Semiannual Report to Congress

October 1, 2025–March 31, 2026

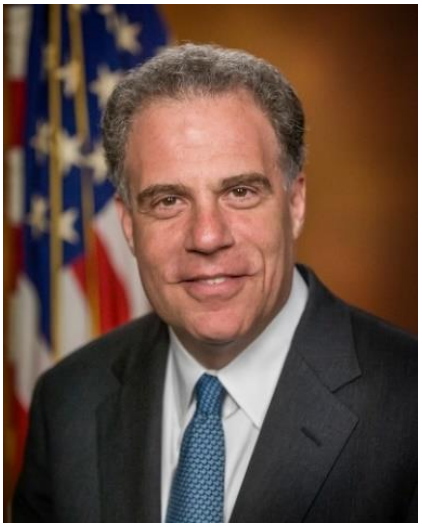
OIG

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 on the operations of the Office of Inspector General for the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau. This report covers the period from October 1, 2025, to March 31, 2026.

During this reporting period, our completed audit and evaluation work included an assessment of the Board and Federal Reserve Banks' approach to processing banking applications. In 2022, the Board implemented FedEZFile, a new document repository and tracking system designed to help reduce delays in the applications process. Despite this and other efficiency measures taken by the Board, processing times across all application types increased between 2021 and 2024. In addition, the Board does not capture sufficient information to pinpoint the root causes of the delays and identify opportunities for improvement. We believe that tracking and documenting key internal milestones in FedEZFile and enhancing monitoring capabilities can help the Board develop solutions that result in a more efficient and timely applications process.

We also completed our annual information security audits for both the Board and the CFPB and found that each agency's program is no longer effective. The Board's information security program declined to a level-3 maturity (*consistently implemented*)—down from level-4 (*managed and measurable*) in 2024—due in part to issues regarding mobile device security and the protection of confidential supervisory information. The CFPB's program declined two levels to a level-2 maturity (*defined*), as we found problems regarding authorizations, continuous monitoring, and outdated software. We issued multiple recommendations to each agency to strengthen these areas in their respective programs.

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 chief financial officer of a Nebraska bank was convicted for submitting fraudulent and inflated invoices from contractors to obtain $4.3 million in loans. In another case, two cofounders of a lender service provider were each sentenced to 10 years in prison and upward of $60 million in restitution for conspiring to submit fraudulent Paycheck Protection Program loan applications and charge borrowers illegal kickbacks. And in a third case, a real estate developer and investor in New York was indicted for allegedly defrauding pandemic relief programs in a scheme that cost taxpayers $8 million.

Overall, the work of our Office of Investigations during this reporting period resulted in 6 arrests, 13 indictments, 7 criminal informations, 20 convictions, 11 referrals for criminal prosecution, and about $171.6 million in civil judgments, forfeiture, criminal fines, restitution, and special assessments.

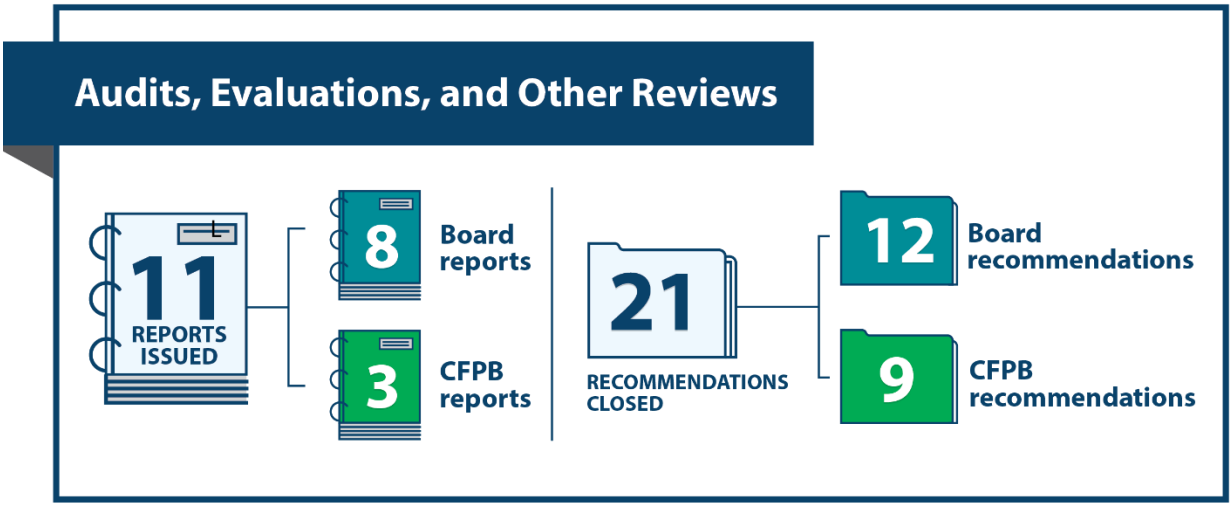
The work summarized in this report reflects our commitment to effective and independent oversight, and it is my honor to have been entrusted to lead this outstanding organization. I am grateful to the OIG staff for their exceptional work, and I look forward to our continued release of impactful reports.

