

Office of Inspector General

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

Semiannual Report to Congress

April 1, 2023–September 30, 2023



Semiannual Report to Congress

April 1, 2023–September 30, 2023



Office of Inspector General

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

Message From the Inspector General



This spring, turmoil in the banking industry captured headlines and raised questions about the stability of certain segments of the financial system. In March, Silicon Valley Bank, headquartered in Santa Clara, California, failed and was placed into receivership, ultimately costing the Deposit Insurance Fund (DIF) an estimated \$16.1 billion. Earlier that same week, the holding company for Silvergate Bank, headquartered in La Jolla, California, announced its intent to begin voluntarily liquidating the bank. In separate reports, we assessed the Board of Governors of the Federal Reserve System's and the Federal Reserve Bank of San Francisco's (FRB San Francisco) supervision of each institution. We made 19 recommendations to improve the Board and FRB San Francisco's supervisory processes.

In July, Heartland Tri-State Bank, located in Elkhart, Kansas, failed and was placed into receivership. At the time of its failure, the loss to the DIF was estimated to be about \$54 million. Our material loss review of Heartland Tri-State Bank will be completed early next year.

Last year, the Board's Federal Open Market Committee (FOMC) adopted a new personal investment and trading policy that prohibits covered individuals from purchasing individual securities, restricts active trading, and revises public reporting and disclosure requirements. We assessed the design and effectiveness of this policy as well as the Board's and the Federal Reserve Banks' approach to monitoring potential conflicts of interest. We determined that the new policy can be significantly enhanced by extending requirements that apply to senior FOMC officials to additional staff who have access to confidential FOMC information, by strengthening ethics programs to make reviews of financial disclosure reports more uniform throughout the Federal Reserve System and to enforce consequences for policy violations, and by verifying the completeness and accuracy of information provided in financial disclosure reports.

Information security remains another key area of focus for both the Board and the Consumer Financial Protection Bureau. We recently evaluated the Board and Reserve Banks' process for responding to cybersecurity incidents at supervised financial institutions and found that guidance documents do not clearly describe the mission or governance structure of the cybersecurity incident response process and that responses to such incidents have not consistently followed the established process. In addition, in a separate evaluation, we assessed the Board's and Reserve Banks' controls for protecting sensitive, nonpublic information in certain examination applications used for supervising community and regional banks. We found that examiners do not consistently use a process to help purge sensitive documents that

are not required to be retained and that some examiners may have access to more sensitive personally identifiable information than is necessary for their job duties.

We conducted a performance audit of the CFPB's Agile systems/software development life cycle processes and found that the CFPB's information security program effectively integrates cybersecurity requirements into its software development life cycle processes. We also performed our annual assessments of the Board's and the CFPB's information security programs; overall, both the Board's and the CFPB's information security programs continue to operate effectively.

Climate risk is a particularly salient topic after this summer's record-breaking heat and natural disasters. In July, we published an OIG Insights paper on the Board's approach to climate risk supervision at financial institutions. Our paper compares the Board's approach to climate risk supervision to the approaches of other central banks and financial regulatory agencies and identifies key areas of consideration as the Board develops and implements its supervisory approach.

Additional work from this reporting period focused on the pandemic lending programs. We assessed the System's vendor selection and management processes for COVID-19 emergency lending facilities and found that the Federal Reserve Bank of New York generally followed established processes for selecting and managing vendors, which helped foster transparency and consistency, mitigate risks and conflicts of interest, and confirm that expected services were delivered. We also evaluated the Board and the Federal Reserve Bank of Boston's process for purchasing Main Street Lending Program (MSLP) loan participations and found that the Board and the Federal Reserve Bank of Boston generally followed their process but can formally document how to approach potentially ineligible MSLP loans.

In other work this reporting period, we found that the Board's purchase card program controls are generally effective, although approving officials could review and approve transaction logs in a more timely manner. We also performed risk assessments of the Board's and the CFPB's government travel card programs; both assessments found that the risk of illegal, improper, or erroneous use of the cards is *low*. Finally, we assessed the CFPB Office of Finance and Procurement's controls for exercising contract options, which allow federal agencies to add supplies or services to existing contracts, and we found that these controls can be improved.

The work of our Office of Investigations continues to send a strong message that those who commit fraud will be brought to justice. Earlier this month, the former president of First NBC Bank was sentenced to 14 years in prison for bank fraud and making false statements in bank records. His fraudulent schemes resulted in the failure of the bank in April 2017, which caused an approximate \$1 billion loss to the DIF and the loss of approximately 500 jobs. In another case, the chief executive officer of Paycheck Protection Program lender MBE Capital was sentenced in July to 54 months in prison in connection with fraudulent loan and lender applications that enabled him to collect over \$71 million in lender fees.

