 Master Contract. This guide will help you answer questions about contract terms and conditions and what your roles and responsibilities are as a purchase card A/OPC.

What is the scope of the GSA SmartPay 2 Master Contract?

The scope of the GSA SmartPay 2 Master Contract is to provide a worldwide procurement, payment, and functional data-storage mechanism to support authorized purchases, expenses, and/or streamline purchase and payment systems for the fleet, travel and purchase card programs, as well as an integrated solution. All financial, management, and administrative products and services (current and emerging), which assist in the support of authorized purchases, expenses, and/or streamline purchase and payment systems, fall within the scope of this contract. Additional requirements may be included in the task order issued to your bank.

What are the purposes of the Governmentwide Purchase Card Program?

The purpose of the purchase card program are to:

- *Provide commercial charge cards and associated services in support of official government purchases;*
- *Streamline ordering, payment and procurement procedures, and reduce administrative cost 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 card?

The GSA SmartPay® 2 Master Contract is a fixed price, indefinite delivery, indefinite quantity (IDIQ) task order contract. The contract period for GSA SmartPay 2 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.

What is a Centrally Billed Account?

A Centrally Billed Account (CBA) is a card/account established by the contractor at the request of the agency/organization or their designee. These accounts may be card/ cardless and payments are made directly to the contractor by the agency/organization or their designee. All purchase cards are set up under a centrally billed account.

How can my agency utilize Purchase Card Services?

The agency's chief financial officer, chief administrative officer, and procurement executive decide which bank will be issued a task order to provide purchase cards 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.

What are the basic roles and responsibilities as the ... ?

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

A/OPC – An A/OPC shall have the overall responsibility for the purchase card program within his/her agency/ organization. The A/OPC generally serves as the focal point for:

- *Answering questions*
- *Contract administration*
- *Coordination of applications*
- *Issuance and destruction of cards*
- *Establishment and review of reports*
- *Administrative training*
- *Establishment of guidelines for the agency/cardholder*
- *Monitoring fraud and misuse within their program*

Cardholder – Cardholders are responsible for:

- *Understanding their respective agency's policies and procedures regarding the use of a purchase card;*
- *Using the card for authorized purchases;*
- *Reporting lost or stolen card;*
- *Keeping a record of purchases;*
- *Reconciling account; and*
- *Disputing transactions in accordance with the bank's policy.*

AO –The approving official is responsible for:

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

What online tools are available to the A/OPC?

The contractor will provide an electronic access system in order for the A/OPC to implement, manage, receive and complete all reporting requirements. The electronic access system 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.

How are accounts set up and cancelled?

The A/OPC is responsible for the set up and maintenance of all accounts. Account set up forms must be completed for each cardholder and approved by the A/OPC. You can acquire the account set-up forms from your official A/OPC guide or from your bank's Web site. Completed account forms can be sent to the bank by fax, mail, e-mail, or the bank's electronic access system. In emergency cases, an A/OPC can give verbal directions to the bank to set up an account with electronic/written confirmation to the bank within three business days. Setting up a convenience check account may also be accomplished by completing a bank-provided form.

When can the bank suspend an account?

The bank shall notify the A/OPC and the Designated Billing Office (DBO) requesting payment on 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.

When can the bank cancel 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.

What items cannot be purchased with the card?

It is the A/OPC's responsibility to coordinate, establish, set up, and understand his or her agency's policies and procedures regarding the definition of authorized purchases. However, the GSA SmartPay® 2 Master Contract specifies that the following items shall *not* be purchased with the purchase card:

- *Long-term rental or leasing of land or buildings;*
- *Travel or travel related expenses (except the purchase card may be used for meeting spaces, and local transportation services, e.g., Metro fare cards, subway tokens, etc.); and*
- *Cash advances.*

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/organization designee. The contractor 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.