Michael E. Horowitz
Inspector General
April 30, 2026

Contents

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.



2025 Audit of the Board's Information Security Program

The Board's information security program decreased from a level-4 maturity (*managed and measurable*) to a level-3 maturity (*consistently implemented*), leading us to conclude that it is no longer effective.

2025 Audit of the CFPB's Information Security Program

The CFPB's information security program decreased from a level-4 maturity (*managed and measurable*) to a level-2 maturity (*defined*), leading us to conclude that it is no longer effective.

The CFPB Can Enhance Its Processes for Storing and Disposing of Its IT Asset Inventory

The CFPB maintains a large inventory of aging, unassigned information technology (IT) assets and does not identify and dispose of these assets timely or store them in a defined manner.

The Board Should Enhance Its Ability to Monitor the Efficiency and Timeliness of Its Processing of Certain Banking Applications

Despite taking measures to increase efficiency and timeliness, the Board's processing times for certain banking applications increased from 2021 to 2024.

The Board Should More Effectively Manage and Secure Its Inventory of Unassigned Laptops and Hard Drives Ready for Disposal

The Board's inconsistent tracking and management of IT assets—including 677 uninventoried laptops worth over $1.4 million and 5 laptops remaining with former employees—creates an inefficient use of resources and a significant risk of data exfiltration, respectively.

Former Bank Executive Convicted of Bank Fraud in Nebraska

Aaron T. Luneke was convicted by a jury of bank fraud and attempted bank fraud. Abusing his position as chief financial officer of a Nebraska bank, Luneke submitted fraudulent and inflated invoices from contractors to obtain $4.3 million in loans from his bank. He also attempted to defraud another bank for a $3.5 million refinancing loan.

Cofounders of Lender Service Provider Sentenced to Prison for $65 Million Pandemic Relief Fraud

Stephanie Hockridge and Nathan Reis were each sentenced to 10 years in prison and ordered to pay restitution of $63 million and $66 million, respectively, for a scheme to defraud the Paycheck Protection Program (PPP). As cofounders of Blueacorn, a lender service provider based in Arizona, Hockridge and Reis conspired to submit fraudulent PPP loan applications and charge borrowers illegal kickbacks.

New York Developer Charged for $8 Million Pandemic Relief Fraud

David Ebrahimzadeh, a New York real estate developer and investor, was indicted by a federal grand jury for a scheme to defraud the PPP and other pandemic relief programs. Ebrahimzadeh allegedly applied for and received $8.5 million in loans using false and fraudulent information, and then used the proceeds to buy luxury items and real estate.

Introduction

Established by Congress, we are the independent oversight authority for the Board and the CFPB. In accordance with the Inspector General Act of 1978 (5 U.S.C. §§ 401–424), we have 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 recommend 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 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 Federal 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-

[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.

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 to determine the scope, frequency, and number of periodic 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 inspector general (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.

[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 176 full investigations; 179 arrests; 174 convictions; and over $634 million in criminal fines, restitution, special assessments, civil judgments, and forfeitures. During this reporting period, we opened 5 full investigations, made 2 arrests, had 10 convictions, and had over $132 million in criminal and civil monetary recoveries. Our recent investigative results and recoveries are described in the Investigations section of this report.

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 or other testing, as well as 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

2025 Audit of the Board's Information Security Program

2025-IT-B-011R **October 31, 2025**

Each year, we audit the Board's information security program as required by FISMA.

The maturity level of the Board's information security program decreased since 2024, leading us to conclude the program is no longer effective. Challenges in cybersecurity governance, coupled with opportunities to strengthen cybersecurity profiles, mobile device security, and information classification for confidential supervisory information (CSI), contributed to the decline.

We made three recommendations to strengthen the Board's information security program. Given the sensitivity of the information in our review, portions of the public version of this report were redacted.

The Board's Contract Solicitation, Selection, and Award Processes for the Contracts We Reviewed Were Generally Effective but Can Be Further Enhanced

2025-FMIC-B-014 **December 15, 2025**

We reviewed the effectiveness of the Board's contract solicitation, selection, and award processes. Our review was limited to a nonstatistical sample of certain types of contracts for goods and services totaling about $30 million in 2022–2023. Among other exclusions—like governmentwide contracts—we excluded construction contracts because we have ongoing work related to the Board's building renovation projects.

