

Semiannual Report to Congress

April 1, 2025–September 30, 2025



Office of Inspector General

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



Message from the Inspector General

It is my pleasure to submit this semiannual report to Congress, the first since I was appointed on June 30, 2025, to be the inspector general for the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau. This report covers the period from April 1, 2025, to September 30, 2025.



Among the oversight work we completed during this reporting period was an assessment of the Board's travel card program. We found that while the Board has established and maintained certain controls for its travel card program, its control system needs to be improved to ensure that employees comply with travel requirements. This report contains three recommendations designed to help ensure that the program has effective internal controls. By strengthening its travel policies, implementing additional preventive and detective controls, and enforcing consequences for travel card misuse, the Board can help ensure consistent application of requirements; promote accountability; and reinforce a culture of compliance, integrity, and ethical values.

In a report regarding the CFPB's safeguards for protecting confidential supervisory information (CSI), we identified numerous issues. In 2023, the CFPB declared a major breach that affected about 256,000 consumers and 46 institutions after an employee sent CSI to a personal email account. We found that the CFPB's guidance does not sufficiently limit access to CSI and that its guidance lacks expectations for assessing the severity of breaches and enforcing consequences for responsible employees. Additionally, the CFPB does not have a defined process to notify affected supervised institutions of breaches. We made seven recommendations to address these issues and improve the agency's protection of CSI.

The work of our Office of Investigations continues to send a strong message that those who commit crimes that affect the integrity of our financial system will be brought to justice. In this reporting period, a former bank general counsel was sentenced in Connecticut to 48 months in prison for a \$7.4 million embezzlement scheme. In another case, an investment adviser pleaded guilty to a bank fraud conspiracy in which he attempted to obtain at least \$45.6 million in loans from financial institutions in Nebraska and Iowa by misrepresenting collateral funds and preparing bogus supporting documents. And in a third case, founders of a lender service provider based in Arizona pleaded guilty to participating in a scheme to fraudulently obtain tens of millions of dollars in pandemic relief loans.

Overall, the work of our Office of Investigations during this reporting period resulted in 29 arrests; 23 indictments; 12 criminal informations; 18 convictions; 11 referrals for criminal prosecution; and over \$104.5 million in civil judgments, forfeiture, criminal fines, restitution, and special assessments.

The work summarized in this report reflects our deep commitment to effective and independent oversight, and it is my honor to have been entrusted to lead this outstanding organization. I am grateful to the Office of Inspector General staff for their exceptional work, and I look forward to our continued release of impactful reports.

A handwritten signature in black ink, reading "Michael E. Horowitz". The signature is fluid and cursive, with the first name "Michael" being more legible than the last name "Horowitz".

Michael E. Horowitz
Inspector General
October 31, 2025

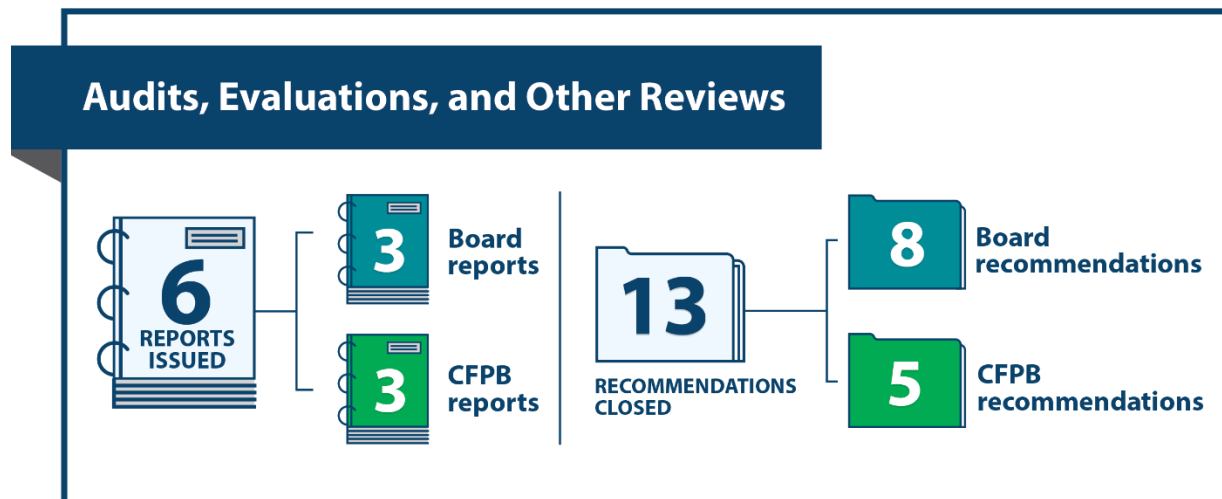


Contents

Highlights.....	1
Introduction	4
Pandemic Response Oversight	6
Audits and Evaluations	6
Investigations.....	6
Major Management Challenges	7
Audits, Evaluations, and Other Reviews	8
Board of Governors of the Federal Reserve System	8
Consumer Financial Protection Bureau	10
Failed State Member Bank Reviews	12
Material Loss Reviews	12
Nonmaterial Loss Reviews	12
Investigations	13
Hotline	17
Legislative and Regulatory Review, Congressional and Media Activities, and CIGIE Participation	18
Legislative and Regulatory Review	18
Congressional and Media Activities.....	18
CIGIE Participation.....	18
Peer Reviews	20
Appendix A: Statistical Tables.....	21
Appendix B: Additional Mandated Reporting Requirements	32
Appendix C: Open Recommendations Made Before the Reporting Period	33
Board of Governors of the Federal Reserve System.....	33
Consumer Financial Protection Bureau	41
Abbreviations	45

Highlights

We continued to promote integrity, economy, efficiency, and effectiveness of the programs and operations of the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau. The following are highlights, in chronological order, of our work during this semiannual reporting period.



The CFPB Can Improve Its Safeguards for Protecting Confidential Supervisory Information

The CFPB’s guidance for safeguarding confidential supervisory information (CSI) does not sufficiently limit access to it or establish expectations for assessing the severity of CSI breaches and enforcing consequences for responsible employees.

The Board Can Strengthen Its Travel Card Program

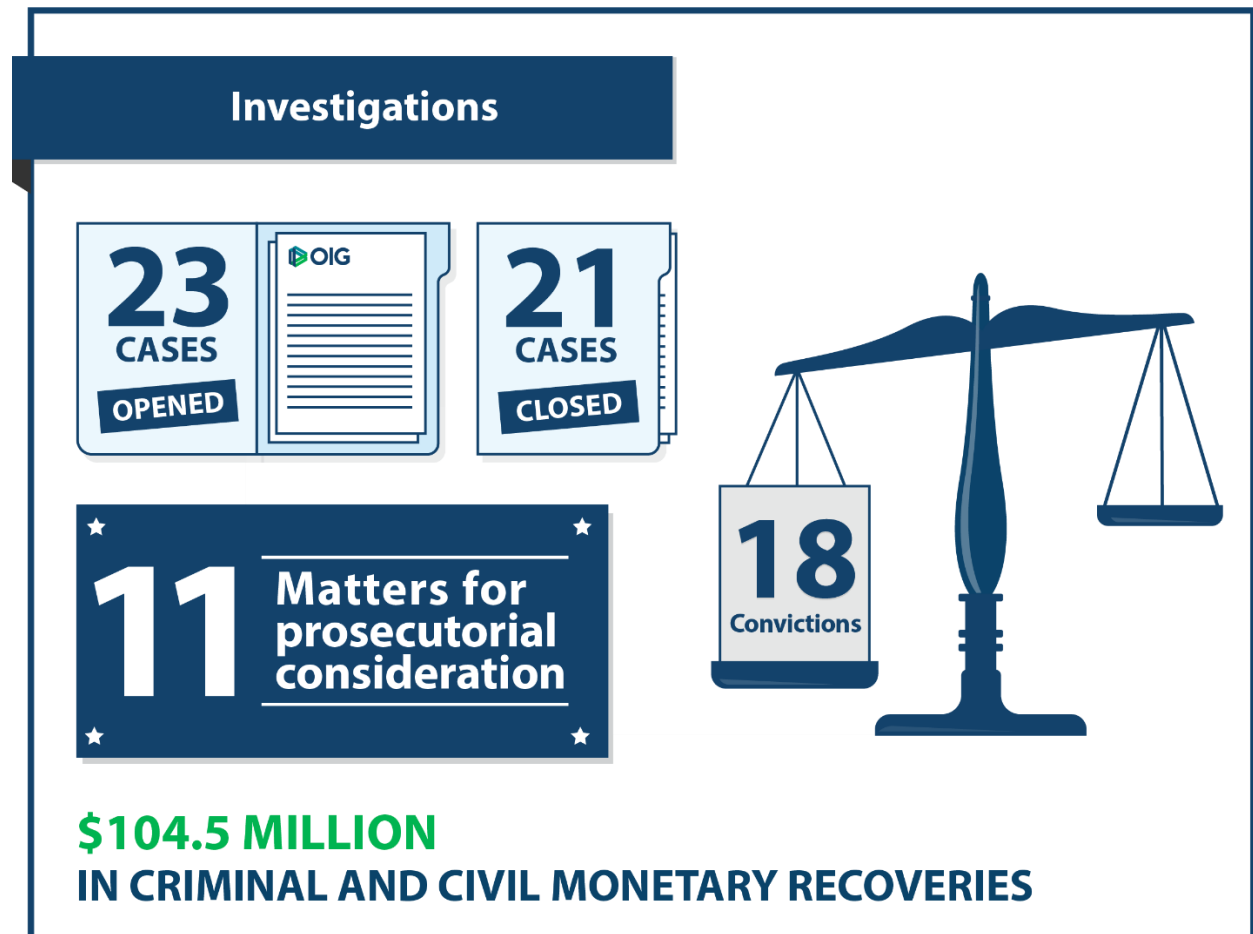
The Board has established and maintained certain controls for its travel card program, but its internal control system needs to be improved to ensure that employees comply with travel requirements.