Disputing Transactions

There are various reasons for disputing transactions including:

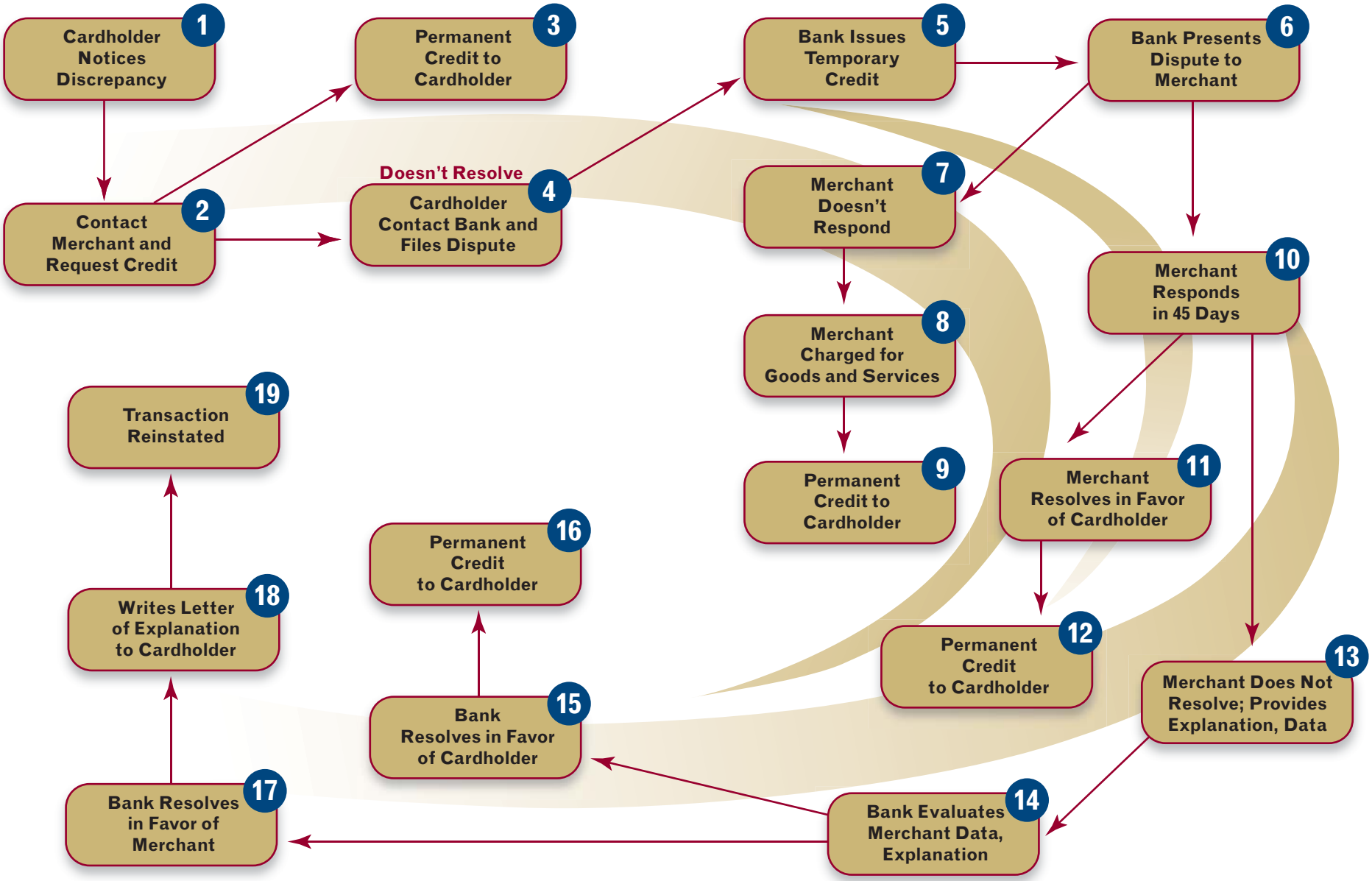
- *Unauthorized or incorrect charges;*
- *Charges for merchandise that has not been received;*
- *Charges for returned merchandise; and*
- *Statement does not include credits for which the cardholder has been issued a credit slip.*

In most cases, the cardholder 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 cardholder and the merchant. In the case of a lost or stolen card, the cardholder should contact the A/OPC and the bank's customer service representative instead of the merchant. If the cardholder and merchant are unable to resolve the dispute, the cardholder can dispute a charge by visiting the bank's Web site, contacting the customer service number, or accessing the bank's electronic access system. The cardholder will have to provide information including the account number, transaction date, merchant name, transaction amount, cardholder 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 cardholder 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 cardholder explaining that the charge will appear on his or her next statement.

