MEMORANDUM

DATE: August 31, 2022

TO: Rohit Chopra
                    Director
                    Bureau of Consumer Financial Protection

FROM: Fred W. Gibson
                    Deputy Inspector General

SUBJECT: *Fiscal Years 2020 and 2021 Risk Assessment of the Bureau's Purchase Card Program*

Executive Summary

We have conducted a risk assessment of the Bureau of Consumer Financial Protection's purchase card program to determine the necessary frequency and scope of purchase card audits. The results of the risk assessment show that the risk of illegal, improper, or erroneous use in the Bureau's purchase card program is *low*. As a result, we will not recommend that an audit of the program for fiscal year 2022 be included in our 2023 annual audit plan.

The results of the risk assessment should not be interpreted to mean that a lower-risk program is free of illegal, improper, or erroneous use or internal control deficiencies. An audit of the program may identify issues not previously noted in the risk assessment. For instance, the overall risk level for the purchase card program may be assessed as *low* based on the design of internal controls and the size of the program; however, an audit may find that controls are not working effectively or that illegal, improper, or erroneous activity has taken place.

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. In September 2013, the Office of Management and Budget (OMB) issued OMB Memorandum M-13-21, *Implementation of the Government Charge Card Abuse Prevention Act of 2012*, which states that inspectors general will conduct annual risk assessments of agency purchase card programs to analyze the risks of illegal, improper, or erroneous purchases. 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 Bureau participates in the U.S. General Services Administration's SmartPay 3 program through a task order with the U.S. Department of the Treasury's master contract with Citibank. Within Treasury, the Bureau of the Fiscal Service, Administrative Resource Center provides purchase card administrative services and acts as the liaison between the Bureau and Citibank. The Bureau's Office of Procurement is responsible for managing the operation of the purchase card program and ensuring that the program complies with applicable laws, regulations, policies, and procedures.

The Office of Procurement also monitors the effectiveness of the purchase card program as a payment vehicle while working to ensure that the proper controls are in place. The Bureau operates its purchase card program under the policies and procedures set forth in its *Purchase Card Policy and Management Plan*, which was finalized in June 2018.

During the period of our review, October 1, 2019, through September 30, 2021, a total of 116 Bureau purchase cardholders had 7,037 purchase transactions totaling about $3.46 million.

Objective, Scope, and Methodology

Our objective was to analyze the risks of illegal, improper, or erroneous purchases and payments associated with the Bureau's purchase card program in order to determine an overall risk level for the program. The scope of our risk assessment covered October 1, 2019, through September 30, 2021.

To conduct our risk assessment, we obtained and reviewed the Office of Procurement's objectives for the program as well as its purchase card policies and procedures. In addition, we surveyed the responsible agency/organization program coordinator (A/OPC) 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 would have a significant financial effect on the Bureau's or the Office of Procurement's budget process

- **strategic**—the risk that an event related to the purchase card could impede the Bureau's or the Office of Procurement'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 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 Bureau's or the Office of Procurement's stature, credibility, or effectiveness

The Office of Procurement identified inherent risks by relevant risk category and assessed the risks' impact and likelihood. *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 assessed the impact and likelihood of risks by risk

category, considering the effect of internal controls and other relevant documentation. 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 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.

In addition to the risk assessment template, we created algorithms for data analytics testing designed to test the entire Citibank data file from October 1, 2019, through September 30, 2021, to identify high-risk transactions. Specifically, we created algorithms to detect

- transactions associated with prohibited merchant category codes (MCCs)

- improper use of convenience checks or cash advances

- potentially split purchases

- transactions that included sales tax

- transactions made with third-party vendors

- the timing of account closure after employee separation

Results of Risk Assessment Survey

Table 2 shows each risk category's risk level for impact and likelihood. The average overall risk level determines the final risk assessment survey score for the Bureau's purchase card program.

Table 2. Impact, Likelihood, and Overall 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 risk level	**Low**	**Low**	**Low**

Source: OIG analysis.

Results of Data Analytics Testing

We created the following algorithms to test the entire Citibank data file and identify high-risk transactions:

- **Unallowable MCCs**—We compared all 7,037 purchase card transactions to the Bureau's allowable MCC list to identify transactions with MCCs that are not on the list. We requested supporting documentation to determine whether the A/OPC identified and authorized transactions with unallowable MCCs.

- **Convenience checks and cash advances**—We filtered all 7,037 purchase card transactions to identify check fees and cash advances. We requested supporting documentation to determine whether these were allowable transactions and whether the purchase card was used properly by approved agency employees.

- **Split purchases**—We sorted and grouped all 7,037 purchase card transactions to identify transactions made by the same cardholder with the same vendor and that, when added together, surpassed the micropurchase threshold to determine whether cardholders appeared to split purchases into multiple transactions to circumvent the micropurchase threshold.[1] We obtained and reviewed supporting documentation to determine whether the total purchase amount exceeded the single purchase limit and to determine whether the A/OPC had identified them as split transactions.

- **Sales tax**—We filtered the tax field for all 7,037 purchase card transactions to identify transactions with sales tax amounts greater than zero. We were not able to use the Citibank data because vendors did not report taxes properly. Instead, we reviewed the transactions identified

---

[1] The micropurchase threshold increased from $3,500 to $10,000 on September 13, 2018.

in the Bureau of the Fiscal Service, Administrative Resource Center's annual compliance reviews and the A/OPC's quarterly reviews to determine whether the A/OPC detected sales taxes paid and followed up with those cardholders.

- **Third-party transactions**—We filtered all 7,037 purchase card transactions to identify transactions with third-party vendors. We requested supporting documentation to determine whether the A/OPC identified and authorized transactions with third-party vendors.

- **Timely closure of accounts**—We compared a list of separated Bureau employees to a list of closed purchase card accounts to determine whether the cards were closed timely for separated employees and whether any transactions occurred after separation. We determined whether the time to close was within the next billing cycle and obtained documentation for any transactions that occurred after employee separation.

Figure 1 shows the results of our data analytics testing.

Figure 1. Summary of Data Analytics Testing Results for the Bureau's Purchase Card Program

Transactions on unallowable MCCs were identified and followed up on with cardholders.
The A/OPC detected all 150 transactions with MCCs not included on the allowable list. Documentation supports that the A/OPC approved all 150 purchases.

Convenience check purchases were properly documented and approved.
Contracting officers properly documented the use of convenience checks for 53 transactions, and check logs were approved. No unauthorized employees used convenience checks for purchases.

Split purchases were detected and followed up on with cardholders.
The A/OPC reviewed 36 potentially split purchases. None of the purchases were confirmed as split; they were under the single purchase limit and monthly credit card limits.

Transactions that included sales tax were detected and followed up on with cardholders.
Internal and external purchase card reviews identified 11 transactions for which the sales tax was improperly collected. The Bureau's ongoing monitoring is reducing risk to an acceptable level.

Third-party transactions were detected and followed up on with cardholders.
The A/OPC confirmed that all 118 third-party transactions made by cardholders were approved, including those made by contracting officers, and determined that those transactions were not subject to third-party purchase restrictions.

Separated employees' purchase cards were closed timely.
All separated employees' purchase cards were closed within the next billing cycle. No cards were used after separation.

Source: OIG analysis.

Conclusion

The results of the risk assessment survey and data analytics testing show that the risk of illegal, improper, or erroneous use in the Bureau's purchase card program is *low*. As a result, we will not recommend that an audit of the Bureau's purchase card program for fiscal year 2022 be included in our 2023 annual 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. Please let me know if you have any questions.

cc: Jean Chang
        Katherine Sickbert
        Joshua Galicki