Overall, in the past 6 months, our Office of Investigations closed 28 investigations and resolved 196 hotline complaints. Our work resulted in 5 referrals for criminal prosecution; 19 arrests; 14 indictments; 12 criminal informations; 27 convictions; and nearly \$400 million in criminal fines, restitution, special assessments, and forfeiture.

Our audit organization recently underwent an external peer review conducted by the National Aeronautics and Space Administration Office of Inspector General, which awarded us a rating of *pass*. The review team found that our system of quality control for the audit organization has been suitably designed and complied with to provide reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. In addition, the OIG for the U.S. Department of Commerce conducted a peer review of our investigative operations and found that our system of internal safeguards and management procedures is in compliance with the quality standards established by the Council of the Inspectors General on Integrity and Efficiency and other applicable guidelines and statutes. The review team identified three aspects of our investigative operations that reflect best practices: our firearms program and other training requirements; the organizational structure of our headquarters personnel; and the organization, documentation, and professionalism of our investigative case files. Finally, we completed an evaluation peer review of the U.S. Small Business Administration OIG and reported that the organization generally complied with Blue Book requirements.

We continue to closely monitor the ongoing legal challenge to the constitutionality of the CFPB's funding mechanism as well as legislative proposals to reform the CFPB. In addition, we recently welcomed new leadership to the Board, as Adriana Kugler took office as a member of the Board of Governors. We have met with Governor Kugler, and we look forward to continuing to work with leadership at the Board and the CFPB as we provide robust independent oversight to improve their programs and operations and to prevent and detect fraud, waste, and abuse.

We could not achieve our mission without our phenomenal staff, who continue to impress me daily with their exceptional talent, expertise, and dedication. I remain deeply grateful for their hard work and steadfast commitment, and I look forward to continuing to work together to fulfill our vitally important mission.