The A/OPC should monitor disputes filed by cardholders. If a transaction is disputed, the AO would not be required to review and approve it. If the bank determines that the cardholder 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.

Dispute Resolution Process



Merchant Category Codes

0742 Veterinary Services
0763 Agricultural Cooperative
0780 Landscaping Services
1520 General Contractors
1711 Heating, Plumbing, AC
1731 Electrical Contractors
1740 Masonry, Stonework, Plaster
1750 Carpentry Contractors
1761 Roofing/Siding, Sheet Metal
1771 Concrete Work Contractors
1799 Special Trade Contractors
2741 Misc. Publishing, Printing
2791 Typesetting, Plate Making
2842 Specialty Cleaning
3000 Airlines, Air Carriers
3351 Car Rental Agencies
3501 Hotels, Motels, Resorts
4011 Railroads
4111 Commuter Transp, Ferries
4112 Passenger Railways
4119 Ambulance Services
4121 Taxicabs/Limousines
4214 Trucking/Freight Carriers
4215 Courier Services
4225 Public Warehousing
4411 Cruise Lines
4457 Boat Rentals and Leases
4468 Marinas, Service and Supplies
4511 Airlines, Air Carriers
4582 Airports, Flying Fields
4722 Travel Agencies, Tour Oper
4723 TUI Travel - Germany
4761 Transportation/Travel
4784 Tolls/Bridge Fees
4812 Telecommunication Equip
4814 Telecom Serv/Fax
4815 VisaPhone
4816 Computer Network Services
4821 Telegraph Services
4829 Wires, Money Orders
4899 Cable/Pay Television
4900 Utilities
5013 Motor Vehicle Supplies
5021 Office Furniture
5039 Construction Materials
5044 Photographic Supplies
5045 Computer Equipment
5046 Commercial Equipment
5047 Medical/Dental Equipment
5051 Metal Service Centers
5065 Electrical Parts/ Equipment
5072 Hardware Equip/Supplies
5074 Plumbing/Heating Supplies
5085 Industrial Supplies
5094 Precious Stones and Metals
5099 Durable Goods
5111 Stationery/Office Supplies
5122 Drugs and Proprietaries
5131 Piece Goods, Notions
5137 Uniforms
5139 Commercial Footwear
5169 Chemicals/Allied Products
5172 Petroleum and Products
5192 Books/Periodicals/Papers
5193 Florists Supplies, Flowers
5198 Paints, Varnishes, Supplies
5199 Nondurable Goods
5200 Home Supply Warehouses
5211 Lumber, Building Materials
5231 Glass, Paint, Wallpaper
5251 Hardware Stores
5261 Lawn and Garden Supplies
5271 Mobile Home Dealers
5300 Wholesale Clubs
5309 Duty Free Stores
5310 Discount Stores
5311 Department Stores
5331 Variety Stores
5399 Misc. General Merchandise
5411 Grocery, Supermarkets
5422 Freezer, Meat Locker
5441 Candy, Nut Stores
5451 Dairy Products Stores
5462 Bakeries
5499 Misc. Food Stores
5511 Auto/Truck Sales, Serv, Repr
5521 Auto/Truck Dealers
5531 Auto and Home Supply
5532 Automotive Tire Stores
5533 Auto Parts, Accessories
5541 Service Stations
5542 Automated Fuel Dispensers
5551 Boat Dealers
5561 Camper Dealers
5571 Motorcycle Shops/Dealers
5592 Motor Homes Dealers