The Board Can Enhance Its Approach to the Cybersecurity Supervision of Community Banking Organizations

Procedures for information technology (IT) examinations of community banking organizations (CBOs) do not reflect the evolving IT and cybersecurity risk environment and need to be updated. In addition, Federal Reserve Banks have varying approaches to training examiners who conduct CBO IT examinations and completing and retaining documents used to scope such examinations.

The CFPB Can Improve Its Records Management Program

The CFPB is beginning to prepare for the required transfer of permanent records to the National Archives and Records Administration but has not yet provided CFPB divisions with instructions or a timeline for the transfer. In addition, the CFPB should conduct routine formal evaluations of its records management program to help promote effective records management.



Former Bank General Counsel Sentenced to Prison for \$7.4 Million Embezzlement Scheme

James Blose was sentenced in Connecticut to 48 months in prison for an embezzlement scheme he ran at banks where he held high-ranking positions. Over the course of a decade, he stole \$7.4 million by fraudulently retaining closing costs from commercial loans, keeping sale proceeds from real estate transactions, and misusing his attorney trust accounts. He used the funds to purchase real estate, luxury vehicles, and private jet charters.

Investment Adviser Pleaded Guilty to \$45.6 Million Bank Fraud Conspiracy

Jesse T. Hill, an investment adviser, pleaded guilty to conspiracy to commit bank fraud. He attempted to obtain at least \$45.6 million in loans from numerous financial institutions in Nebraska and Iowa by misrepresenting collateral funds and preparing bogus supporting documents. Hill faces up to 30 years in prison and a \$1 million fine. He agreed to pay restitution and forfeit any interest generated from the scheme.

Founders of Lender Service Provider Convicted, Pleaded Guilty for Multimillion-Dollar Pandemic Relief Fraud

Stephanie Hockridge was convicted and Nathan Reis pleaded guilty to a scheme to fraudulently obtain tens of millions of dollars in Paycheck Protection Program (PPP) loans. As cofounders of Blueacorn, a lender service provider based in Arizona, they conspired to submit fraudulent PPP loan applications for small businesses and individuals, charging borrowers illegal kickbacks based on a percentage of the funds received. They each face up to 20 years in prison.



Introduction

Established by Congress, we are the independent oversight authority for the Board and the CFPB. In fulfilling this responsibility, we conduct audits, evaluations, investigations, and other reviews related to Board and CFPB programs and operations.

In accordance with the Inspector General Act of 1978 (5 U.S.C. §§ 401–424), our office has the following responsibilities:

- conduct and supervise independent and objective audits, evaluations, investigations, and other reviews to promote economy, efficiency, and effectiveness in Board and CFPB programs and operations
- help prevent and detect fraud, waste, abuse, and mismanagement in Board and CFPB programs and operations
- review existing and proposed legislation and regulations to make recommendations about possible improvements to Board and CFPB programs and operations
- keep the Board of Governors, the CFPB director, and Congress fully and currently informed

Congress has also mandated additional responsibilities that influence our priorities, including the following:

- Section 15010 of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act; 15 U.S.C. § 9001 note) established the Pandemic Response Accountability Committee (PRAC) within the Council of the Inspectors General on Integrity and Efficiency (CIGIE). PRAC is required to conduct and coordinate oversight of covered funds and the coronavirus response to detect and prevent fraud, waste, abuse, and mismanagement and to identify major risks that cut across programs and agency boundaries. PRAC is also required to submit reports related to its oversight work to relevant federal agencies, the president, and appropriate congressional committees. The CIGIE chair named our inspector general (IG) the acting chair of PRAC, and as such, we hold meetings, conduct oversight activities, and direct reporting responsibilities.
- The Federal Information Security Modernization Act of 2014 (FISMA; 44 U.S.C. § 3555) established a legislative mandate for ensuring the effectiveness of information security controls over resources that support federal operations and assets. In accordance with FISMA requirements, we perform annual independent reviews of the Board’s and the CFPB’s information security programs and practices, including testing the effectiveness of security controls and practices for selected information systems.
- Section 11B of the Federal Reserve Act (12 U.S.C. § 248b) mandates annual independent audits of the financial statements of each Reserve Bank and of the Board. The Board performs the accounting function for the Federal Financial Institutions Examination Council (FFIEC), and we

oversee the annual financial statement audits of the Board and of the FFIEC.¹ Under the Dodd-Frank Wall Street Reform and Consumer Protection Act, the U.S. Government Accountability Office performs the financial statement audit of the CFPB.

- The Payment Integrity Information Act of 2019 (PIIA; 31 U.S.C. §§ 3351–58) requires agency heads to periodically review and identify programs and activities that may be susceptible to significant improper payments. The CFPB has determined that its Civil Penalty Fund is subject to the PIIA. The PIIA requires us each fiscal year to determine whether the agency complies with the act.
- The Government Charge Card Abuse Prevention Act of 2012 (5 U.S.C. § 5701 note and 41 U.S.C. § 1909(d)) requires us to conduct periodic risk assessments and audits of the Board’s and the CFPB’s purchase card, convenience check, and travel card programs to identify and analyze risks of illegal, improper, or erroneous purchases and payments.
- Section 211(f) of the Dodd-Frank Act (12 U.S.C. § 5391(f)) requires that we review and report on the Board’s supervision of any covered financial company that is placed into receivership. We are to evaluate the effectiveness of the Board’s supervision, identify any acts or omissions by the Board that contributed to or could have prevented the company’s receivership status, and recommend appropriate administrative or legislative action.
- Section 989E of the Dodd-Frank Act (5 U.S.C. § 424 note) established the Council of Inspectors General on Financial Oversight (CIGFO), which is required to meet at least quarterly to share information and discuss the ongoing work of each IG, with a focus on concerns that may apply to the broader financial sector and ways to improve financial oversight.² Additionally, CIGFO must report annually about the IGs’ concerns and recommendations, as well as issues that may apply to the broader financial sector. CIGFO can also convene a working group of its members to evaluate the effectiveness and internal operations of the Financial Stability Oversight Council, which was created by the Dodd-Frank Act and is charged with identifying threats to the nation’s financial stability, promoting market discipline, and responding to emerging risks to the stability of the nation’s financial system.
- Section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Act (12 U.S.C. § 1831o(k)), outlines certain review and reporting obligations for our office when a state member bank failure occurs. The nature of those review and reporting requirements depends on the size of the loss to the Deposit Insurance Fund (DIF).
- The Federal Reserve Act, as amended by the USA PATRIOT Act of 2001 (12 U.S.C. § 248(q)), grants the Board certain federal law enforcement authorities. We perform the external oversight function for the Board’s law enforcement program.

¹ The FFIEC is a formal interagency body empowered to (1) prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the CFPB and (2) make recommendations to promote uniformity in the supervision of financial institutions.

² CIGFO comprises the IGs of the Board and the CFPB, the Commodity Futures Trading Commission, the U.S. Department of Housing and Urban Development, the U.S. Department of the Treasury, the Federal Deposit Insurance Corporation, the Federal Housing Finance Agency, the National Credit Union Administration, the U.S. Securities and Exchange Commission, and the Office of the Special Inspector General for the Troubled Asset Relief Program.



Pandemic Response Oversight

In response to the economic disruptions caused by the COVID-19 pandemic, the Board took steps to support the flow of credit to U.S. households and businesses. Notably, the Board used its emergency lending authority under section 13(3) of the Federal Reserve Act to create lending programs, with the approval of the secretary of the U.S. Department of the Treasury, to ensure liquidity in financial markets and to provide lending support to various sectors of the economy. In addition, the CFPB played a vital role throughout the pandemic by enforcing federal consumer protection laws and protecting consumers from abuse.