For the 30 sampled contracts we reviewed, the Board generally designed and operated its solicitation, selection, and award processes effectively to help ensure the agency acquires goods and services at the best possible value. However, guidance for using independent government estimates, which can further help ensure that prices are fair and reasonable, was not clear.

Our report does not contain recommendations because, after we presented our draft findings, the Board clarified guidance for independent government estimates.

The Board Has Generally Effective Processes for Approving and Monitoring the Currency Budget's Multicycle Projects but Can Better Document Those Processes

2025-FMIC-B-015 **December 17, 2025**

The Board is the sole issuing authority of the nation's currency, and it pays the Bureau of Engraving and Printing (BEP) for expenses related to producing banknotes. As part of this arrangement, BEP develops a multicycle project budget for its large-scale capital investments (such as production equipment and facilities) that span multiple years.

The Board's processes for approving and monitoring the multicycle project budget are generally effective, providing sufficient resources to the BEP and promoting effective stewardship of funds. However, the Board has not incorporated all of its approval and monitoring processes into its memorandum of understanding with BEP.

We made one recommendation for the Board to incorporate these processes to ensure both parties agree to and are accountable for their respective responsibilities.

Results of Scoping of the Evaluation of the Board's Practices and Controls for Safeguarding Confidential Supervisory Information in OASIS

2026-SR-B-001 **February 3, 2026**

The Board's OASIS technology platform, which examiners use to document their supervisory activities of the nation's largest financial institutions, contains CSI. The loss or misuse of CSI could result in significant legal, reputational, or financial risk to the Board, Reserve Banks, financial institutions, and individuals.

We identified several concerns regarding CSI access in OASIS, which the Board must address before we conduct further work. For example, users have more access to sensitive information than appears to be warranted based on their specific financial institution examination assignments, which is inconsistent with Board policy and a key information security principle.

We made four recommendations to enhance the Board's practices and controls for safeguarding CSI in OASIS.

Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2025 and 2024, and Independent Auditors' Report

2026-FMIC-B-002 **March 3, 2026**

The Board performs the accounting function for the FFIEC, and we contracted with an independent public accounting firm to audit the FFIEC's financial statements as of and for the years ended December 31, 2025 and 2024.

In the firm's opinion, the financial statements present fairly, in all material respects, the financial position of the FFIEC.

Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2025 and 2024, and Independent Auditors' Reports

2026-FMIC-B-003 **March 12, 2026**

We contracted with an independent public accounting firm to audit the Board's financial statements as of and for the years ended December 31, 2025 and 2024.

In the firm's opinion, the financial statements present fairly, in all material respects, the financial position of the Board, and the Board maintained effective control over financial reporting.

The Board Should Enhance Its Ability to Monitor the Efficiency and Timeliness of Its Processing of Certain Banking Applications

2026-SR-B-004 **March 23, 2026**

Before engaging in certain activities like mergers or acquisitions, banks must apply for approval from Reserve Banks or the Board, which review applications for legal issues and considerations and for safety and soundness principles.

Despite recent measures to increase efficiency, median application processing times increased from 2021 to 2024—by about 11 percent for all application types and by about 40 percent for small community bank mergers and acquisitions. Board officials and staff cited numerous reasons for delays, such as time needed to consult with other regulatory agencies and conduct internal reviews before final action. We could not validate these explanations for the delays, because the Board does not track sufficient information to pinpoint opportunities for improvement.

We made three recommendations to enhance the Board's efforts to increase the efficiency and timeliness of the banking application process.

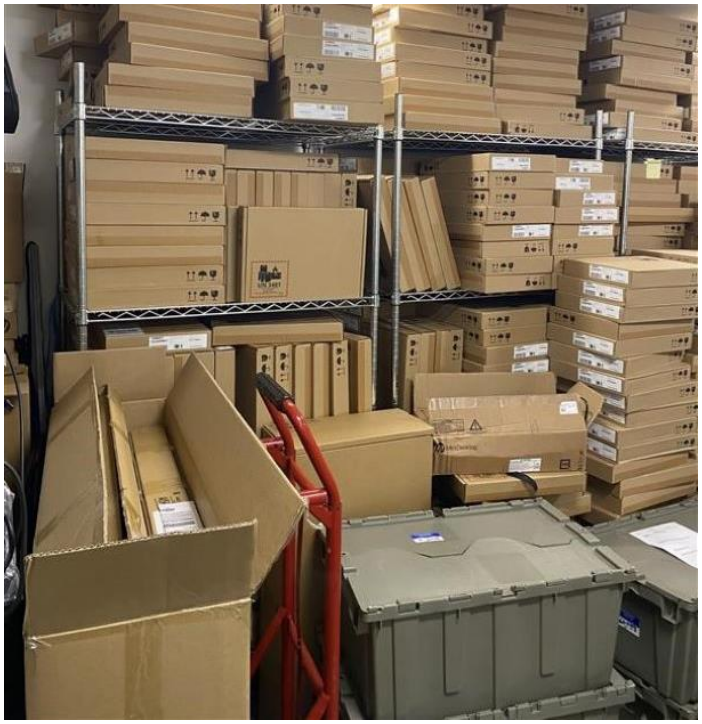
The Board Should More Effectively Manage and Secure Its Inventory of Unassigned Laptops and Hard Drives Ready for Disposal