5598 Snowmobile Dealers
5599 Misc. Auto Dealers
5611 Men's/Boy's Clothing
5621 Women's Ready-to-Wear
5631 Women's Accessories
5641 Children's/Infants' Clothing
5651 Family Clothing Stores
5655 Sports Apparel
5661 Shoe Stores
5681 Fur Stores
5691 Clothing Stores
5697 Tailors, Alterations
5698 Wig and Toupee Stores
5699 Misc. Apparel Stores
5712 Furniture, Excl Appliances
5713 Floor Covering Stores
5714 Drapery/Upholstery Stores
5718 Fireplace Accessory Stores
5719 Misc Home Furnishings
5722 Home Appliance Stores
5732 Electronic Sales
5733 Music Stores
5734 Computer Software Stores
5735 Record Shops
5811 Caterers
5812 Eating Places, Restaurants
5813 Drinking Places
5814 Fast Food Restaurants
5912 Drug Stores, Pharmacies
5921 Package Liquor Stores
5931 Used Merchandise
5932 Antique Shops
5933 Pawn Shops
5935 Wrecking/Salvage Yards
5937 Antique Reproductions
5940 Bicycle Shops
5941 Sporting Goods Stores
5942 Book Stores
5943 Stationery/Office Supplies
5944 Jewelry Stores
5945 Hobby, Toys and Game Shops
5946 Camera and Supplies
5947 Gift, Card, Novelty Shops
5948 Luggage, Leather Shops
5949 Sewing/Fabric Stores
5950 Glassware/Crystal Stores
5960 Direct Mrktg - Insurance Serv
5962 Direct Marketing - Travel
5963 Door-to-Door Sales
5964 Direct Mktg – Catalog
5965 Direct Mktg Catalog, Retail
5966 Direct Mktg – Outbound Tele
5967 Direct Mktg – Inbound Tele
5968 Direct Mktg – Subscription
5969 Direct Mktg – Other
5970 Artists' Supplies, Crafts
5971 Art Dealers and Galleries
5972 Stamp and Coin Stores
5973 Religious Goods Stores
5975 Hearing Aids
5976 Orthopedics, Prosthetics
5977 Cosmetic Stores
5978 Typewriter Sales, Rent, Serv
5983 Fuel Dealers
5992 Florists
5993 Cigar Stores and Stands
5994 News Dealers, Newsstands
5995 Pet Shops, Food, Supplies
5996 Swimming Pools Sales/Serv
5997 Electric Razors – Sales/Serv
5998 Tent and Awning Shops
5999 Misc./Specialty Retail
6010 Manual Cash Disburse
6011 Automated Cash Disburse
6012 Financial Institutions
6051 Non FI, Money Orders
6211 Security Brokers/Dealers
6300 Insurance Underwriting, Prem
6760 Savings Bonds
7011 Hotels, Motels, Resorts
7012 Timeshares
7032 Sporting/Recr Camps
7033 Trailer Parks, Campgrounds
7210 Laundry, Cleaning Services
7211 Laundries
7216 Dry Cleaners
7217 Carpet/Upholstery Clean
7221 Photographic Studios
7230 Barber and Beauty Shops
7251 Shoe Repair/Hat Cleaning
7261 Funeral Serv, Crematories
7273 Dating/Escort Services
7276 Tax Preparation Service
7277 Counseling Service
7278 Buying/Shopping Services
7296 Clothing Rental
7297 Massage Parlors
7298 Health and Beauty Spas

7299 Misc. General Services
7311 Advertising Services
7321 Credit Reporting Agencies
7333 Commercial Photography
7338 Quick Copy, Repro, Blueprint
7339 Secretarial Support Services
7342 Exterminating Services
7349 Cleaning and Maintenance
7361 Employ/Temp Agencies
7372 Computer Programming
7375 Information Retrieval Serv
7379 Computer Repair
7392 Consulting, Public Relations
7393 Detective Agencies
7394 Equipment Rental
7395 Photo Developing
7399 Misc Business Services
7512 Car Rental Agencies
7513 Truck/Utility Trailer Rentals
7519 Recreational Vehicle Rentals
7523 Parking Lots, Garages
7531 Auto Body Repair Shops
7534 Tire Retreading & Repair
7535 Auto Paint Shops
7538 Auto Service Shops
7542 Car Washes
7549 Towing Services
7622 Electronics Repair Shops
7623 A/C, Refrigeration Repair
7629 Small Appliance Repair
7631 Watch/Jewelry Repair
7641 Furniture Repair, Refinishing
7692 Welding Repair
7699 Miscellaneous Repair Shops
7829 Picture/Video Production
7832 Motion Picture Theaters
7841 Video Tape Rental Stores
7911 Dance Hall, Studios, Schools
7922 Theatrical Ticket Agencies
7929 Bands, Orchestras
7932 Billiard/Pool Establishments
7933 Bowling Alleys
7941 Sports Clubs/Fields
7992 Golf Courses - Public
7993 Video Game Supplies
7994 Video Game Arcades
7995 Betting/Casino Gambling
7996 Amusement Parks/Carnivals
7997 Membership Clubs
7998 Aquariums
7999 Misc Recreation Services
8011 Doctors
8021 Dentists, Orthodontists
8031 Osteopaths
8041 Chiropractors
8042 Optometrists, Ophthalmologist
8043 Opticians, Eyeglasses
8049 Chiropodists, Podiatrists
8050 Nursing/Personal Care
8062 Hospitals
8071 Medical and Dental Labs
8099 Medical Services
8111 Legal Services, Attorneys
8211 Elemen, Secondary Schools
8220 Colleges, Universities
8241 Correspondence Schools
8244 Business/Secretarial Schools
8249 Vocational/Trade Schools
8299 Educational Services
8351 Child Care Services
8398 Charitable Organizations
8641 Civic, Social, Fraternal Assoc
8651 Political Organizations
8661 Religious Organizations
8675 Automobile Associations
8699 Membership Organizations
8734 Testing Laboratories
8911 Architectural/Surveying Serv
8931 Accounting/Bookkeeping Serv
8999 Professional Services
9211 Court Costs
9222 Fines
9223 Bail and Bond Payments
9311 Tax Payments
9399 Government Services
9402 Postal Services
9700 Automated Referral Serv
9950 Gov't to Gov't Sales

