



Office of Inspector General

Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

MEMORANDUM

DATE: February 22, 2021

TO: Board of Governors

FROM: Peter Sheridan *Peter Sheridan*
Associate Inspector General for Information Technology

SUBJECT: *Calendar Year 2019 Risk Assessment of the Board's Purchase Card Program*

Executive Summary

We have conducted a risk assessment of the Board of Governors of the Federal Reserve System's government purchase card program to determine the necessary frequency and scope of government purchase card audits. The results of the risk assessment show that the risk of illegal, improper, or erroneous use in the Board's purchase card program is *low*.

A risk level of *low* means that illegal, improper, or erroneous use is unlikely to occur and that such an occurrence would be expected to have a minimal effect on current operations and long-term objectives. Nonetheless, the Board's Purchase Card section should continue to take appropriate actions to ensure proper oversight of its program. As a result of the low risk level, we will not include an audit of the Board's purchase card program in our 2021 audit plan.

Background

The Government Charge Card Abuse Prevention Act of 2012 requires the inspector general of each executive agency to conduct periodic assessments or audits of purchase card programs to identify and analyze the risks of illegal, improper, or erroneous purchases and payments. The Office of Management and Budget (OMB) issued OMB Circular A-123 appendix B, *A Risk Management Framework for Government Charge Card Programs*, which states that inspectors general will conduct assessments of their agency's purchase card programs to identify and analyze the risks of illegal, improper, or erroneous purchases and payments. OMB directed that these risk assessments be used to determine the necessary scope, frequency, and number of audits or reviews of the purchase card program.

The Board participates in the U.S. General Services Administration's SmartPay3 program for government employees, and Citibank, the card issuer, provides a purchase card to each eligible Board employee to

reduce administrative costs and promote efficient business practices.¹ The Board operates its purchase card program under the procedures set forth in the *Purchase Card Procedures* document, which outlines the requirements regarding the use of the purchase card and details the requirements of the purchase card program.²

During calendar year 2019, the Board had 86 active purchase card accounts totaling about \$2.8 million in total program spending.

The Board's Purchase Card Procedures Document

Under the Board's *Purchase Card Procedures* document, cardholders must comply with applicable federal regulations and Board policies and guidance, including the Board's *Acquisition Policy*, which governs the procurement of micropurchases (those under \$5,000) and supplies and services subject to the Service Contract Act (those under \$2,500). A cardholder's intentional use of the charge card for other than official Board business is considered an attempt to commit fraud and could result in immediate cancellation of the charge card. The cardholder may also be subject to disciplinary action up to and including termination of employment.

According to the *Purchase Card Procedures* document, cardholders are required to complete initial, annual, and refresher training as needed. Upon completion of the training, cardholders review and sign the applicable Cardholder Acknowledgement Form, which outlines the cardholder's roles and responsibilities. Cardholders are responsible for, among other things, making authorized purchases for official Board business only, ensuring that funds are available, complying with spending limitations, maintaining a monthly purchase card log for all transactions, complying with internal control procedures, reconciling posted transactions, providing timely review of reconciled transactions for approving official review, and disputing unresolved or invalid transactions. The Board is not liable for unauthorized use of the purchase card by an individual other than the cardholder.

Objective, Scope, and Methodology

Our objective was to analyze the risks of illegal, improper, or erroneous purchases and payments associated with the Board's purchase card program to determine an overall risk level for the program. The scope of our risk assessment covered purchase card transactions during calendar year 2019 (January 1, 2019, through December 31, 2019). We conducted our risk assessment work from April 2020 through October 2020.

Risk Assessment Survey

To conduct our risk assessment, we obtained and reviewed relevant Board policies and procedures and the results of prior audits and reviews of the program. In addition, we surveyed applicable Board officials

¹ The U.S. General Services Administration's SmartPay 2 contract ended on February 4, 2019. The successor program, SmartPay 3, was implemented on February 5, 2019.

² The *Purchase Card Procedures* document is dated June 15, 2016. The Board is currently in the process of updating this document.

and the responsible agency program coordinator to identify (1) risks that could prevent the office from achieving its goals and (2) controls to mitigate these risks.

We used five risk categories in our risk assessment—financial, strategic, operational, compliance, and reputational—as defined below:

- **Financial**—the risk that an event related to the purchase card could occur that has a significant financial effect on the Board’s or the Division of Financial Management’s budget process
- **Strategic**—the risk that an event related to the purchase card could impede the Board’s or the Division of Financial Management’s ability to achieve its mission and strategic objectives
- **Operational**—the risk that an event related to the purchase card could be negatively affected by inadequate, ineffective, or failed business processes, human capital, or technology and information management
- **Compliance**—the risk that an event related to the purchase card could hamper the purchase card program’s ability to comply with applicable laws, regulations, or internal policies and procedures
- **Reputational**—the risk that an internal or external event related to the purchase card could diminish the Board’s or the Division of Financial Management’s stature, credibility, or effectiveness

The Board’s Purchase Card section, which is part of the Board’s Division of Financial Management, identified inherent risks by relevant risk category and assessed the risks’ impact and likelihood. *Inherent risk* is the risk that exists in the absence of controls that management may take to alter the likelihood or impact of the risk. *Impact* is the magnitude of deficiency that could result from the risk, and *likelihood* is the level of possibility that a risk will occur. We then identified the residual risks by assessing the impact and likelihood of risks by risk category, considering the effect of internal controls and other relevant documentation. *Residual risk* is the risk that remains after management implemented controls to alter a risk’s likelihood or impact. We assigned a level of risk using the criteria in table 1. We then combined the impact and likelihood of individual risk category levels to arrive at an average overall residual risk level.

