



Office of Inspector General

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

MEMORANDUM

DATE: September 13, 2023

TO: Rohit Chopra
Director
Consumer Financial Protection Bureau

FROM: Khalid Hasan 
Assistant Inspector General for Information Technology

SUBJECT: *Fiscal Years 2020–2022 Risk Assessment of the CFPB’s Government Travel Card Program*

Executive Summary

We have conducted a risk assessment of the Consumer Financial Protection Bureau’s government travel card (GTC) program to determine the necessary frequency and scope of GTC audits. The results of the risk assessment show that the risk of illegal, improper, or erroneous use in the CFPB’s GTC 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 CFPB’s Office of Travel and Relocation (Travel Office) 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 CFPB’s GTC program in our 2023 audit plan.

Background

The CFPB 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’s, Administrative Resource Center provides travel card administrative services and acts as the liaison between the CFPB and Citibank.

During fiscal years 2020–2022, 23,495 purchases were made on individually billed CFPB GTCs totaling approximately \$5.2 million. The Government Charge Card Abuse Prevention Act of 2012 requires the inspector general of each executive agency with more than \$10 million in travel card spending to conduct periodic assessments or audits of travel 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 (Appendix B), which states that inspectors general will conduct annual risk assessments of agency travel card programs to analyze the risks of illegal, improper, or erroneous purchases.¹

The CFPB's Travel Policies and Procedures

Under the CFPB's travel policy, the Travel Office (located in the Office of the Chief Financial Officer) is responsible for operating the GTC program and ensuring that the program complies with applicable laws, regulations, policies, and procedures, including the CFPB's *Travel Desk Procedures* and *Policy on Travel*, which were finalized in March 2017 and December 2017, respectively. As part of their work, Travel Office staff train and inform travelers of their roles and responsibilities and issue updates and reminders on the program's policies and practices.

Cardholders who are part of the travel program must abide by the travel policies and procedures. All employees traveling for the CFPB must obtain and use an individually billed GTC for travel expenses incurred while on official business unless their travel expenses are charged to the centrally billed account. Cardholders must pay statement balances promptly, keep accounts current, and reconcile travel card statements to ensure that proper payments are received by Citibank and to allow for the detection of unauthorized transactions.

Travelers are required to use the GTC for common carrier transportation to and from their temporary duty location as well as for lodging and car rentals. They may also use their GTC for other reimbursable expenses while on official travel such as meals, gas for rental cars, taxis, car services, ridesharing services, car sharing services, and parking.

Citibank or the CFPB may cancel or suspend an account for nonpayment, delinquency, returned checks, or unauthorized purchases. CFPB employees are generally not allowed to travel on official business without an active travel card. The Travel Office provides travelers, their supervisors, and the Office of Human Capital with delinquency notices when there is an unpaid balance on the traveler's GTC.

Objective, Scope, and Methodology

Our objective was to analyze the risks of illegal, improper, or erroneous purchases and payments associated with the CFPB's GTC program to determine an overall risk level for the program. Our scope included travel card purchases during fiscal years 2020–2022 (October 1, 2019, through September 30, 2022). We conducted our risk assessment work from March through August 2023.

¹ This revision is effective as of August 2019 and replaces and rescinds the previously issued Appendix B policy dated January 2009 as well as OMB Memorandum M-13-21 dated September 2013. The purpose of Appendix B is to consolidate current governmentwide charge card program management requirements and guidance issued by OMB, the U.S. General Services Administration, the U.S. Government Accountability Office, Treasury, and other federal agencies.

Travel Card Program Information Systems

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 cardholders with individually billed accounts.

The CFPB uses HRConnect to manage human resource records, such as hiring and separation information. We obtained HRConnect data to identify active, separated, and hired employees. We independently extracted GTC transaction data from Citibank, and we observed the CFPB's extraction of personnel (active, separation, and hiring) data from HRConnect. Additionally, we obtained and reviewed system-level information security control requirements to determine whether the data used were reliable for the purpose of our review.