2026-FMIC-B-005 **March 30, 2026**

A lack of standardization in managing IT assets increases the risk that Board data may be exfiltrated.

We found that the Board does not consistently track and account for all its laptops. For example, 677 laptops worth over $1.4 million sat uninventoried and in storage for 8 months before being properly inventoried in March 2026. Further, several laptops were still in the possession of former employees, putting data at risk of compromise. Among other issues we identified, some IT asset storage rooms, though secured, lack safeguards like access logs.

Uninventoried Laptops



Source: OIG.

We made seven recommendations to ensure that the Board standardizes inventory management consistent with leading practices.

Consumer Financial Protection Bureau

2025 Audit of the CFPB's Information Security Program

2025-IT-C-012 **October 31, 2025**

Each year, we audit the CFPB's information security program as required by FISMA.

The maturity level of the CFPB's information security program has decreased since 2024, leading us to conclude the program is no longer effective. For example, authorizations to operate for many systems are not maintained, risk acceptance memorandums lack documented analysis of cybersecurity risks, and outdated software remains in use. While the agency was able to maintain or even strengthen information security in some areas, such as transitioning to continuous vetting of employees, those efforts do not mitigate the overall decline.

We made six recommendations to strengthen the CFPB's information security program.

The CFPB Can Enhance Its Processes for Storing and Disposing of Its IT Asset Inventory

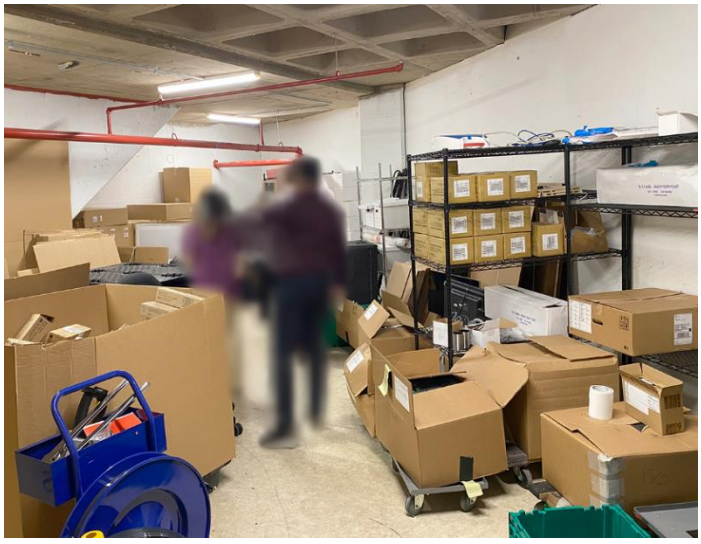
2025-FMIC-C-013 **November 4, 2025**

In 2024, we received a referral that the CFPB could not account for 74 newly purchased laptops, which it believed were lost or stolen as a result of potential control weaknesses during receiving and inventorying.

Our audit activities revealed that the CFPB established and followed internal controls that addressed many of those weaknesses. However, the agency still maintains a large inventory of aging, unassigned IT assets and has not established processes to effectively manage the storage or reduction of its inventory. Systematically organizing and better managing the reduction of IT assets will help to limit the risk of loss or theft, save space and time, and protect agency data.

We made two recommendations to strengthen the CFPB's storage and disposition practices, which should be addressed urgently as workforce reductions will likely result in an influx of returned IT assets.

CFPB Storage Room for In-Stock IT Assets



Source: OIG.

Fiscal Years 2023–2024 Risk Assessment of the CFPB's Government Travel Card Program

March 10, 2026

Over 44,000 purchases totaling about $10.5 million were made on CFPB government travel cards during fiscal years 2023–2024.