Examples of Cardholder Misuse and Fraud

Case #1 – A cardholder conspired with a local business owner to make purchases not authorized by the cardholder's agency. The merchant circumvented the authorization process to allow the cardholder to make purchases for his personal consumption. The cardholder approved the transactions.

Case #2 – A cardholder 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 cardholders. The goods or services purchased were never delivered to the government.

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

Case #4 – A cardholder 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 cardholder advised the merchant to split transactions to ensure they would not exceed the cardholder's single-purchase limit.

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

Case #6 – Vendors continually charged $2,499 to $2,500, more than once on the same day, and/or every day for one week. It was also identified that on an unspecific date and time the vendors would meet to split profits with cardholder(s).

Case #7 – Cardholders would establish front companies to receive payment for merchandise never received. The cardholders 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.

Appendix 1: Sample Annual Review Process

Disclaimer: The following information contained in Appendix 1 (Sample Annual Review Process) is intended to serve as a guide for your A/OPCs in order to detect cardholder misuse/fraud. It is not intended to serve as a template for all agencies.

Sample Memorandum

TO: Program Coordinators

FROM:

SUBJECT: Purchase Card Annual Review

In accordance with your Delegation of Procurement Authority, you are required to perform an annual review of your post or bureau's purchase card activity and implement program improvements where non-compliant issues have been identified. The purpose of the annual review is to ensure that cardholders and Approving Officials are complying with established procurement management practices, operating procedures and established purchase card controls. To facilitate the annual review process, the following [sample] documents are attached for your use: (1) Purchase Card Annual Review Checklist (Attachment 1); (2) Summary of Findings (Attachment 2); and (3) Certification of Completion of Purchase Card Annual Review (Attachment 3). These documents are available from [your agency's] Web site, _____.

Annual reviews and reports are to be performed and completed by each bureau or post on a fiscal year basis. Reviews of the previous fiscal year purchase card activity must be conducted and completed in the first quarter of each new fiscal year. During the second and third quarter of each fiscal year, the A/OPC will conduct random reviews of bureau and post findings. If your bureau or post is selected, you will be required to submit a copy of your findings along with any supporting documentation.

As a result of your participation and support, the purchase card program has been a success since its implementation at the Department in 1992. This is reflected in the tremendous growth of the program. We encourage posts and bureaus to share annual review best practices with each other. Your continued cooperation and support will help us to make future improvements to the program and standardize purchase card processes wherever possible. Should you have any questions regarding the annual review process, please contact _____.

Thank you very much.

Sample of Purchase Card Annual Review

I. Background

Under the governmentwide purchase card program, an annual review of cardholder and Approving Official (AO) records must be performed on a fiscal year basis. The purpose of the annual review is to improve program operations continually while ensuring cardholders and AOs comply with established procurement management practices, operating procedures, and established purchase card controls. This policy provides an overview of the annual review process, introduces sample forms to be used in the review, and explains the steps involved in conducting the annual review.