Risk Assessment Survey

To conduct our risk assessment, we obtained and reviewed relevant CFPB policies, procedures, and the results of prior audits and reviews of the program. In addition, we surveyed the program coordinator of the CFPB's Travel Office to identify (1) risks that could prevent their 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 travel card could occur that has a significant financial effect on the CFPB's or the Travel Office's budget process
- **Strategic**—the risk that an event related to the travel card could impede the CFPB's or the Travel Office's ability to achieve its mission and strategic objectives
- **Operational**—the risk that an event related to the travel 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 travel card could hamper the travel 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 travel card could diminish the CFPB's or the Travel Office's stature, credibility, or effectiveness

The CFPB's Travel Office identified risks by relevant risk category and assessed the risks' impact and likelihood. *Impact* is the magnitude of deficiency that could result from a 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.

Data Analytics Testing

In addition to the risk assessment survey, we developed and ran algorithms for data analysis designed to test the fiscal years 2020–2022 universe of Citibank transactions for potentially illegal, improper, or erroneous transactions. Specifically, we tested for transactions that occurred in the following categories:

- **Prohibited merchant category codes (MCCs)**—We compared all transactions to the CFPB's allowable MCC list to identify transactions with MCCs that are on blocked codes.²
- **Non-CFPB employees**—We compared all transactions to a list of active and separated CFPB employees to identify any transactions made by a cardholder who was not a CFPB employee.
- **Separated CFPB employees**—We compared all transactions to a list of separated CFPB employees to determine whether transactions occurred after the employee left the CFPB.

Lastly, we assessed the Travel Office's process for monitoring delinquent accounts to ensure proper follow-up was conducted. We selected 36 cardholders identified by the CFPB to be delinquent on payment: We selected 12 cardholders randomly, using a random number generator, another 12 cardholders among the accounts with the highest amount past due, and the final 12 cardholders were selected among the accounts with the most days past due. We obtained and reviewed emails between the Travel Office and delinquent accountholders to determine whether the Travel Office monitored delinquent accounts pursuant to the *Policy on Travel and Travel Desk Procedures*.

Results of Risk Assessment

The results of our risk assessment work, including both the survey and data analytics testing results, are summarized below.

² MCCs are used to classify merchants and businesses by the type of goods or services provided. Organizations can use MCCs to categorize, track, and restrict transactions.

Risk Assessment Survey Results

Table 2 shows each risk category’s level for impact and likelihood for the GTC program. The average overall risk level determines the final risk assessment for the CFPB’s GTC 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	Medium	Low
Average risk level	Low	Low	Low

Source: OIG analysis.

Data Analytics Testing Results

Our testing of 30,724 Citibank transactions for potentially illegal, improper, or erroneous transactions identified the following:

- **Transactions on prohibited MCCs**—We identified one transaction that occurred on a blocked MCC for \$125.46. Although we were not able to determine the cause of this transaction, the Travel Office stated that a technical glitch may have allowed the cardholder to make a purchase on a blocked MCC.
- **Transactions by non-CFPB employees**—We did not identify any transactions made by a cardholder who was not a CFPB employee.
- **Transactions after separation**—We did not identify any transactions made by a cardholder after their separation from the CFPB.
- **Monitoring of delinquent accounts**—Of the delinquent accounts selected for testing, we identified one account that did not receive delinquency notification emails from the Travel Office. The Travel Office stated that this account did not appear on its delinquency reports, so no email was sent.

Conclusion

The results of the risk assessment survey and data analytics testing led us to determine that the risk of illegal, improper, or erroneous use in the CFPB's GTC 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. While this risk assessment is an improvement from the previous risk assessment, the Travel Office should continue to take appropriate actions to ensure proper oversight of its program.

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 or any related issues.

cc: Adam Martinez
Jafnar Gueye
Dana James
Regina Braham