Our assessment of the CFPB's government travel card program shows that the risk of illegal, improper, or erroneous use of the cards is low. Since our review, and in response to Executive Order 14222 and a directive from the General Services Administration, the CFPB changed its approach to official travel, including by centralizing government travel card program elements and significantly reducing travel in calendar year 2025. We plan to assess the effect of these changes in future risk assessments.

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 Board'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 Board'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, we 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.

Former Bank Executive Convicted of Bank Fraud in Nebraska

Aaron T. Luneke, of Nebraska, was convicted by jury of bank fraud and attempted bank fraud. Luneke faces up to 30 years in prison and a fine of up to $1 million for each count.

Luneke abused his position as chief financial officer of Bank of the Valley by submitting fraudulent and inflated invoices from contractors as the basis for loan proceeds for a carwash construction project,

obtaining two loans from his bank totaling about $4.3 million. He also attempted to defraud a Minnesota bank by using fraudulent contractor invoices to artificially inflate the valuation of the car wash property in pursuit of a $3.5 million refinancing loan. Luneke failed to disclose significant personal debts owed to family members in connection with the application. He also relied on a series of corporate shell entities to conceal that additional individuals were benefiting from his ownership interest in the car wash.

We investigated this case with the Federal Bureau of Investigation (FBI), FDIC OIG, and Federal Housing Finance Agency OIG. The U.S. Attorney's Office for the District of Nebraska is prosecuting.

Nebraska Residential Builder Convicted of Three Counts of Wire Fraud

Bryce A. Nolde, of Nebraska, was convicted by a federal jury of three counts of wire fraud. Each count carries up to 30 years in prison and a fine of up to $1 million. Nolde could also be ordered to pay restitution to the victims of his crimes.

Nolde operated BV Builders, a residential construction company. The company took large downpayments or drew large amounts from customers' construction loans to purportedly pay subcontractors and suppliers for the customers' builds. But, instead of new homes, customers were left with construction liens on their property after Nolde used the money for himself rather than pay the subcontractors and suppliers for their work. Dozens of victims testified at trial to the devastating financial crimes.

We investigated this case with the FBI, FDIC OIG, Federal Housing Finance Agency OIG, and the Nebraska State Patrol. The U.S. Attorney's Office for the District of Nebraska is prosecuting.

Unfinished Residential Construction

Source: Government exhibits.

Cofounders of Lender Service Provider Sentenced to Prison for $65 Million Pandemic Relief Fraud

Stephanie Hockridge and Nathan Reis, of Puerto Rico and previously Arizona, were each sentenced to 10 years in prison for their scheme to fraudulently obtain about $65 million in PPP loans. Hockridge was ordered to pay over $63 million in restitution, and Reis was ordered to pay over $66 million in restitution.

Hockridge was found guilty by jury of one count of conspiracy to commit wire fraud, and Reis pleaded guilty to conspiracy to commit wire fraud.

Hockridge and Reis cofounded Blueacorn, a lender service provider that purportedly helped small businesses and individuals obtain PPP loans. However, Hockridge and Reis conspired to submit false and fraudulent PPP loan applications on behalf of themselves and their businesses to receive loan funds they were not eligible for. 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 the borrowers received. In total, the scheme involved more than 530 fraudulent loans and caused over $65 million in losses.

We investigated these cases with the FBI, Internal Revenue Service Criminal Investigation, Special Inspector General for Pandemic Recovery, and SBA OIG. The DOJ and the U.S. Attorney's Office for the Northern District of Texas prosecuted.

New York Developer Charged for $8 Million Pandemic Relief Fraud

David Ebrahimzadeh, a New York real estate developer and investor, was charged for a scheme to defraud pandemic relief programs. He was indicted by a federal grand jury on one count of bank fraud, two counts of wire fraud affecting a financial institution, one count of wire fraud, and two counts of procuring a false tax return. Sentences for the charges range from 3 to 30 years in prison and fines of up to $1 million, or twice the gross gain or loss, whichever is greater. 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, Ebrahimzadeh operated Corniche Capital, LLC, as a holding company for various commercial real estate limited liability companies. Under SBA rules, such businesses were ineligible for loans through the PPP, the Economic Injury Disaster Loan program, and the MSLP. However, Ebrahimzadeh applied for and received loans using false and fraudulent information, including about revenue and payroll. He also applied for loans for a number of companies that had been dissolved years before the pandemic. Ebrahimzadeh spent loan proceeds on luxury items, personal and business debt, and homes on Long Island. In total, Ebrahimzadeh allegedly obtained about $8.5 million in loans he was not entitled to.

We are investigating this case with the FBI and Internal Revenue Service Criminal Investigation, with assistance from the Special Inspector General for Pandemic Recovery. The U.S. Attorney's Office for the District of Massachusetts is prosecuting.