Although the federal government announced an end to the COVID-19 public health emergency on May 11, 2023, matters related to the lending programs—in particular, investigations of alleged fraud—will continue for the foreseeable future. Two of the Board’s lending facilities are still active. The Main Street Lending Program (MSLP) and the Paycheck Protection Program Liquidity Facility (PPPLF) are in the repayment phase, with borrowers repaying MSLP loans and PPPLF participants providing payments against advances. The Board continues to submit monthly reports to Congress summarizing this activity.

Audits and Evaluations

In 2020, we initiated a pandemic response monitoring effort for risk assessment purposes and as part of our audit planning activities. We primarily focused on the Board’s pandemic response lending programs, which helped to inform our selection of prospective audit and evaluation topics. Although the CFPB was not directly funded by the CARES Act or tasked with CARES Act requirements, the agency played a vital role in protecting consumers from pandemic-related consumer financial fraud and abuse. Since the start of our monitoring effort, we have issued 11 pandemic response–related audit and evaluation reports.

Investigations

Our Office of Investigations is dedicated to identifying and investigating potential fraud related to the lending facilities that are central to the Board’s pandemic response. In conducting our work in this area, we have leveraged our relationships with various federal law enforcement organizations, U.S. attorney’s offices, PRAC, and other offices of inspector general. Since the start of the pandemic, our work has resulted in 171 full investigations; 174 arrests; 142 convictions; and over \$482 million in criminal fines, restitution, civil judgments, and special assessments. During this reporting period, we opened 5 full investigations; made 22 arrests; had 12 convictions; and had over \$91 million in criminal and civil monetary recoveries. Our recent investigative results and recoveries are described in the [Investigations](#) section of this report.



Major Management Challenges

Although not required by statute, we periodically report on the major management challenges facing the Board and the CFPB. These challenges identify the areas that, if not addressed, are most likely to hamper the Board's and the CFPB's accomplishment of their strategic objectives.

For the Board, the major management challenges, in order of significance, are as follows:

- Strengthening Organizational Governance and Enterprise Risk Management
- Managing Workforce Planning and Updating the Human Capital System
- Enhancing Cybersecurity Oversight at Supervised Financial Institutions and Service Providers
- Remaining Adaptable While Supervising Financial Institutions
- Ensuring that Physical Infrastructure Effectively Meets Mission Needs
- Modernizing Information Technology Systems, Services, and Operating Models
- Ensuring an Effective Information Security Program
- Evolving with Financial Sector Innovations
- Leveraging Artificial Intelligence to Enhance Mission Delivery
- Wind-Down of COVID-19 Pandemic Emergency Lending Facilities and Their Underlying Loan Portfolios

The CFPB's major management challenges will be updated at a later date.

See our website for our full [management challenges reports](#).



Audits, Evaluations, and Other Reviews

Audits assess aspects of the economy, efficiency, and effectiveness of Board and CFPB programs and operations. For example, we oversee audits of the Board’s financial statements and conduct audits of (1) the efficiency and effectiveness of the Board’s and the CFPB’s processes and internal controls over their programs and operations; (2) the adequacy of controls and security measures governing these agencies’ financial and management information systems and their safeguarding of assets and sensitive information; and (3) compliance with applicable laws and regulations related to the agencies’ financial, administrative, and program operations. We perform our audits according to *Government Auditing Standards*, issued by the comptroller general of the United States.

Evaluations also assess aspects of the economy, efficiency, and effectiveness of Board and CFPB programs and operations. Evaluations are generally focused on the effectiveness of specific programs or functions; we also conduct our legislatively mandated reviews of failed financial institutions supervised by the Board as evaluations. We perform our evaluations according to *Quality Standards for Inspection and Evaluation*, issued by CIGIE.

Other reviews may include risk assessments, data analytics or other testing, and program and operational reviews that may not be performed in accordance with audit or evaluation standards.

The information below summarizes our audits, evaluations, and other reviews completed during the reporting period.

Board of Governors of the Federal Reserve System

The Board Can Strengthen Its Travel Card Program

2025-FMIC-B-007

May 21, 2025

In 2023, Board employees used government credit cards for about \$8.2 million in travel expenses. The Board participates in the governmentwide U.S. General Services Administration SmartPay Program, which requires employees to apply for and receive government travel cards based on their own credit history. The Board is not subject to federal travel regulations and therefore governs its travel card program under its own policy, which has historically afforded travelers considerable flexibility. The objective of our audit was to determine whether the Board had established and maintained effective internal controls for its government travel card program.

While certain controls have been established and maintained, the Board’s internal control system needs to be improved to ensure that employees comply with travel requirements. We did not find widespread noncompliance but identified multiple instances of significant noncompliance, including employees using their cards for personal expenses and not paying their balances timely. Strengthening the internal control system—including clarifying policy and establishing additional preventative and detective controls, as well as establishing monitoring for travel card misuse and delinquent accounts—can help the Board ensure good stewardship of agency resources and correct use of travel cards by employees.

Our report contains three recommendations to help ensure that the Board’s travel card program has effective internal controls. The Board concurs with our recommendations.

The Board Can Enhance Its Approach to the Cybersecurity Supervision of Community Banking Organizations

2025-SR-B-008

May 28, 2025

Cyber threats are continually evolving and becoming more complex. The Board and the Reserve Banks assess CBOs’ cybersecurity as part of their IT supervisory activities. Reserve Banks use the Information Technology Risk Examination, or InTREx, work programs to assess CBOs’ ability to identify and address IT and cybersecurity risks. We assessed the effectiveness of the Board’s and the Reserve Banks’ cybersecurity supervision approach for CBOs.

The Board can enhance its approach to supervising CBOs for cybersecurity purposes. Specifically, the InTREx work programs do not reflect the evolving IT and cybersecurity risk environment and need to be updated. In addition, selected Reserve Banks’ approaches to CBO IT training vary, and the Federal Reserve System does not provide clear training expectations for generalist examiners assigned to conduct CBO IT examinations. Finally, the Reserve Banks we reviewed had varying practices for completing and retaining IT Profile documents, which examiners use to assess the technology risk of institutions and scope CBO IT examinations.

Our report contains five recommendations to enhance the Board’s approach to its cybersecurity supervision of CBOs. The Board concurs with our recommendations.

The Board’s Law Enforcement Unit Can Clarify Its Authority and Document Processes for Its Physical Security Program

2025-MO-B-010

August 20, 2025

The Board owns four buildings and leases space in two others. To execute its physical security program, the Board’s Law Enforcement Unit protects these facilities with access control systems, surveillance monitoring, security posts, reinforced entry points, and other physical and technical security countermeasures. We evaluated whether the Board has an effective oversight structure to manage its physical security program and whether selected security measures are effective.

While the Board’s physical security program is generally effective, its foundational elements can be strengthened. The Law Enforcement Unit executes the physical security program without formally delegated decisionmaking authority and without established physical security standards. The Board also lacks a process for collecting and deactivating departing employees’ access cards for leased spaces, which creates potential building access vulnerabilities.

Our report contains six recommendations to address these and other issues we identified in our evaluation. The Board concurs with our recommendations.

Consumer Financial Protection Bureau

The CFPB Can Improve Its Safeguards for Protecting Confidential Supervisory Information

2025-SR-C-005

May 5, 2025

In 2023, the CFPB declared a major incident breach that affected about 256,000 consumers and 46 institutions after an examiner sent CSI, including personally identifiable information, to a personal email account. We assessed the CFPB's controls for safeguarding CSI.

CFPB guidance does not effectively limit access to CSI in its system of record for supervision activities and does not sufficiently limit access to CSI used to prioritize supervisory activities. Additionally, the CFPB's guidance for managing CSI breaches does not include expectations for assessing and documenting the severity of breaches and determining, enforcing, and documenting consequences for responsible employees. Further, the agency does not conduct trend analysis on the causes of breaches to determine the appropriate adjustments to controls based on reoccurring themes. Finally, the CFPB does not have a defined process to notify affected supervised institutions of breaches.

Our report contains seven recommendations to improve the CFPB's safeguards for protecting CSI. The CFPB concurs with our recommendations.

Independent Accountants' Report on the CFPB's Fiscal Year 2024 Compliance with the Payment Integrity Information Act of 2019

2025-FMIC-C-006

May 14, 2025

PIIA requires agency heads to periodically review and identify all programs and activities that may be susceptible to significant improper payments. In addition, each fiscal year, the IG of each agency must determine and report on whether the agency complies with the act. We contracted with an independent accounting firm to audit the CFPB's compliance with the PIIA for the Civil Penalty Fund for fiscal year 2024. We reviewed and monitored the work of the firm to ensure compliance with the contract and *Government Auditing Standards*.

The firm determined that the CFPB complied with the applicable requirements of PIIA for fiscal year 2024. Specifically, the CFPB met the first two requirements by (1) publishing an annual financial statement for the most recent fiscal year and posting that report and (2) conducting a program-specific risk assessment for the Civil Penalty Fund. The firm made no recommendations in its report.