Table 1. Definitions of Risk Impact and Risk Likelihood, by Level

Level	Risk impact definition	Risk likelihood definition
High	Significant impact on current operations and long-term objectives	Highly likely to occur
Medium	Limited impact on current operations and long-term objectives	Likely to occur
Low	Minimal impact on current operations and long-term objectives	Unlikely to occur

Source: OIG adaptation of tables from the Federal Reserve Bank of Cleveland’s *Toolkit for Functional Risk Assessments*, November 2009.

Information Systems Used by the Board's Purchase Card Program

Cardholders and program officials use the Citibank electronic credit card management system to review transactions, and program officials use the system to run reports for program administration. We obtained Citibank data to evaluate all charges incurred by purchase cardholders in 2019.

The Board uses PeopleSoft, an Oracle system, to manage human resource records, such as hiring and separation information. We obtained Oracle PeopleSoft data to identify separated employees. We independently extracted purchase card transaction data. Additionally, we obtained and reviewed system-level information security control reports to determine whether the data within each system were reliable for the purpose of our review.

Data Analytics Testing

In addition to the risk assessment survey, we developed and ran algorithms for data analysis designed to test purchase card transactions made during calendar year 2019. This analysis was conducted to identify potentially illegal, improper, or erroneous transactions to support the residual risk ranking for the Board's purchase card program. Specifically, we tested for transactions that occurred in the following categories:

- **Prohibited merchant category codes (MCCs)**—We compared transactions to the Board's blocked MCC list to identify transactions with MCCs that occurred on blocked codes.³ We also followed up to determine whether the agency/organization program coordinator (A/OPC) approved the cardholder's request to unblock the MCC.
- **Split purchases**—We sorted and grouped all Citibank transactions to identify those made (1) by the same cardholder, (2) with the same vendor, (3) with the same transaction date, and (4) with totals greater than the micropurchase threshold to determine whether cardholders appeared to split purchases into multiple transactions to circumvent the single purchase limit of \$5,000. We compared those transactions to the A/OPC's monthly review to determine whether the A/OPC had identified them as split transactions and, if so, whether the A/OPC followed up with the cardholder.
- **Sales tax**—We filtered the tax field for Citibank transactions to identify transactions with sales tax amounts greater than zero. We then compared those transactions to the A/OPC's monthly tax audits to determine whether the A/OPC identified paid sales tax and whether the A/OPC followed up with the cardholders.
- **Single purchase limit**—We filtered the transaction amount field for transactions greater than the single purchase limit of \$5,000 to determine whether cardholders exceeded their single purchase limit.
- **Transactions made after separation**—We compared Citibank transactions to the Board's 2019 separation report to identify employees who made purchases after separating from the Board.

³ According to the GSA SmartPay glossary, an MCC is a four-digit code used to identify the type of business (for example, a gas station, a restaurant, an airline). The merchant selects its MCC with its bank based on its primary business. Agencies can block or flag MCCs to guard against unallowable charges.

Results of Risk Assessment

Table 2 shows for each risk category the impact that illegal, improper, or erroneous use would have on the Board's purchase card program and the likelihood that such use will occur in the Board's purchase card program. The average overall residual risk level contributes to the final risk assessment for the Board's purchase card program.

Table 2. Impact, Likelihood, and Overall Residual Risk Level, by Risk Category

Risk category	Impact	Likelihood	Overall risk level
Financial	Low	Low	Low
Strategic	Low	Low	Low
Operational	Low	Low	Low
Compliance	Low	Low	Low
Reputational	Low	Low	Low
Average overall residual risk level	Low	Low	Low

Source: OIG analysis.

Results of Data Analytics Testing

The results of our testing of purchase card transactions for potentially illegal, improper, or erroneous transactions are shown in table 3.

Table 3. Summary of Data Analytics Testing Results

Tests	Results
Prohibited MCCs	All 46 prohibited MCC transactions were approved by the A/OPC. The purchase card program has controls in place for MCC requests and approvals.
Split purchases	The A/OPC did not detect any potential split purchases. The purchase card program has controls in place to detect and address potential split purchases.
Sales tax	The A/OPC identified and addressed sales tax issues. The purchase card program has established a new method for identifying, reviewing, and monitoring sales tax transactions.

Tests	Results
Single purchase limit	Cardholders did not make any purchases that exceeded their single purchase limit. The purchase card program has controls in place to ensure that cardholders do not exceed their single purchase limit.
Transactions made after separation	Cardholders did not make any purchases after separating from the Board. The purchase card program has controls in place to address separating cardholders.

Source: OIG analysis.

Conclusion

The results of the risk assessment survey and the data analytics testing led us to determine that the risk of illegal, improper, or erroneous use in the Board's purchase card program is *low*.

A risk level of *low* means that illegal, improper, or erroneous use is unlikely to occur and that such an occurrence would likely have a minimal effect on the Board's current operations and long-term objectives. Nonetheless, the Board's Purchase Card section should continue to take appropriate actions to ensure proper oversight of its program. As a result of the low risk level, we will not include an audit of the Board's purchase card program in our 2021 audit plan.

This report is provided for informational purposes, and a response is not required. We appreciate the cooperation and assistance provided by your staff during this risk assessment. If you have any questions, please contact Victor Calderon, OIG manager for data analytics, or me.

cc: Patrick J. McClanahan
Ricardo A. Aguilera
Steve Bernard
Monica Manning
Kimberly Briggs
Craig Delaney