In addition to the guidance described in the following sections, there are two other resources available to assist you with conducting reviews. The first is the "Practical Guide for Reviewing Government Purchase Card Programs." The guide was developed by the President's Council on Integrity and Efficiency and is a valuable addition to the tools that many federal Inspectors General (IGs) have developed for use in overseeing purchase card activities in their agencies. It provides common-sense advice on conducting purchase card reviews and includes a number of practical features to enhance the review process, such as questionnaires, templates, and sample reports. This document is intended to supplement existing federal law, regulations, and internal agency guidelines. The guide is available at the following Web site: www.oig.doc.gov/oig/reports/other_publications/credit-cards-06-002.pdf.

The second resource is the GAO Audit Guide for Auditing and Investigating the Internal Control of the Government Purchase Card Programs. You can access this report by searching for Report GAO-04-87G at the following Web site: www.gao.gov. GAO also publishes reports of agency charge card program audits.

II. Overview of Annual Review Process

Annual reviews and reports are to be performed and completed by each bureau or post on a fiscal year basis. Reviews of the previous fiscal year purchase card activity must be conducted and completed in the first quarter of each new fiscal year. AOs may assist the program coordinator in the annual review process where needed. The process consists of a review of a random sampling of cardholder records, the documentation of any findings for improvement, and the certification of completion of the annual review process. The individual steps in the process are discussed under Part IV on page 36.

During the second and third quarter following each fiscal year, the A/OPC will conduct random reviews of each bureau and post findings. If your bureau or post is selected, you will be required to submit a copy of your annual review package consisting of the three attachments noted above along, with any supporting documentation. Annual reviews and supporting documentation must be retained in the file for a minimum of three years.

III. Annual Review Forms

To facilitate the annual review process, sample forms have been developed. The annual review forms are available from [your agency's] Web site and include:

- Purchase Card Annual Review Checklist
- Summary of Findings
- Certification of Completion of Purchase Card Annual Review

Sample Purchase Card Annual Review Checklist (Attachment 1): The Purchase Card Annual Review Checklist is used in the initial review of each cardholder's records to determine compliance with procurement buying policies, regulations, and procedures. The program coordinator must complete one checklist per each individual cardholder record reviewed in the random sample selected.

Sample Summary of Findings (Attachment 2): This form is used to summarize findings, including areas of non-compliance and recommendations for improvements identified in the checklists, cardholder records, or interviews with purchase card participants. Best practices and recommendations for improving the purchase card program are to be addressed at the end of the Summary of Findings form.

Sample Certification of Completion of Purchase Card Annual Review (Attachment 3): This form consists of a certification that must be dated and signed by the program coordinator upon completion of the annual review. The annual review package, including the certification of completion, must be retained in the bureau or post files for a minimum period of three years.

IV. Steps in Review Process

The following steps are provided for your guidance in conducting the annual review:

1. **Select Random Sample:** Randomly select a sufficient number of purchase cardholder records under each of your established AO accounts. The number selected must be large enough to provide an adequate sampling of purchase card operations within your bureau or post. Pertinent information related to the random sample selected must be documented in the space provided on the Annual Review Checklist and the Summary of Findings (the number of accounts selected, the names and individual account numbers of the AOs and the cardholders, the individual cardholder's single and monthly purchase limits, total number of cardholder records reviewed, etc).

2. **Conduct Interviews:** Conduct short interviews with the AO, cardholder, and budget or finance officer to discuss how the purchase card program and related procedures are working. The interviews can be a valuable source of information regarding bureau or post operational procedures and individual concerns or recommendations about the program. Both positive and negative comments should be solicited.

3. **Complete the Purchase Card Annual Review Checklist:** Complete an Annual Review Checklist for each cardholder record selected in your random sample. Address each specific review criterion contained in the Annual Review Checklist provided in Attachment 1 of this policy for each cardholder record reviewed, and document findings. A separate checklist must be completed for each cardholder record reviewed.

4. **Complete Summary of Findings:** Document areas of non-compliance, recommendations for improvement, and areas of purchase card best practices. For example, any areas of concern or problems found during any aspect of the review should be summarized, along with a discussion of what steps have been taken to correct the areas of non-compliance. Specific examples should be cited whenever possible. Only findings related to areas of non-compliance need to be summarized by the program coordinator unless addressing best practices, recommendations, or comments. The program coordinator may also address in the Summary of Findings general or miscellaneous areas not addressed on the checklists, such as whether your bank and the merchants are providing acceptable customer service. Areas of best practices are to be documented on the last page of the Summary of Findings. Any best practices or recommendations provided will be used to improve the purchase card program.

