




Office of Inspector General

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

MEMORANDUM

DATE: September 4, 2024

TO: Rohit Chopra
Director
Consumer Financial Protection Bureau

FROM: Khalid Hasan 
Assistant Inspector General for Information Technology

SUBJECT: *Fiscal Years 2022 and 2023 Risk Assessment of the CFPB's Purchase Card Program*

Executive Summary

We have conducted a risk assessment of the Consumer Financial Protection Bureau's purchase card program to inform 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 CFPB'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. Although two purchase card controls were not operating as effectively as they should (third-party payment provider forms and annual inspections from the Bureau of the Fiscal Service) and one analytics test had potential exceptions (potentially split purchases), these findings were not significant enough to raise the overall risk level above *low*. Nonetheless, the CFPB's Office of Procurement should continue to take appropriate actions to ensure proper oversight of its program.

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. Additionally, the Office of Management and Budget (OMB) has issued OMB Circular A-123, "Appendix B: A Risk Management Framework for Government Charge Card Programs," which states that inspectors general will conduct periodic risk assessments of agency purchase card programs to analyze the risks of illegal, improper, or erroneous purchases.

The CFPB is enrolled in a Citibank Card Management Service, which is provided through the U.S. Department of the Treasury under the U.S. General Services Administration SmartPay3 contract. The Bureau of the Fiscal Service, Administrative Resource Center (BFS ARC) provides the CFPB with government purchase card program administration support services. CFPB purchase cards are linked to a centrally billed account.

The purchase card program is coordinated by the CFPB agency/organization program coordinator (A/OPC). The CFPB A/OPC, in the CFPB's Office of Procurement, is the authorized liaison between the CFPB and BFS ARC. The A/OPC is responsible for oversight of cardholders' purchasing, which includes monitoring monthly statement reconciliations. The CFPB 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, 2021, through September 30, 2023, 5,720 purchases were made totaling about \$4.79 million.¹

Objective, Scope, and Methodology

Our objective was to assess the risks of illegal, improper, or erroneous purchases and payments associated with the CFPB's purchase card program to determine the overall risk level.² Our risk assessment covered transactions from October 1, 2021, through September 30, 2023. To conduct our risk assessment, we performed controls testing, data analytics testing, and a trend analysis.

For controls testing, we tested five purchase card controls against the relevant data files to determine if the controls were operating effectively:

- **New cardholder forms**—Identify purchase cards opened during the scope period and determine if a Citibank Government Purchase Card Setup Form was submitted for each account.
- **Third-party payment provider forms**—Identify purchase card transactions made through a third-party payment provider and determine if a Purchase Card Intake Form was submitted or if A/OPC approval was obtained before the purchase.
- **Micropurchase thresholds**—Identify purchase card transactions exceeding the three micropurchase thresholds of \$2,000 for services covered under the *Federal Acquisition Regulation*, subpart 22.40, Construction Wage Rate Requirements; \$2,500 for services subject to the Service Contract Act; and \$10,000 for supplies and services not subject to the *Federal Acquisition Regulation*, subpart 22.10, Service Contract Labor Standards. Determine if these transactions followed the CFPB's procurement process as stated in the purchase card control.

¹ This includes only those transactions above a \$0 value, as transactions less than \$0 are for refunds, payments, credits, and so on. The total number of all transactions is 6,828.

² Risk level was determined on a *low-medium-high* scale using the Federal Reserve Bank of Cleveland's *Toolkit for Functional Risk Assessments*, November 2009.

- **Quarterly A/OPC reviews**—Determine if the CFPB purchase card A/OPC performed quarterly reviews throughout the review period to verify that purchase cards were being used in accordance with policies and procedures.
- **Annual BFS inspections**—Review the annual BFS inspections of the CFPB purchase card program and determine if the CFPB A/OPC appropriately followed up on any findings.