The CFPB Can Improve Its Records Management Program

2025-MO-C-009

June 25, 2025

The CFPB creates and maintains both permanent and temporary records in electronic and hard-copy formats. Many of the CFPB's permanent records have a 15-year retention period; therefore, the earliest agency records, created when the agency began operating in 2011, are due for transfer to the National Archives and Records Administration by December 31, 2026. We assessed the CFPB's records management program, including the agency's policies and procedures; responsibilities; and practices for creating, maintaining, and dispositioning records.

The CFPB's Records Management Office is beginning to prepare agency divisions and offices for the required transfer of permanent records to the National Archives and Records Administration by the end of 2026. The office should conduct routine formal evaluations to ensure that agency records are being effectively managed.

Our report contains four recommendations to improve the CFPB's records management program. The CFPB concurs with our recommendations.



Failed State Member Bank Reviews

Material Loss Reviews

Section 38(k) of the Federal Deposit Insurance Act, as amended, requires that we complete a review of the agency's supervision of a failed institution and issue a report within 6 months of notification from the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General that the projected loss to the DIF is material. Section 38(k) defines a material loss to the DIF as an estimated loss in excess of \$50 million.

The material loss review provisions of section 38(k) require that we do the following:

- review the institution's supervision, including the agency's implementation of prompt corrective action
- ascertain why the institution's problems resulted in a material loss to the DIF
- make recommendations for preventing any such loss in the future

No material state member bank failures occurred during the reporting period.

Nonmaterial Loss Reviews

The Federal Deposit Insurance Act, as amended, requires that we semiannually report certain information about financial institutions that incur nonmaterial losses to the DIF and that fail during the 6-month period.

When bank failures result in nonmaterial losses to the DIF, the IG must determine (1) the grounds identified by the federal banking agency or the state bank supervisor for appointing the FDIC as receiver and (2) whether the losses to the DIF present unusual circumstances that would warrant in-depth reviews. Generally, the in-depth review process is the same as that for material loss reviews, but in-depth reviews are not subject to the 6-month reporting deadline.

The IG must semiannually report the completion dates for each such review. If an in-depth review is not warranted, the IG must explain this determination. In general, we consider a loss to the DIF to present unusual circumstances if the conditions associated with the bank's deterioration, ultimate closure, and supervision were not addressed in any of our prior bank failure reports or if there was potential fraud.

No nonmaterial state member bank failures occurred during the reporting period.



Investigations

Our Office of Investigations investigates criminal, civil, and administrative wrongdoing by Board and CFPB employees as well as alleged misconduct or criminal activity that affects the Board's or the CFPB's ability to effectively supervise and regulate the financial community. We operate under statutory law enforcement authority granted by the U.S. attorney general, which vests our special agents with the authority to carry firearms, to seek and execute search and arrest warrants, and to make arrests without a warrant in certain circumstances. Our investigations are conducted in compliance with *Quality Standards for Investigations*, issued by CIGIE, and *Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority*.

The Board is responsible for consolidated supervision of bank holding companies and state-chartered banks that are members of the Federal Reserve System, known as *state member banks*. Under delegated authority from the Board, the Reserve Banks supervise bank holding companies and state member banks, and the Board's Division of Supervision and Regulation oversees the Reserve Banks' supervisory activities. Our investigations concerning bank holding companies and state member banks typically involve allegations that senior officials falsified financial records, lied to or misled examiners, or obstructed examinations.

The CFPB implements and enforces federal consumer financial law and supervises large banks, thrifts, and credit unions with total assets of more than \$10 billion and certain nonbank entities, including mortgage brokers, loan modification providers, payday lenders, consumer reporting agencies, debt collectors, and private education lenders. Our investigations concerning the CFPB's responsibilities typically involve allegations that company directors or officers provided falsified business data and financial records to the CFPB, lied to or misled examiners, or obstructed examinations. Additionally, with certain exceptions, the CFPB's enforcement jurisdiction generally extends to individuals or entities that are engaging or have engaged in conduct that violates federal consumer financial law.

Many of our investigations during this semiannual reporting period concern fraud related to the Federal Reserve's pandemic response efforts, including the MSLP, which supported lending to small and medium-sized for-profit and nonprofit organizations in sound financial condition before the COVID-19 pandemic, and the PPPLF, which extended credit to eligible financial institutions and took PPP loans guaranteed by the U.S. Small Business Administration (SBA) as collateral. In addition, our office also conducted investigations in support of our membership in PRAC. Our office is also part of the U.S. Department of Justice's (DOJ) COVID-19 Fraud Enforcement Task Force.

The following are examples of our investigative activity made public during this reporting period.

Owner of Oklahoma City Nonprofit Indicted for Pandemic Relief Fraud

Victor Kensington Colbert Jr. was indicted on two counts of bank fraud related to a scheme to fraudulently obtain pandemic relief loans. The fact that a defendant has been charged with a crime is merely an accusation, and a defendant is presumed innocent until and unless proven guilty.

According to the allegations, Colbert submitted at least five applications for PPP and Economic Injury Disaster Loan (EIDL) funds on behalf of Heartland Heroes, the nonprofit he owned and operated. He successfully obtained at least two PPP loans and one EIDL totaling about \$217,000. However, to support the applications he submitted false payroll documentation and claimed that any funds he received would be used to retain workers, maintain payroll, and cover operating expenses.

The U.S. Attorney's Office for the Northern District of Oklahoma is prosecuting this case.

Former Bank Executive Sentenced to Prison for \$2 Million Bank Fraud Scheme

Andrew P. Blassie, of Missouri, was sentenced to 63 months in prison for defrauding the Bank of O'Fallon while he served as its executive vice president. He was also ordered to pay over \$2.4 million in restitution.

Blassie admitted to defrauding the bank of about \$2 million by falsely inflating the balance of his personal account by depositing checks he knew to be backed by nonsufficient funds—therefore using bank funds for personal expenses. He used his position as executive vice president to conceal his fraud by scrubbing his name and account number from the bank's reports of suspicious activity. In addition, Blassie admitted to defrauding a couple of their \$429,000 retirement savings.

We investigated this case with the FDIC OIG, the Federal Housing Finance Agency OIG, the O'Fallon Police Department, and the U.S. Secret Service. The U.S. Attorney's Office for the Southern District of Illinois prosecuted.

Former Bank General Counsel Sentenced to Prison for \$7.4 Million Embezzlement Scheme

James Blose, of Connecticut, was sentenced to 48 months in prison followed by 3 years of supervised release for offenses stemming from a decade-long embezzlement scheme at banks where he was employed.

Blose held high-ranking positions, including executive vice president and general counsel, at Hudson Valley Bank, Sterling National Bank, and Webster Bank, where he defrauded his employers in various ways. He retained closing costs from commercial loans and sale proceeds from real estate transactions, and he used his attorney trust accounts to steal \$7.4 million to purchase real estate, luxury vehicles, private jet charters, and more.

We investigated this case with the Federal Bureau of Investigation (FBI) and the Internal Revenue Service (IRS) Criminal Investigation, with assistance from Webster Bank. The U.S. Attorney's Office for the District of Connecticut prosecuted.

New York Tax Preparer Sentenced to Prison for Pandemic Relief Fraud

Baltej Singh Brar, of New York, was sentenced to 2 years in prison for making false statements on PPP loan applications he submitted on behalf of his clients.

Brar owned and operated Aspire Tax & Accounting Services. He filed PPP loan applications on behalf of others in exchange for a flat up-front fee plus 10 percent of the approved loan value. He then falsified information to obtain loans for ineligible borrowers or to obtain larger loans for eligible borrowers. Across hundreds of PPP loan applications, Brar caused at least \$550,000 in losses.

We investigated this case with the FDIC OIG, IRS Criminal Investigation, SBA OIG, U.S. Postal Inspection Service, and the U.S. Secret Service. The U.S. Attorney's Office for the Eastern District of Virginia prosecuted.

Nebraska Investment Adviser Pleaded Guilty to \$45.6 Million Bank Fraud Conspiracy

Jesse T. Hill, of Nebraska, pleaded guilty to conspiracy to commit bank fraud. He faces up to 30 years in prison and a \$1 million fine. Hill also agreed to pay restitution and forfeit any interest generated from the scheme.

Hill was an investment adviser operating in Nebraska. Hill and another individual (now deceased) attempted to obtain at least \$45.6 million in loans from at least 19 financial institutions throughout Nebraska and western Iowa through fraudulent means, including misrepresenting the value of collateral funds and preparing bogus supporting documents. Most of the funds they obtained went into a failed investment scheme or were used to purchase property and an ownership interest in an aircraft.

We investigated this case with the FBI, the FDIC OIG, and the Federal Housing Finance Agency OIG, with assistance from the Nebraska State Patrol, Lincoln Police Department, and the Lancaster County Sheriff's Office. The U.S. Attorney's Office for the District of Nebraska is prosecuting.