5. **Complete Certification of Completion:** Complete the certification contained in Attachment 3 upon completion of the annual review.

6. **Retain Files for Three Years:** Retain copies of the annual review package and any supporting information in the files for a minimum period of three years.

Attachment 1 : Sample Annual Review Checklist

Cardholder Name: _____ Period Covered:_____

Date of Review: _____ AO Name:_____

CH Account No.: _____ AO Account Number: _____

Specific Review Criteria	Compliant Yes	Compliant No	Compliant N/A
A. Card Usage Requirements			
1. The cardholder is the only individual who has used his or her card. (Determine if others have used the card or card number in the cardholder's absence.)	❑	❑	❑
2. Purchases have not exceeded the cardholder's single purchase limit (SPL). The cardholder's SPL is _____.	❑	❑	❑
3. Cardholder has not split requirements to stay under single purchase limit (SPL). (Look for repeated orders during a short time period for the same goods or services.)	❑	❑	❑
4. Back orders have not been permitted. All goods and services ordered were available for immediate delivery.	❑	❑	❑
5. Cardholder has checked required sources of supplies or services prior to ordering on the open market (e.g., agency inventories or excess property, FPI or UNICOR, NIB/NISH or AbilityOne, GSA Supply Programs, Federal Supply Schedules).	❑	❑	❑
6. Purchases by the cardholder were for official government business only.	❑	❑	❑
7. Purchase card was not used to purchase any of the following unless a specific authorization was granted in writing by the A/OPC:			
a. Cash advances	❑	❑	❑
b. Advance payments (except for subscriptions or publications)	❑	❑	❑

Attachment 1 : Sample Annual Review Checklist (continued)

Specific Review Criteria	Compliant Yes	Compliant No	Compliant N/A
c. Rental or lease of land or buildings	❑	❑	❑
d. Individual travel expenses	❑	❑	❑
e. Professional services for medical, legal, design/ engineering, or consulting services	❑	❑	❑
f. Vehicle rental or lease	❑	❑	❑
g. Caterers, restaurants, bars	❑	❑	❑
h. Telephone services (excludes cell phones and service)	❑	❑	❑
i. Construction above $2,000/year	❑	❑	❑
j. Services other than construction above $2,500/year	❑	❑	❑
k. Supplies that contain hazardous substances or require hazardous waste clean-up and disposal	❑	❑	❑
l. Rental and maintenance agreements above $2,500/year	❑	❑	❑
m. Membership in organizations, including charitable and social organizations	❑	❑	❑
n. Personal services	❑	❑	❑
o. Entertainment, amusement, and recreational services	❑	❑	❑
p. Firearms	❑	❑	❑
q. Pesticide purchase or application	❑	❑	❑
r. Copying jobs that exceed 5,000 copies of one page (single sided) or 25,000 copies total of multiple pages	❑	❑	❑
s. Print jobs that exceed $1,000	❑	❑	❑
8. Cardholder should not pay any U.S. state taxes (examine receipts to verify if any taxes have been included).	❑	❑	❑

Attachment 1 : Sample Annual Review Checklist (continued)

Specific Review Criteria	Compliant Yes	Compliant No	Compliant N/A
B. Documentation Requirements			
1. All purchases reviewed are supported by:			
a. A valid written authorization that describes what is to be purchased and signed by someone with authorized requisitioning authority (i.e., procurement request); and	❑	❑	❑
b. Budget Office approval.	❑	❑	❑
2. The cardholder's monthly statement of account is supported by the following documentation:			
a. Each transaction is supported by a purchase card receipt and/or cash register tape. If these are not available, a statement indicating why a receipt and/or cash register tape are not available (e.g., telephone orders).	❑	❑	❑
b. Proof of delivery or completion of performance.	❑	❑	❑
c. A description is on the statement for each line item delivered.	❑	❑	❑
d. The appropriate accounting, budget or project code is shown on the statement for each transaction. (Spot check budget and accounting codes to verify they are accurate.)	❑	❑	❑
e. Disputed purchases are annotated on the statement and a copy of the Cardholder Dispute Form is attached.	❑	❑	❑
f. Credit vouchers are attached to the statement if applicable.	❑	❑	❑
g. Statement is signed and dated by cardholder and AO.	❑	❑	❑