Virginia Men Indicted for Conspiring to Destroy Government Databases

Brothers Muneeb Akhter and Sohaib Akhter, of Virginia, were indicted for their roles in a conspiracy to destroy government databases hosted by a federal government contractor, among other crimes. Muneeb Akhter was charged with conspiracy to commit computer fraud and to destroy records, two counts of computer fraud, theft of U.S. government records, and two counts of aggravated identity theft. Sohaib

Akhter was charged with conspiracy to commit computer fraud and to destroy records and computer fraud (password trafficking). Sentences for the charges against Muneeb Akhter range from 2 to 45 years in prison. Sentences for the charges against Sohaib Akhter carry up to 6 years in prison. 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, both men were federal contractors. After being terminated from their employment, the brothers allegedly sought to harm the company and its federal customers by accessing computers without authorization, issuing commands to prevent others from modifying the databases before deletion, deleting databases, stealing information, and destroying evidence of their unlawful activities. About 96 databases were deleted, many containing records and documents related to Freedom of Information Act matters and sensitive federal investigative files. The brothers then attempted to conceal their actions.

We are investigating this case with the U.S. Department of Homeland Security, FDIC OIG, and Homeland Security Investigations, with assistance from over a dozen OIGs and federal and local law enforcement partners. The DOJ and U.S. Attorney's Office for the Eastern District of Virginia are prosecuting.

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 194 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 our office, 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 20 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. The website contains public reports from federal OIGs, providing access to over 35,000 reports and about 12,770 open recommendations to improve programs across the federal government.

In addition, through March 2026, the IG served 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.

- In September 2023, the OIG for the National Aeronautics and Space Administration assigned a *pass* rating to our audit operations. There were no new or pending report recommendations.
- In February 2026, the Treasury Inspector General for Tax Administration assigned a *pass* rating to our evaluation operations. There were no new or pending report recommendations.
- In September 2023, the OIG for the U.S. Department of Commerce rated our investigative operations as *compliant*. There were no new or pending report recommendations.

See our website for the full peer review reports.

We did not conduct any peer reviews of other OIGs during the reporting period.

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
2025 Audit of the Board's Information Security Program	Audit
The Board's Contract Solicitation, Selection, and Award Processes for the Contracts We Reviewed Were Generally Effective but Can Be Further Enhanced	Audit
The Board Has Generally Effective Processes for Approving and Monitoring the Currency Budget's Multicycle Projects but Can Better Document Those Processes	Audit
Results of Scoping of the Evaluation of the Board's Practices and Controls for Safeguarding Confidential Supervisory Information in OASIS	Evaluation
Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2025 and 2024, and Independent Auditors' Report	Audit
Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2025 and 2024, and Independent Auditors' Reports	Audit
The Board Should Enhance Its Ability to Monitor the Efficiency and Timeliness of Its Processing of Certain Banking Applications	Evaluation
The Board Should More Effectively Manage and Secure Its Inventory of Unassigned Laptops and Hard Drives Ready for Disposal	Audit
Total number of audit reports: 6 Total number of evaluation reports: 2	

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

Report title	Issue date	Recommendations			Status		
		Number	Management agrees	Management disagrees	Last follow-up	Closed	Open
2016 Audit of the Board's Information Security Program	11/16	9	9	0	02/26	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	03/26	7	1
2017 Audit of the Board's Information Security Program	10/17	9	9	0	10/25	9	0
2018 Audit of the Board's Information Security Program	10/18	6	6	0	02/26	5	1
2019 Audit of the Board's Information Security Program	10/19	6	6	0	10/25	4	2
The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems	03/22	3	3	0	01/26	1	2
Testing Results for the Board's Software and License Asset Management Processes (nonpublic)	06/22	1	1	0	11/25	0	1
2022 Audit of the Board's Information Security Program	09/22	1	1	0	10/25	1	0
The Board Can Further Enhance the Design and Effectiveness of the FOMC's Investment and Trading Rules	04/23	6	6	0	03/26	4	2
Material Loss Review of Silicon Valley Bank	09/23	7	7	0	03/26	2	5

See notes at end of table.