For the data analytics testing, we created algorithms to review all Citibank transactions for high-risk transactions. Specifically, we tested for transactions in the following categories:

- **Prohibited merchant category codes (MCCs)**—Identify transactions that occurred on blocked MCCs.
- **Convenience checks or cash advances**—Identify transactions involving cash advances or convenience checks to determine whether only approved cardholders were involved.
- **Split purchases**—Identify purchases that have been intentionally split into multiple transactions to stay below the micropurchase threshold.³
- **Sales tax**—Identify transactions where sales tax was charged.⁴
- **Non-CFPB employees**—Identify transactions made by individuals not currently or previously employed by the CFPB.
- **Timely closure of accounts**—Identify employees who separated from the CFPB during our scope period and determine if their purchase cards were closed timely. For those employees whose cards were not closed timely, identify any transactions that occurred after their departure date.

For the trend analysis, we identified trends in purchase card activity between fiscal year 2022 and fiscal year 2023. We created visualizations to analyze the following areas:

- **Total agency spending**—Compare total agency spending from fiscal year 2022 and fiscal year 2023 to identify any significant changes.
- **Spending by division**—Compare divisional spending from fiscal year 2022 and fiscal year 2023 to identify any significant changes or divisional outliers.
- **Spending by employee**—Compare the highest-spending employees from fiscal year 2022 and fiscal year 2023 to identify any significant changes or employee outliers.

³ According to the CFPB's *Purchase Card Policy and Management Plan*, June 2018, cardholders are prohibited from splitting a purchase to stay under the micropurchase threshold. This practice violates *Federal Acquisition Regulation* 13.003(c)(2), which states, "Do not break down requirements aggregating more than the . . . micro-purchase threshold into several purchases that are less than the applicable threshold merely to . . . [a]void any requirement that applies to purchases exceeding the micro-purchase threshold."

⁴ According to the CFPB's *Purchase Card Policy and Management Plan*, June 2018, the CFPB does not pay state and local taxes on its purchases. Each cardholder is responsible for ensuring that no taxes are charged.

Results of Controls Testing

The results of our purchase card controls testing are as follows:

- **New cardholder forms**—We identified nine new cardholders during the period of our review, all of whom submitted the necessary Citibank Government Purchase Card Setup Form.
- **Third-party payment provider forms**—We identified 100 transactions that were made using third-party payment providers, specifically PayPal. We tested a sample of 10 transactions and found that 6 had the Purchase Card Intake Form on file or received A/OPC approval before the purchase was made. The other 4 transactions did not have approval before the purchase was made. The A/OPC informed us that the approval process for using PayPal recently changed, which could explain the deviations from policy. Further, the failures occurred in 2022, and all third-party payments that occurred in 2023 followed the correct procedure, indicating that the control's performance improved over time. However, given the 40 percent failure rate in the sample, we considered this control to be operating ineffectively.
- **Micropurchase thresholds**—We tested a sample of 25 transactions associated with the three micropurchase thresholds of \$2,000, \$2,500, and \$10,000. We requested documentation from the A/OPC and verified that each transaction followed the appropriate procurement process with no outstanding issues.
- **Quarterly A/OPC reviews**—We obtained the eight quarterly A/OPC reviews performed during the review period and verified that each was complete with no outstanding issues.
- **Annual BFS inspections**—We obtained the two annual BFS inspections and noted that the 2021–2022 inspection had a 3.5 percent response rate to its 170 findings and the 2022–2023 inspection had a 61 percent response rate to its 349 findings. Both the number of total findings and the number of Section 889–related findings increased from one year to the next.⁵ In the 2021–2022 inspection, 163 of the 170 findings were related to Section 889, and in the 2022–2023 inspection, 203 of the 349 findings were related to Section 889. We agreed with the A/OPC's assessment that the volume of findings inaccurately reflected the level of risk posed to the purchase card program because most of the purchases made were not related to covered telecommunications as stated in Section 889, and therefore the risk posed by the Section 889–related findings was low. However, because of the control's requirements to respond to all findings, we still considered the control to be operating ineffectively.

⁵ Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, prohibits the purchase of covered telecommunications equipment and services from vendors who sell products containing spyware. These devices could pose a threat to U.S. security by spying on or disrupting communications within the United States. A contractor is required to submit a form to SAM.gov certifying that they do not utilize such equipment before they can enter into federal contracts. During the annual BFS inspections, a lack of these certification forms prompted a large number of Section 889–related findings.

We were informed by the A/OPC that, after discussing the matter internally and weighing the benefits of responding to each finding versus the time needed to pull each certificate from SAM.gov, the CFPB decided not to respond to the Section 889 findings.