Attachment 1 : Sample Annual Review Checklist (continued)

Specific Review Criteria	Compliant Yes	Compliant No	Compliant N/A
3. The cardholder entered the purchase in the Purchase Card Buying Log each time the card is used. (Ensure that the cardholder is not constructing the log from the monthly purchase card statement, i.e. purchases on the log and statement are in the same order.)	❑	❑	❑
4. Cardholder has a copy of the Purchase Card Online Training Guide.	❑	❑	❑
5. Cardholder has a copy of his or her delegation of Procurement Authority on file.	❑	❑	❑
C. Processing Requirements			
1. Cardholder has sent statement to AO within five working days of receipt.	❑	❑	❑
2. The AO has sent statement to finance office within three working days of receipt. Determine how many days elapsed between the date the cardholder and the AO signed the statement. This should not exceed eight working days.	❑	❑	❑
3. Records have been retained for three years after date of final payment (if cardholder has had card over three years, verify that records are being retained).	❑	❑	❑
D. Miscellaneous Requirements			
1. Purchase card is kept adequately secured. (Is the card kept locked up in the office when not in use?)	❑	❑	❑

Attachment 2: Sample Summary of Findings

Bureau/Post: _____ Date of Review: _____

Program Coordinator Name: _____ Period Covered: _____

Program Total No. of Coordinator Cardholder Records Title: _____ Reviewed: _____

Total No. of Percentage of Cardholders: _____ Total Records Reviewed: _____

Attachment 3: Sample Certification of Completion of Purchase Card Annual Review

The certification below must be completed by the Program Coordinator and retained in the file with the Purchase Card Annual Review Checklist (Attachment 1) and the Summary of Findings (Attachment 2) for a minimum period of three years.

Reviewer (Program Coordinator, Print Name): _____

Reviewer (Signature): _____

Reviewer Title: _____

Date: _____

Appendix 2

Sample Questionable Purchases Form

Questionable Government Purchase Card Purchases(s):

A review of the Account Cycle Report (_____) identified a questionable purchase(s) charged to your account and is/are described below. Also, please give a detailed explanation in the space provided at the bottom of this form. Fax any supporting documentation that relates to this purchase within five (5) working days to the Installation Purchase Card Program Manager's office. This is a surveillance method and does not necessarily mean an unauthorized purchase was made. However, failure to provide a timely response may result in suspension of your government purchase card privileges. Any questions should be directed to _____. Thank you!!!

Billing Official: _____ Cardholder: _____

Master Account Code/Company Number: _____

Organization: _____ Name of Vendor: _____

Purchase Date: _____ Amount of Charge(s): _____

Please provide clarification regarding the following questionable government purchase card (GPC) purchase(s) and submit all supporting documentation to the purchase card help desk.

- May be a split requirement. Repeated purchases appear to have been made from the same vendor. Provide an explanation of the item(s) purchased below.
- May be an unauthorized purchase based upon vendor – provide a detailed description of the item(s) purchased below and the purpose of the items.
- Purchase may require a special approval – provide a copy of the signed special approval you obtained prior to the purchase.
- Purchase may be a mandatory source item (UNICOR/AbilityOne) – provide a copy of applicable waiver and any other supporting documentation to justify using another source.
- May have been duplicate billed – verify if duplicate billing has occurred. If so, contact vendor for credit and or fill out and attach a copy of Cardholder Questioned Item Form and fax to bank.
- Purchases may have been partially billed without cardholder's permission – if this has occurred without cardholder's permission, document problems and attach a copy of documentation.
- Cash advances/money orders – Prohibited under the purchase card program.
- Other:

GSA SmartPay®
Supporting your mission

GSA SmartPay® Program Support
https://smartpay.gsa.gov
(703) 605-2808
gsa_smartpay@gsa.gov

Scan this code with your smartphone and a QRreader app to obtain a pdf version of this publication, or to order a paper copy.

www.gsa.gov
July 2012
5-12-00612
Order catalogs at gsa.gov/cmls

F Federal Audience
M Military Audience