Report title	Issue date	Recommendations			Status		
		Number	Management agrees	Management disagrees	Last follow-up	Closed	Open
Review of the Supervision of Silvergate Bank (nonpublic)	09/23	12	12	0	03/26	4	8
2023 Audit of the Board's Information Security Program	09/23	7	7	0	03/26	3	4
Results of Security Control Testing of the Board's Embargo Application (nonpublic)	04/24	1	1	0	11/25	0	1
2024 Audit of the Board's Information Security Program	10/24	9	9	0	02/26	2	7
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	03/26	1	1
The Board Can Strengthen Its Travel Card Program	05/25	3	3	0	03/26	3	0
The Board Can Enhance Its Approach to the Cybersecurity Supervision of Community Banking Organizations	05/25	5	5	0	03/26	0	5
The Board's Law Enforcement Unit Can Clarify Its Authority and Document Processes for Its Physical Security Program	08/25	6	6	0	03/26	1	5
2025 Audit of the Board's Information Security Program	10/25	3	3	0	03/26	0	3
The Board Has Generally Effective Processes for Approving and Monitoring the Currency Budget's Multicycle Projects but Can Better Document Those Processes	12/25	1	1	0	03/26	1	0

See notes at end of table.

Report title	Issue date	Recommendations			Status		
		Number	Management agrees	Management disagrees	Last follow-up	Closed	Open
Results of Scoping of the Evaluation of the Board's Practices and Controls for Safeguarding Confidential Supervisory Information in OASIS	02/26	4	4	0	03/26	0	4
The Board Should Enhance Its Ability to Monitor the Efficiency and Timeliness of Its Processing of Certain Banking Applications	03/26	3	3	0	n.a.	0	3
The Board Should More Effectively Manage and Secure Its Inventory of Unassigned Laptops and Hard Drives Ready for Disposal	03/26	7	7	0	n.a.	0	7

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
2025 Audit of the CFPB's Information Security Program	Audit
The CFPB Can Enhance Its Processes for Storing and Disposing of Its IT Asset Inventory	Audit
Fiscal Years 2023–2024 Risk Assessment of the CFPB's Government Travel Card Program	Evaluation
Total number of audit reports: 2 Total number of evaluation reports: 1	

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

Report title	Issue date	Recommendations			Status		
		Number	Management agrees	Management disagrees	Last follow-up	Closed	Open
2018 Audit of the Bureau's Information Security Program	10/18	4	4	0	10/25	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	10/25	5	1
2023 Audit of the CFPB's Information Security Program	09/23	1	1	0	10/25	0	1
Results of Scoping of the Evaluation of the CFPB's Healthcare Benefits Eligibility Processes	03/24	4	4	0	03/26	4	0
The CFPB Can Enhance Certain Aspects of Its Examiner Commissioning Program	05/24	3	3	0	03/26	0	3
2024 Audit of the CFPB's Information Security Program	10/24	8	8	0	10/31	3	5
The CFPB Can Improve Its Process for Onboarding Depository Institutions That Transition to Its Oversight	12/24	4	4	0	12/25	4	0
The CFPB Can Improve Its Safeguards for Protecting Confidential Supervisory Information	5/25	7	7	0	03/26	3	4
The CFPB Can Improve Its Records Management Program	6/25	4	4	0	03/26	0	4
2025 Audit of the CFPB's Information Security Program	10/25	6	6	0	n.a.	0	6

See notes at end of table.

Report title	Issue date	Recommendations			Status		
		Number	Management agrees	Management disagrees	Last follow-up	Closed	Open
The CFPB Can Enhance Its Processes for Storing and Disposing of Its IT Asset Inventory	11/25	2	2	0	03/26	0	2

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 Should More Effectively Manage and Secure Its Inventory of Unassigned Laptops and Hard Drives Ready for Disposal	$1.447 million

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
Investigative caseload	
Investigations open at end of previous reporting period	116
Investigations opened during the reporting period	25
Investigations closed during the reporting period	24
Investigations open at end of the reporting period	117
Investigative results for the reporting period	
Persons referred to DOJ prosecutors	10
Persons referred to state/local prosecutors	1
Declinations received	7
Joint investigations	93
Reports of investigation issued	0
Oral and/or written reprimands	0
Terminations of employment	2
Unannounced entries (no-knock entries)	0
Arrests	6
Suspensions	0
Debarments	0
Prohibitions from banking industry	2

See note at end of table.

Investigative actions	Number or dollar value
Indictments	13
Criminal informations	7
Criminal complaints	0
Convictions	20
Civil actions	$0
Administrative monetary recoveries and reimbursements	$0
Civil judgments	$0
Criminal fines, restitution, and special assessments	$171,152,955
Forfeiture	$430,437

Note: These statistics were compiled from our investigative case management and tracking system. Some statistics may include data also captured by other OIGs.

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

Hotline complaints	Number
Complaints pending from previous reporting period	8
Complaints received during reporting period	194
Total complaints for reporting period	202
Complaints resolved during reporting period	198
Complaints pending	4

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	1	1
2018	1	1
2019	1	2
2022	2	3
2023[a]	4	19
2024	2	8
2025[b]	3	11

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

[a] Our follow-up activities are on hold for 13 of the 19 open recommendations from 2023. The Board is considering the strategic direction of aspects of its supervision program related to these 13 recommendations, which were issued in two reports, *Material Loss Review of Silicon Valley Bank* and *Review of the Supervision of Silvergate Bank*.