Business Owner Sentenced to Prison for \$1.6 Million Pandemic Relief Fraud

Shawn Ray Murnan, of Florida, was sentenced for bank fraud to 33 months in prison followed by 5 years of supervised release. He was also ordered to pay over \$1.6 million in restitution to the SBA.

Murnan, who owned businesses in Oklahoma, Florida, and other states, falsified 14 CARES Act applications to the SBA. He submitted the applications on behalf of his businesses with fraudulent information about employees and payroll expenses. Murnan received over \$1.6 million from seven PPP loans and two EIDLs. After receiving the funds, Murnan applied for the loans to be forgiven.

We investigated this case with the SBA OIG and the U.S. Treasury Inspector General for Tax Administration. The U.S. Attorney's Office for the Northern District of Oklahoma prosecuted.

Founders of Lender Service Provider Convicted, Pleaded Guilty for Multimillion-Dollar Pandemic Relief Fraud

Stephanie Hockridge, of Puerto Rico and previously Arizona, was convicted for a scheme to fraudulently obtain tens of millions of dollars in PPP loans. She faces up to 20 years in prison for conspiracy to commit wire fraud. In addition, Nathan Reis, also of Puerto Rico and previously Arizona, pleaded guilty to conspiracy to commit wire fraud. He faces up to 20 years in prison.

Hockridge and Reis, cofounders of Blueacorn, a lender service provider that purportedly helped small businesses and individuals obtain PPP loans, conspired to submit false and fraudulent PPP loan applications on behalf of themselves and their businesses to receive loan funds for which they were not eligible. To obtain larger loans for certain PPP applicants, they fabricated documents, including payroll records, tax documentation, and bank statements. Hockridge and Reis charged borrowers illegal kickbacks based on a percentage of the funds received.

We investigated this case with the FBI, IRS Criminal Investigation, the SBA OIG, and the Special Inspector General for Pandemic Recovery. The DOJ and the U.S. Attorney's Office for the Northern District of Texas are prosecuting.

Florida Couple Sentenced to Prison for \$6.1 Million Pandemic Relief Fraud

Florida spouses Fawaad Welch and Julia Youngblood were sentenced to a combined 9 years in prison after pleading guilty to defrauding pandemic relief loan programs. Welch was sentenced for wire fraud to 97 months in prison followed by 3 years of supervised release. He was also ordered to pay victims restitution of more than \$6.1 million. Youngblood was sentenced for misprision of a felony to 15 months in prison followed by 1 year of supervised release.

Welch and Youngblood made false statements to obtain loans for their Arkansas business, Slipstream Creative, through the EIDL program and the MSLP. Welch then diverted a large share of the \$6.1 million received for the business to use for his and his partner's benefit, including purchasing real estate.

We investigated this case with the FBI and the Special Inspector General for Pandemic Recovery. The U.S. Attorney's Office for the Western District of Arkansas prosecuted.

Nevada Resident Sentenced to Prison for \$11 Million Pandemic Relief Fraud

Meelad Dezfooli, of Nevada, was sentenced to more than 15 years in prison and 5 years of supervised release for fraudulently obtaining more than \$11 million in PPP loans. He was also ordered to pay restitution of nearly \$11.8 million and forfeit over \$11.2 million, two vehicles, and five properties. Previously, a jury found Dezfooli guilty of three counts of bank fraud, three counts of money laundering, and four counts of conducting transactions using criminally derived property.

Dezfooli submitted three fraudulent PPP loan applications to federally insured banks, purportedly for the benefit of companies that he controlled. Dezfooli falsely represented material information in his loan applications, including about taxes, payroll, employees, and use of the loan proceeds. After obtaining more than \$11.2 million in funds, Dezfooli laundered or spent the proceeds by, among other things, buying 25 residences and two luxury cars, funding a personal investment account, and gambling extensively.

We investigated this case with the FDIC OIG, the IRS Criminal Investigation, and the SBA OIG. The U.S. Attorney's Office for the District of Nevada prosecuted.



Hotline

The [OIG Hotline](#) helps people report fraud, waste, abuse, and mismanagement related to the programs or operations of the Board and the CFPB. Hotline staff can be reached [online](#), by phone, or by mail. We review all incoming hotline communications, research and analyze the issues raised, and determine how best to address the complaints.

During this reporting period, the OIG Hotline received 239 complaints. Complaints within our purview are evaluated and, when appropriate, referred to the relevant component within the OIG for audit, evaluation, investigation, or other review. Some complaints convey concerns about matters within the responsibility of other federal agencies or matters that should be addressed by a program or operation of the Board or the CFPB. We refer such complaints to the appropriate federal agency for evaluation and resolution.

We continue to receive noncriminal consumer complaints regarding consumer financial products and services. For these matters, we typically refer complainants to the consumer group of the appropriate federal regulator for the institution involved, such as the CFPB's Office of Consumer Response, Federal Reserve Consumer Help, or other law enforcement agencies as appropriate. In addition, we receive misdirected complaints regarding COVID-19 pandemic-related programs and operations. In such cases, we refer either the individual or the original complaint to the appropriate agency for further evaluation.



Legislative and Regulatory Review, Congressional and Media Activities, and CIGIE Participation

Legislative and Regulatory Review

Our Office of Legal Services (OLS) is the independent legal counsel to the IG and OIG staff. OLS provides comprehensive legal advice, research, counseling, analysis, and representation in support of our audits, evaluations, and investigations, as well as other professional, management, and administrative functions. OLS also keeps the IG and OIG staff aware of recent legal developments that may affect us, the Board, or the CFPB.

In accordance with the Inspector General Act of 1978 (5 U.S.C. 404(a)(2)), OLS independently reviews newly enacted and proposed legislation and regulations to determine their potential effect on the economy and efficiency of the Board's and the CFPB's programs and operations.

Congressional and Media Activities

The OIG's congressional and media relations function coordinates congressional testimonies and briefings; responds to congressional correspondences and inquiries; and manages all media relations activities, including issuing news releases and statements on behalf of the OIG.

During this reporting period, the IG conducted 12 outreach meetings with members of our oversight committees to talk about our work and hear their feedback regarding the Board and the CFPB.

CIGIE Participation

The IG is a member of CIGIE, which provides a forum for IGs from various government agencies to discuss governmentwide issues and shared concerns. Collectively, CIGIE's members work to improve government programs and operations.

As part of the OIG community, we are proud to be part of the Oversight.gov effort. [Oversight.gov](https://www.oversight.gov) is a searchable website containing the latest public reports from federal OIGs. It provides access to nearly 34,000 reports and more than 12,400 open recommendations to improve programs across the federal government.

In addition, the IG serves as the acting chair of PRAC, which coordinates oversight of federal funds authorized by the CARES Act and the COVID-19 pandemic response.

Our assistant inspector general for information technology, as the chair of the Information Technology Committee of the Federal Audit Executive Council, works with IT professionals throughout the OIG community and reports to the CIGIE Technology Committee on common IT audit issues.

Our OLS attorneys are members of the Council of Counsels to the Inspector General, and our Quality Assurance staff founded the Federal Audit Executive Council’s Quality Assurance Work Group, which in 2023 became a permanent committee called the Quality Management Committee. Our Quality Assurance staff are members of the permanent committee.



Peer Reviews

Government auditing and investigative standards require that our audit, evaluation, and investigative units be reviewed by a peer OIG organization every 3 years. The Inspector General Act of 1978 requires that OIGs provide in their semiannual reports to Congress information about (1) the most recent peer reviews of their respective organizations and (2) their peer reviews of other OIGs conducted within the semiannual reporting period. The following information addresses these requirements.

- In March 2023, the DOJ OIG completed an inspection and evaluation peer review of our evaluation activities. The review team determined that our evaluation policies and procedures are consistent with the December 2020 *Quality Standards for Inspection and Evaluation* and that the reports reviewed generally complied with the covered standards and our internal policies and procedures. There were no pending recommendations from prior peer reviews.
- In September 2023, the OIG for the National Aeronautics and Space Administration conducted a peer review of our audit organization. We received a peer review rating of *pass*. There were no pending recommendations from prior peer reviews.
- In September 2023, the OIG for the U.S. Department of Commerce completed the latest peer review of our Office of Investigations and rated us as *compliant*. There were no report recommendations, and we had no pending recommendations from previous peer reviews of our investigations organization.
- In September 2025, we completed a peer review of the FDIC OIG's audit organization and assigned a *pass* rating. Our report did not contain any recommendations, and there were no pending recommendations from previous peer reviews.

See our website for [peer review reports](#) of our organization.