Results of Data Analytics Testing

The results of our data analytics testing include the following:

- **Prohibited MCCs**—We compared all 5,720 purchase card transactions to the CFPB’s allowable MCC list to identify transactions with MCCs that were not on the list. We identified 116 transactions with prohibited MCCs, spanning 32 different MCCs across 12 MCC categories. We selected a sample of 11 transactions and requested supporting documentation from the CFPB to determine whether the A/OPC authorized these transactions. We found there was sufficient supporting documentation and authorization for each transaction.
- **Convenience checks or cash advances**—We filtered all 5,720 purchase card transactions to identify check fees and cash advances. We identified 55 cash advance fees and requested documentation from the CFPB to determine whether these were allowable transactions and whether the purchase card was used properly by approved agency employees. We verified that each transaction was associated with an approved convenience check written by an employee authorized to do so.
- **Split purchases**—We sorted and grouped all 5,720 purchase card transactions to identify those occurring by the same cardholder with the same vendor on the same day that, when added together, surpassed the micropurchase threshold of \$10,000 to determine whether cardholders appeared to intentionally split purchases into multiple transactions to circumvent this threshold. Our testing identified 4 potentially split purchases (each made up of multiple transactions) that exceeded this \$10,000 threshold, and we followed up with the A/OPC for further documentation.

Of these 4 potentially split purchases, we believe that 2 of them were split, but without a purposeful intent to avoid this threshold. Communication between the cardholder and the A/OPC shows that the cardholder misunderstood the policy. The A/OPC agreed and determined that these 2 purchases were not intentionally split and counseled the cardholder on proper policy. We agree that these 2 purchases reflected a misunderstanding of policy.

It was unclear if the remaining 2 purchases were intentionally split to avoid the micropurchase threshold. While our testing showed that the purchases exceeded the \$10,000 threshold (\$10,210.15 and \$11,348.14), the A/OPC believed that these purchases were not intentional splits based on her conversations with the cardholders. The documentation provided for these 2 purchases was ambiguous regarding the cardholders’ reasoning for making multiple purchases on the same day from the same vendor. Therefore, we could not determine based on the materials provided why the separate same-day purchases from the vendor occurred.

Determining if purchases are intentionally split is subjective, and the A/OPC believed that none of the 4 were intentionally split. Based on our review, the A/OPC followed up on each transaction at the time of purchase, and the A/OPC is properly identifying and reviewing potentially split purchases. Given the details surrounding each purchase, we believe that these potentially split purchases do not contribute to a higher overall risk level. However, we will continue to monitor this area in future risk assessments.

- **Sales tax**—We filtered the sales tax field on the Citibank reallocation reports to determine whether any sales tax was reported on purchase card transactions. We also reviewed the A/OPC

quarterly reviews to determine whether the A/OPC identified any instances of sales tax being paid. We verified that no sales tax was paid on purchases.

- **Non-CFPB employees**—We compared all 5,720 purchase card transactions to the lists of active and separated CFPB employees to identify any transactions that might have occurred from non-CFPB employees. We verified that all purchase card transactions were made by current or former CFPB employees.
- **Timely closure of accounts**—We compared the list of separated CFPB employees to the 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 verified that all purchase cards were closed in a timely manner for employees who separated from the CFPB during the review period.

Results of Trend Analysis

We noted no unusual activity from the trend analysis. However, the visualizations helped us better understand the purchase card program as a whole. We were able to identify which divisions and employees were associated with the most purchase card spending between fiscal year 2022 and fiscal year 2023.⁶ While there was no unusual activity detected during our trend analysis, we will use these results as baselines for comparison in future risk assessments.

Conclusion

The results of our risk assessment show that, although two controls were not operating as effectively as they should and one analytics test had potential exceptions, the overall risk of illegal, improper, or erroneous use in the CFPB'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.

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 contact me if you would like to discuss this report.

cc: Adam Martinez
Jean Chang
Jafnar Gueye
Dana James
Joshua Galicki
Gail Neyland
Michael Gleason
Nicholas Olson

⁶ Because of the sensitive nature of the purchasing data, we presented our trend analysis results to CFPB stakeholders in a separate meeting.