[b] Through September 30, 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 servicer firms and technology service providers.

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 Federal Reserve 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: 2

1. Ensure that the Cloud Resource Center's inventory of cloud projects in the configuration and production phases is comprehensive and periodically maintained.

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.

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 community banking organization (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: 4

1. Prioritize the definition and incorporation of a cybersecurity risk tolerance into the agency's cybersecurity policies, procedures, and processes, as appropriate.
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.

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: 7

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.

8. Incorporate targeted phishing exercises into the Board's security awareness and training program and processes.

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: 1

1. Develop training for examination staff that
   a. provides an overview of the BETR model risk metrics, adjustment factors, and bump-up rules.
   b. provides an overview of the process for using BETR to scope an examination.
   c. reinforces the resources and guidance materials available to help examination staff understand these topics.

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

2025-SR-B-008 **May 28, 2025**

Total recommendations: 5
Recommendations open: 5

1. Assess whether the Information Technology Profile (ITP) and InTREx work programs used by Reserve Bank examiners address emerging IT and cybersecurity risks and, based on this assessment, provide supplemental guidance and customize the ITP and InTREx work programs for System-led examinations as needed.

2. Establish a process to periodically assess whether the ITP and InTREx work programs used by Reserve Bank examiners, including the Board's customized guidance, address current material risks in the IT and cybersecurity environment and update the ITP and InTREx work programs as needed.

3. Clarify accountability for defining Systemwide CBO IT and cybersecurity training requirements.

4. Develop IT and cybersecurity training guidance that describes expectations for generalist examiners conducting CBO IT examinations, including expectations for on-the-job training and expectations following the completion of the CBO Examiner Commissioning Program (ECP).

5. Clarify in guidance the expectations for updating and reaffirming responses in ITPs and retaining ITPs for each IT examination in the appropriate system of record, and expectations for assessing ongoing compliance.

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**

Total recommendations: 6
Recommendations open: 5

2. Establish and document physical security standards for the agency that include a risk-based decisionmaking framework to
   a. raise and resolve physical security considerations and concerns.
   b. document physical security decisions, including describing the rationale for any deviations from physical security standards.
3. Assign responsibility for managing third-party access cards for Board-leased spaces.
4. Ensure that the responsible group develops and implements a process to
   a. collect and deactivate third-party access cards from offboarded Board personnel.
   b. periodically reconcile third-party access card rights against human resources' list of active Board employees and contractors.
5. Establish a policy that defines the Technical Security Bureau's responsibilities and the standard operating procedures needed to fulfill those responsibilities.
6. Develop and document
   a. measurable performance objectives for the Technical Security Bureau's responsibilities.
   b. a monitoring process to assess the Technical Security Bureau's progress toward achieving those objectives.

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	2	8
2025[a]	2	8

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

[a] Through September 30, 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

4. 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.

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 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 Safeguards for Protecting Confidential Supervisory Information

2025-SR-C-005 May 5, 2025

Total recommendations: 7
Recommendations open: 4

3. Develop and require training for CFPB staff involved in the examination process for the policy and guidance resulting from recommendations 1 and 2.

5. Update the guidance for managing breaches of CSI to include expectations for
   a. assessing and documenting the level of harm associated with a breach.
   b. counseling, training, or taking other measures to hold CFPB staff responsible for breaches accountable, as appropriate, and documenting such actions.
   c. analyzing the causes of breaches to identify trends and implement appropriate control adjustments, as necessary.
6. Develop required training on the updated guidance after it is implemented.
7. Update the CFPB's confidential information breach response directive to
   a. provide guidance for assessing the risk to institutions affected by breaches of CSI and notifying those institutions.
   b. define the roles and responsibilities for those involved in the process.

The CFPB Can Improve Its Records Management Program

2025-MO-C-009 June 25, 2025

Total recommendations: 4
Recommendations open: 4

1. Communicate to divisions and offices and Record Liaison Officers general instructions, including an expected timeline, for transferring permanent records to National Archives and Records Administration, and monitor their timely execution.

2. Establish a routine formal records management evaluations process to ensure that agency records management activities comply with federal regulations.

3. Establish a remediation process for instances of noncompliance identified during routine evaluations.
4. Identify the resources needed to routinely complete records management evaluations.

Abbreviations

BEP	Bureau of Engraving and Printing
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
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
IT	information technology
ITP	Information Technology Profile
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