Appendix A: Statistical Tables

Table A-1. Audit and Evaluation Reports and Other Reviews Issued to the Board During the Reporting Period

Report title	Type of report
The Board Can Strengthen Its Travel Card Program	Audit
The Board Can Enhance Its Approach to the Cybersecurity Supervision of Community Banking Organizations	Evaluation
The Board’s Law Enforcement Unit Can Clarify Its Authority and Document Processes for Its Physical Security Program	Evaluation
Total number of audit reports: 1	
Total number of evaluation reports: 2	

Table A-2. OIG Reports to the Board with Recommendations Open During the Reporting Period

Report title	Issue date	Recommendations			Status		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
2016 Audit of the Board's Information Security Program	11/16	9	9	0	09/25	8	1
The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing	04/17	8	8	0	06/25	7	1
2017 Audit of the Board's Information Security Program	10/17	9	9	0	04/25	8	1
2018 Audit of the Board's Information Security Program	10/18	6	6	0	01/25	5	1
2019 Audit of the Board's Information Security Program	10/19	6	6	0	10/24	4	2
The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems	03/22	3	3	0	03/25	0	3
Testing Results for the Board's Software and License Asset Management Processes (nonpublic)	06/22	1	1	0	09/24	0	1
2022 Audit of the Board's Information Security Program	09/22	1	1	0	06/25	0	1
The Board Can Enhance Certain Governance Processes Related to Reviewing and Approving Supervisory Proposals	12/22	9	9	0	07/25	9	0

See notes at end of table.

Report title	Issue date	Recommendations			Status		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Board Can Further Enhance the Design and Effectiveness of the FOMC's Investment and Trading Rules	04/23	6	6	0	09/25	4	2
Material Loss Review of Silicon Valley Bank	09/23	7	7	0	09/25	2	5
Review of the Supervision of Silvergate Bank (nonpublic)	09/23	12	12	0	09/25	4	8
2023 Audit of the Board's Information Security Program	09/23	7	7	0	06/25	0	7
Results of Security Control Testing of the Board's Embargo Application (nonpublic)	04/24	1	1	0	n.a.	0	1
FRB Minneapolis Followed Its Paycheck Protection Program Liquidity Facility Collateral Risk Management Processes and Can Enhance Monitoring and Collection Processes	09/24	1	1	0	07/25	1	0
2024 Audit of the Board's Information Security Program	10/24	9	9	0	09/25	0	9
The Bank Exams Tailored to Risk Process Promotes Risk-Focused Supervision of Community Banking Organizations, but Training Can Be Enhanced	03/25	2	2	0	08/25	0	2
The Board Can Strengthen Its Travel Card Program	05/25	3	3	0	09/25	1	2
The Board Can Enhance Its Approach to the Cybersecurity Supervision of Community Banking Organizations	05/25	5	5	0	n.a.	0	5

See notes at end of table.

Report title	Issue date	Recommendations			Status		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Board's Law Enforcement Unit Can Clarify Its Authority and Document Processes for Its Physical Security Program	08/25	6	6	0	09/25	1	5

Note: A recommendation is closed if (1) the corrective action has been taken; (2) the recommendation is no longer applicable; or (3) the appropriate oversight committee or administrator has determined, after reviewing the position of the OIG and division management, that no further action by the agency is warranted. A recommendation is open if (1) division management agrees with the recommendation and is in the process of taking corrective action or (2) division management disagrees with the recommendation, and we have referred or are referring it to the appropriate oversight committee or administrator for a final decision.

n.a. not applicable.

Table A-3. Audit and Evaluation Reports and Other Reviews Issued to the CFPB During the Reporting Period

Report title	Type of report
The CFPB Can Improve Its Safeguards for Protecting Confidential Supervisory Information	Evaluation
Independent Accountants’ Report on the CFPB’s Fiscal Year 2024 Compliance with the Payment Integrity Information Act of 2019	Audit
The CFPB Can Improve Its Records Management Program	Evaluation
Total number of audit reports: 1	
Total number of evaluation reports: 2	

Table A-4. OIG Reports to the CFPB with Recommendations Open During the Reporting Period

Report title	Issue date	Recommendations			Status		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
2018 Audit of the Bureau's Information Security Program	10/18	4	4	0	01/25	3	1
Technical Testing Results for the Bureau's Legal Enclave (nonpublic)	07/20	4	4	0	07/25	3	1
2022 Audit of the CFPB's Information Security Program	09/22	6	6	0	01/25	5	1
2023 Audit of the CFPB's Information Security Program	09/23	1	1	0	10/24	0	1
Results of Scoping of the Evaluation of the CFPB's Healthcare Benefits Eligibility Processes	03/24	4	4	0	09/25	2	2
The CFPB Can Enhance Certain Aspects of Its Examiner Commissioning Program	05/24	3	3	0	08/25	0	3
2024 Audit of the CFPB's Information Security Program	10/24	8	8	0	09/25	3	5
The CFPB Can Improve Its Process for Onboarding Depository Institutions that Transition to Its Oversight	12/24	4	4	0	09/25	0	4
The CFPB Can Strengthen Guidance on Cost-Increase Modifications	12/24	1	1	0	08/25	1	0
The CFPB Can Improve Its Safeguards for Protecting Confidential Supervisory Information	05/25	7	7	0	08/25	0	7

See notes at end of table.

Report title	Issue date	Recommendations			Status		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The CFPB Can Improve Its Records Management Program	06/25	4	4	0	n.a.	0	4

Note: A recommendation is closed if (1) the corrective action has been taken; (2) the recommendation is no longer applicable; or (3) the appropriate oversight committee or administrator has determined, after reviewing the position of the OIG and division management, that no further action by the agency is warranted. A recommendation is open if (1) division management agrees with the recommendation and is in the process of taking corrective action or (2) division management disagrees with the recommendation, and we have referred or are referring it to the appropriate oversight committee or administrator for a final decision.

n.a. not applicable.

Table A-5. Audit and Evaluation Reports Issued to the Board and the CFPB During the Reporting Period with Questioned Costs, Unsupported Costs, or Recommendations that Funds Be Put to Better Use

Report	Dollar value
The Board Can Strengthen Its Travel Card Program	\$16,101.28

Note: Because the Board and the CFPB are primarily regulatory and policymaking agencies, our recommendations typically focus on program effectiveness and efficiency, as well as strengthening internal controls. As such, the monetary benefit associated with their implementation typically is not readily quantifiable.

Table A-6. Summary Statistics on Investigations During the Reporting Period

Investigative actions	Number or dollar value ^a
Investigative caseload	
Investigations open at end of previous reporting period	114
Investigations opened during the reporting period	23
Investigations closed during the reporting period	21
Investigations open at end of the reporting period	116
Investigative results for the reporting period	
Persons referred to DOJ prosecutors	11
Persons referred to state/local prosecutors	0
Declinations received	6
Joint investigations	91
Reports of investigation issued	0
Oral and/or written reprimands	0
Terminations of employment	1
Unannounced entries (no-knock entries)	0
Arrests	29
Suspensions	0
Debarments	0
Prohibitions from banking industry	4
Indictments	23
Criminal informations	12

See notes at end of table.

Investigative actions	Number or dollar value ^a
Criminal complaints	0
Convictions	18
Civil actions	\$0
Administrative monetary recoveries and reimbursements	\$0
Civil judgments	\$399,604
Criminal fines, restitution, and special assessments	\$103,792,685
Forfeiture	\$326,999

Note: Some of the investigative numbers may include data also captured by other OIGs.

^a Metrics: These statistics were compiled from our investigative case management and tracking system.

Table A-7. Summary Statistics on Hotline Activities During the Reporting Period

Hotline complaints	Number
Complaints pending from previous reporting period	9
Complaints received during reporting period	239
Total complaints for reporting period	248
Complaints resolved during reporting period	240
Complaints pending	8



Appendix B: Additional Mandated Reporting Requirements

The Inspector General Empowerment Act of 2016 and the Securing Inspector General Independence Act of 2022 amended the semiannual reporting requirements for OIGs under section 5 of the Inspector General Act of 1978 (5 U.S.C. § 405) to include additional summaries and statistics for the reporting period. Our response to these requirements is below.

A report on each investigation in which allegations of misconduct were substantiated involving a senior government employee.

- We have nothing to report.

Detailed descriptions of investigations involving a senior government employee that were closed and not disclosed to the public.

- We have nothing to report.

Detailed descriptions of inspections, evaluations, and audits that were closed and not disclosed to the public.

- We have nothing to report.

A detailed description of any instance of whistleblower retaliation.

- We have nothing to report.

Information related to interference by the Board or the CFPB.

- We have nothing to report.



Appendix C: Open Recommendations Made Before the Reporting Period

The Securing Inspector General Independence Act of 2022 requires that we identify each recommendation made before the reporting period for which corrective action has not been completed, including the cost savings associated with the recommendation. Because the Board and the CFPB are primarily regulatory and policymaking agencies, our recommendations typically focus on program effectiveness and efficiency, as well as strengthening internal controls. As such, the monetary benefit associated with their implementation typically is not readily quantifiable.

Board of Governors of the Federal Reserve System

Table C-1. Reports to the Board Issued Before the Reporting Period with Open Recommendations, by Calendar Year

Year	Number of reports with open recommendations	Number of open recommendations
2016	1	1
2017	2	2
2018	1	1
2019	1	2
2022	3	5
2023	4	22
2024	2	10
2025 ^a	1	2

Note: For any years not listed, all recommendations were closed before the start of the reporting period.

^a Through March 31, 2025.

2016 Audit of the Board's Information Security Program

2016-IT-B-013

November 10, 2016

Total recommendations: 9

Recommendations open: 1

1. Work with the chief operating officer to perform a risk assessment to determine which aspects of an insider threat program are applicable to other types of sensitive Board information and develop and implement an agencywide insider threat strategy for sensitive but unclassified Board information, as appropriate.

The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing

2017-IT-B-009

April 17, 2017

Total recommendations: 8

Recommendations open: 1

1. Reiterate to financial institutions the requirement to notify their primary regulator of the existence of new service relationships, and develop a process to periodically reconcile and refresh the listing of multiregional data processing service firms and technology service providers.

2017 Audit of the Board's Information Security Program

2017-IT-B-018

October 31, 2017

Total recommendations: 9

Recommendations open: 1

8. Develop, implement, and regularly update an information security continuous monitoring strategy that includes performance measures to gauge the effectiveness of related processes and provides agencywide security status.

2018 Audit of the Board's Information Security Program

2018-IT-B-017

October 31, 2018

Total recommendations: 6

Recommendations open: 1

6. Develop and implement a process to assess the knowledge, skills, and abilities of Board staff with significant security responsibilities and establish plans to close identified gaps.

2019 Audit of the Board's Information Security Program

2019-IT-B-016

October 31, 2019

Total recommendations: 6

Recommendations open: 2

5. Work with the System to ensure that the data loss protection replacement solution
 - a. functions consistently across the Board's technology platforms.
 - b. supports rulesets that limit the exfiltration weaknesses we identified, to the extent practicable.
6. Develop and implement a Boardwide process to incorporate the review of data loss protection logs into employee and contractor offboarding processes to identify any potential unauthorized data exfiltrations or access.

The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems

2022-IT-B-006

March 23, 2022

Total recommendations: 3

Recommendations open: 3

1. Ensure that the Cloud Resource Center's inventory of cloud projects in the configuration and production phases is comprehensive and periodically maintained.
2. Develop and implement a process to ensure that the Federal Risk and Authorization Management Program Project Management Office has an accurate inventory of Federal Risk and Authorization Management Program–approved cloud systems used by the Board.
3. Ensure that the Board's information security continuous monitoring standards and associated procedures provide consistent guidance on continuous monitoring frequencies and associated documentation review requirements for cloud service providers.

Testing Results for the Board's Software and License Asset Management Processes (nonpublic)

2022-IT-B-008R

June 15, 2022

Total recommendations: 1

Recommendations open: 1

The open recommendation relates to strengthening software asset management processes.

2022 Audit of the Board's Information Security Program

2022-IT-B-013

September 30, 2022

Total recommendations: 1

Recommendations open: 1

1. Ensure that risks are appropriately categorized and prioritized on the Board's cybersecurity risk register.

The Board Can Further Enhance the Design and Effectiveness of the FOMC's Investment and Trading Rules

2023-SR-B-006

April 26, 2023

Total recommendations: 6

Recommendations open: 2

5. Develop a process to verify the accuracy of the information on financial disclosure reports for individuals subject to the *Investment and Trading Policy for FOMC Officials*. As part of this effort,
 - a. require covered individuals to provide brokerage statements to their respective ethics officer for all accounts with holdings and transactions reported on their annual financial disclosure report.
 - b. update financial disclosure review guidance to include the use of employee-provided brokerage statements to check annual financial disclosure reports for accuracy and completeness.
6. Develop an approach to verify the accuracy of the information on financial disclosure reports for individuals who have access to confidential Class I FOMC information and are not covered by the *Investment and Trading Policy for FOMC Officials*. As part of this effort,
 - a. determine the method and frequency for checking the accuracy and completeness of financial disclosure reports against brokerage statements, for example, by conducting periodic random sampling or full reviews.
 - b. update financial disclosure review guidance to include the use of employee-provided brokerage statements to check annual financial disclosure reports for accuracy and completeness and describe the method and frequency of this review.
 - c. assess the costs and benefits of establishing a system to automatically detect prohibited assets or failure to preclear trades using employee-provided brokerage statements and determine whether to implement such an automated approach.

Material Loss Review of Silicon Valley Bank

2023-SR-B-013

September 25, 2023

Total recommendations: 7

Recommendations open: 5

1. Assess the current regional banking organization (RBO) supervision framework and determine whether adjustments should be made based on a supervised institution's size and complexity, such as unique or concentrated business models or rapid growth. Based on the determination, develop and implement training for RBO Supervision staff that emphasizes the need for varying approaches based on an institution's size, complexity, and business model.
2. Assess whether the Bank Exams Tailored to Risk (BETR) models are appropriate for RBOs, specifically those that are large or complex or that present unique risk factors such as concentrated business models or rapid growth, and determine whether a different approach to determining the scope and resources for examinations is needed.
3. Assess the current RBO supervisory planning process and implement measures to tailor supervisory plans to better promote a timely focus on salient risks.

4. Develop an approach for transitioning institutions from the RBO portfolio to the large and foreign banking organization (LFBO) portfolio and determine how best to involve LFBO Supervision earlier, such as through joint reviews with RBO Supervision, and how to more timely form a dedicated supervisory team. Based on the approach developed, finalize and issue formal guidance on transitioning RBOs to the LFBO portfolio that includes steps and a timeline for forming a dedicated supervisory team, approaches for the two Supervision sections to collaborate, and a list of potential RBO and LFBO joint reviews to conduct to better prepare an institution for the transition.
5. Reiterate to examination teams the purpose of the Risk and Surveillance Sections' reports and the need to closely reflect on their contents to help inform their ongoing supervisory activities.

Review of the Supervision of Silvergate Bank (nonpublic)

2023-SR-B-014R

September 27, 2023

Total recommendations: 12

Recommendations open: 8

1. Update Supervision and Regulation Letter 02-9 to provide additional details on what may constitute a change in the general character of a state member bank's business, including providing examiners with a variety of examples or scenarios that could help them to determine when a bank needs to file an application and receive approval from the Board under Regulation H.
2. Discuss and reinforce the updates made to Supervision and Regulation Letter 02-9 in response to recommendation 1 with Reserve Banks through training.
5. Develop and implement a plan for instructing CBO and RBO examiners to take a forward-looking view of a bank's risk profile and the possible and plausible outcomes of that risk profile when assigning CAMELS composite and component ratings, including
 - a. guidance for examiners on effectively balancing a bank's financial results and condition with its risk profile when assigning CAMELS composite and component ratings, particularly for banks with concentrated business models susceptible to boom and bust cycles.
 - b. guidance for examiners on circumstances that warrant a heightened sense of urgency to initiate CAMELS composite or component ratings downgrades, identify when a bank is exhibiting unsafe or unsound banking practices, or designate a bank as being in "troubled condition."
 - c. required training for examiners that reinforces the guidance developed as part of this recommendation, including scenarios that exemplify the challenges of assigning CAMELS composite and component ratings and the implications of potentially deferring composite or component ratings downgrades when a disconnect has developed between a bank's financial condition and results and its escalating risk profile.
6. Develop guidance for examiners on preparing firms to transition from the CBO portfolio to the RBO portfolio that includes references to updated and relevant guidance applicable to firms that cross the \$10 billion asset size threshold.
7. Develop a plan to minimize the time necessary to establish a new RBO central point of contact and supervisory team for CBOs approaching the \$10 billion asset size threshold.

8. Develop guidance for examiners on supervising firms approaching the \$10 billion total assets threshold that describes
 - a. how to prepare for the transition, including the roles and responsibilities of the Board, the CBO team, and the RBO team, and the expectations for sharing relevant information between the portfolio teams.
 - b. procedures for developing and updating the supervisory plan before, during, and after the transition.
11. Develop guidance for examiners on supervising banks projecting or experiencing rapid growth. The guidance should include
 - a. parameters for identifying significant, rapid growth that may hinder a bank's ability to operate in a safe and sound manner and parameters for identifying when a bank is growing in an unchecked manner based on conditions in the market that have surpassed management's capability to effectively manage it.
 - b. actions examiners should take as a bank projects or experiences such growth or in response to sustained, unchecked growth, including any expected escalations.
 - c. actions examiners should take when supervising banks susceptible to volatile market conditions.
12. Develop guidance for banks projecting or experiencing significant, rapid growth that includes expectations for ensuring that they have requisite staff and risk management capabilities and effective key control functions.

2023 Audit of the Board's Information Security Program

2023-IT-B-015

September 29, 2023

Total recommendations: 7

Recommendations open: 7

1. Prioritize the definition and incorporation of a cybersecurity risk tolerance into the agency's cybersecurity policies, procedures, and processes, as appropriate.
2. Ensure all required attributes are consistently documented within the agency's cybersecurity risk register.
3. Document and implement a process to consistently inventory the Board's web applications, including its public-facing websites.
4. Document and implement a process to consistently inventory and prioritize the Board's third-party systems, including the identification of subcontractors.
5. Enforce the agency's *iOS Update and Device Inactivity Policy* to ensure that agency services are denied to mobile devices that are out of compliance.
6. Develop, document, and implement a process to review and update the Board's privacy impact assessments.
7. Ensure that the process to update privacy impact assessments is adequately resourced for effective implementation.

Results of Security Control Testing of the Board’s Embargo Application (nonpublic)

2024-IT-B-011R

April 10, 2024

Total recommendations: 1

Recommendations open: 1

The open recommendation relates to strengthening access controls.

2024 Audit of the Board’s Information Security Program

2024-IT-B-020

October 31, 2024

Total recommendations: 9

Recommendations open: 9

1. Develop a supply chain risk management strategy that includes
 - a. a supply chain risk appetite and tolerance.
 - b. an enterprise supply chain risk management governance structure.
 - c. supply chain risk assessment processes that include migration strategies or controls.
2. Document and implement a baseline review and escalation process for data loss prevention alerts.
3. Reinforce the requirements for identifying and documenting system interconnections as part of the Board’s training on its cyber risk management application, and require all relevant individuals to take the training.
4. Evaluate and implement options to enforce the agency’s existing guidance related to identifying and documenting system interconnections.
5. Develop and implement a mobile application scanning program that includes a vulnerability scanning solution and process to identify and remediate vulnerabilities.
6. Ensure that the Board’s *Incident Notification and Breach Response Plan* is reviewed, tested, and approved annually.
7. Develop and implement a role-based privacy training program.
8. Incorporate targeted phishing exercises into the Board’s security awareness and training program and processes.
9. Update the Board’s standard language in cloud service provider contracts to ensure that it is consistent with FedRAMP’s *Incident Communications Procedures* incident reporting requirements.

The Bank Exams Tailored to Risk Process Promotes Risk-Focused Supervision of Community Banking Organizations, but Training Can Be Enhanced

2025-SR-B-003

March 3, 2025

Total recommendations: 2

Recommendations open: 2

1. Develop training for examination staff that
 - a. provides an overview of the BETR model risk metrics, adjustment factors, and bump-up rules.
provides an overview of the process for using BETR to scope an examination.
 - b. reinforces the resources and guidance materials available to help.
 - c. examination staff understand these topics.
2. Establish a process to periodically assess the need for additional training as the BETR Program redevelops the models and implements new adjustment factors and bump-up rules.

Consumer Financial Protection Bureau

Table C-2. Reports to the CFPB Issued Before the Reporting Period with Open Recommendations, by Calendar Year

Year	Number of reports with open recommendations	Number of open recommendations
2018	1	1
2020	1	1
2022	1	1
2023	1	1
2024	4	14
2025 ^a	0	0

Note: For any years not listed, all recommendations were closed before the start of the reporting period.

^a Through March 31, 2025.

2018 Audit of the Bureau’s Information Security Program

2018-IT-C-018

October 31, 2018

Total recommendations: 4
Recommendations open: 1

- 3. Determine whether established processes and procedures for management of user-access agreements and rules-of-behavior forms for privileged users are effective and adequately resourced and make changes as needed.

Technical Testing Results for the Bureau’s Legal Enclave (nonpublic)

2020-IT-C-017R

July 22, 2020

Total recommendations: 4
Recommendations open: 1

The open recommendation relates to strengthening configuration management.

2022 Audit of the CFPB’s Information Security Program

2022-IT-C-014

September 30, 2022

Total recommendations: 6

Recommendations open: 1

4. Ensure that an enterprisewide software inventory is conducted and maintained.

2023 Audit of the CFPB’s Information Security Program

2023-IT-C-016

September 29, 2023

Total recommendations: 1

Recommendations open: 1

1. Maintain a comprehensive schedule for testing current contingency plans, documenting test procedures, and maintaining relevant updates to the contingency plan.

Results of Scoping of the Evaluation of the CFPB’s Healthcare Benefits Eligibility Processes

2024-MO-C-010

March 20, 2024

Total recommendations: 4

Recommendations open: 2

2. Ensure that the Office of Human Capital conducts a comprehensive annual review of the control activities for administering the agency’s vision and dental programs to ensure that they are operating effectively.
4. Develop and periodically provide tailored training for employees who administer the agency’s vision and dental programs.

The CFPB Can Enhance Certain Aspects of Its Examiner Commissioning Program

2024-SR-C-013

May 15, 2024

Total recommendations: 3

Recommendations open: 3

1. Issue guidance that clearly defines responsibilities and outlines expectations for those serving in Examiner Commissioning Program (ECP) support roles, including
 - a. mentors on their support during an examiner’s acting examiner in charge (EIC) assignment.
 - b. regional training leads on their support during rotations.
 - c. field managers on providing support, identifying examinations, and selecting acting EIC assignments for examiners pursuing commissioning.
2. Develop a standardized process for Supervision Learning and Development and the regions to collaborate when providing supplemental ECP support to examiners who are preparing for the ECP.

3. Assess the current EIC case study assessment feedback process and determine how to enhance the feedback provided to examiners while safeguarding the content of the EIC case study assessment. Based on the results of the assessment, update guidance to clearly outline expectations for delivering specific, actionable EIC case study assessment feedback and develop and implement training on those expectations.

2024 Audit of the CFPB's Information Security Program

2024-IT-C-019

October 31, 2024

Total recommendations: 8

Recommendations open: 5

1. Complete finalization of an agencywide data classification policy that accounts for the sensitivity of the data maintained by the CFPB.
2. Ensure that data classification and sensitivity labels are incorporated into the CFPB's data loss prevention program.
3. Strengthen flaw remediation processes by developing and implementing a process to clearly map identified vulnerabilities to system IP addresses, host names, and remediation owners within the CFPB's configuration management database.
6. Ensure that testing of mission-essential functions identified in the CFPB's continuity of operations plan is periodically performed.
8. Implement a process that ensures the cyber risk information in the CFPB's governance, risk, and compliance tool is accurate and maintained.

The CFPB Can Improve Its Process for Onboarding Depository Institutions that Transition to Its Oversight

2024-SR-C-021

December 2, 2024

Total recommendations: 4

Recommendations open: 4

1. Establish Supervision's objectives for the onboarding process for transitioning depository institutions.
2. Establish clear roles and responsibilities at the headquarters level for overseeing Supervision's onboarding process.
3. Develop and implement an officewide policy that describes management's expectations for onboarding depository institutions that transition to the CFPB's supervisory oversight. The policy should articulate
 - a. key onboarding steps that the Office of Supervision Examinations should take before and after a depository institution transitions.
 - b. expected time frames for completing the key steps.

- c. guidance on coordinating with the prudential regulator of the onboarding institution, including discussion topics; documentation needs; and the process for managing preexisting supervisory issues, such as Matters Requiring Attention and enforcement actions.
- 4. Develop methods to monitor the Office of Supervision Examinations' execution of the onboarding process, including
 - a. a tracking mechanism to determine whether the key onboarding steps have been completed.
 - b. a process for obtaining feedback from the depository institutions that transitioned regarding the effectiveness of the onboarding process.
 - c. a forum for the regional offices to share their experiences regarding the onboarding process to drive continuous improvement.



Abbreviations

BETR	Bank Exams Tailored to Risk
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CBO	community banking organization
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CSI	confidential supervisory information
DIF	Deposit Insurance Fund
DOJ	U.S. Department of Justice
ECP	Examiner Commissioning Program
EIC	examiner in charge
EIDL	Economic Injury Disaster Loan
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act of 2014
FOMC	Federal Open Market Committee
IG	inspector general
IRS	Internal Revenue Service
IT	information technology
LFBO	large and foreign banking organization
MSLP	Main Street Lending Program
OLS	Office of Legal Services
PIIA	Payment Integrity Information Act of 2019
PPP	Paycheck Protection Program
PPPLF	Paycheck Protection Program Liquidity Facility
PRAC	Pandemic Response Accountability Committee
RBO	regional banking organization
SBA	U.S. Small Business Administration



Office of Inspector General

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

Hotline

Report fraud, waste, abuse, and mismanagement involving the programs and operations of the Board or the CFPB.

oig.federalreserve.gov/hotline

OIG Hotline

Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I 2322
Washington, DC 20551

1 800 827 3340

General Contact Information

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I 2322
Washington, DC 20551

202 973 5000

Media and Congressional Inquiries

oig.media@frb.gov