Sincerely,



Mark Bialek
Inspector General
October 31, 2023

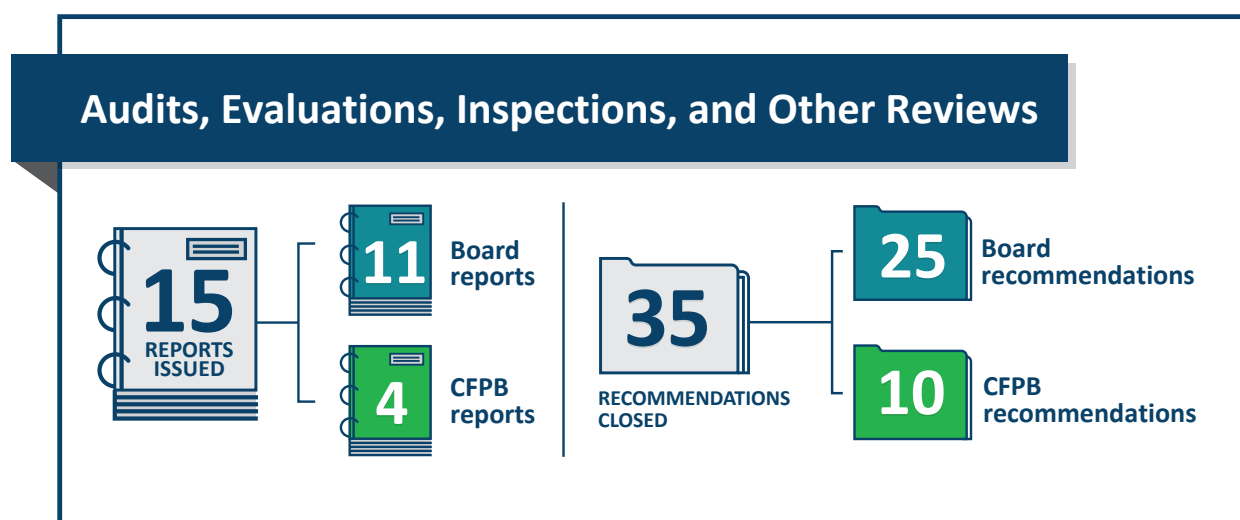


Contents

Highlights	1
Introduction	5
Pandemic Response Oversight	9
Status Updates for Completed, Initiated, and Planned Work	9
Pandemic-Related Investigations	11
Major Management Challenges	13
Audits, Evaluations, and Other Reviews	15
Board of Governors of the Federal Reserve System	15
Consumer Financial Protection Bureau	21
Failed State Member Bank Reviews	25
Material Loss Reviews	25
Nonmaterial Loss Reviews	25
Investigations	27
Hotline	35
Legislative and Regulatory Review, Congressional and Media Activities, and CIGIE Participation	37
Legislative and Regulatory Review	37
Congressional and Media Activities	38
CIGIE Participation	38
Peer Reviews	41
Appendix A: Statistical Tables	43
Appendix B: Additional Mandated Reporting Requirements	55
Appendix C: Open Recommendations Made Before the Reporting Period	57
Board of Governors of the Federal Reserve System	57
Consumer Financial Protection Bureau	63
Abbreviations	69

Highlights

We continued to promote the 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.



Federal Open Market Committee Investment and Trading Rules

The Board's and the Federal Reserve Banks' approach to monitoring personal investment and trading activities for possible conflicts of interest can be strengthened.

Main Street Lending Program Loan Participation Purchases

Some key processes for purchasing Main Street Lending Program (MSLP) loan participations were not formally documented, which can lead to loss of institutional knowledge or inconsistency in process.

Climate Risk Supervision

Uncertainty about the timing and magnitude of the effects of climate change and the lack of quality data pose challenges for supervisors and financial institutions.

The CFPB’s Exercise of Contract Options

The CFPB did not consistently document that all *Federal Acquisition Regulation* requirements were met before exercising options, did not always exercise options before the associated contracts expired, and did not always notify the contractors of the option extension within contract-required time frames.

Material Loss Review of Silicon Valley Bank

Silicon Valley Bank (SVB) failed because of unchecked, rapid growth; significant concentrations; and ineffective leadership. The Board and the Federal Reserve Bank of San Francisco (FRB San Francisco) should have acted earlier or taken stronger action to address identified weaknesses at SVB.

Supervision of Silvergate Bank

Silvergate’s concentration in crypto industry deposit customers, rapid growth, and multilayered funding risks, as well as weaknesses in the bank’s corporate governance and risk management capabilities, led to the bank’s voluntary liquidation. The Board and FRB San Francisco should have escalated concerns through stronger, earlier, and more-decisive supervisory action.

The Board’s Information Security Program

The Board’s information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity.

The CFPB’s Information Security Program

The CFPB’s information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity.



Former First NBC Bank President Sentenced to 14 Years in Prison and \$214 Million Restitution

Convicted of all 46 counts against him, Ashton J. Ryan Jr., former president and chief executive officer (CEO) of First NBC Bank, was sentenced to 170 months in prison, 3 years of supervised release, and \$214 million in restitution. Ryan was at the center of a long-running fraud scheme that caused the \$5 billion New Orleans bank to fail.

CEO of MBE Capital Sentenced to Prison and Restitution for \$823 Million Paycheck Protection Program Fraud

Rafael Martinez, CEO and primary owner of MBE Capital Partners, was sentenced in New York to 54 months in prison for an \$823 million Paycheck Protection Program (PPP) loan and lender fraud scheme. He was also sentenced to 3 years of supervised release and ordered to pay over \$71 million in restitution and forfeit about \$45 million.

CEO of California Residential Reentry Home Convicted for \$34 Million in PPP Fraud

Attila Colar, former CEO of All Hands on Deck, was convicted of 44 counts involving a \$34 million PPP fraud scheme and other crimes. The counts—including conspiracy, bank fraud, wire fraud, aggravated identity theft, obstruction, and witness tampering—carry up to 30 years in prison and fines up to \$1 million.

Two Loan Brokers and a Loan Officer Pleaded Guilty to Bank Fraud Conspiracy

Ted Capodilupo and Joseph Masci, operators of a loan brokerage business, pleaded guilty to conspiracy to commit bank fraud against a Massachusetts-based bank and the U.S. Small Business Administration (SBA). Brian Ferris, a loan officer at the bank, also pleaded guilty to conspiracy to commit bank fraud. The charges carry up to 30 years in prison plus fines, restitution, and forfeiture.



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) as a member of PRAC, and as such, we participate in PRAC meetings, conduct PRAC oversight activities, and contribute to PRAC 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. § 248(b)) 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 Consumer Financial Civil Penalty Fund is subject to the PIIA. The PIIA requires us to determine each fiscal year 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. app. 3 § 11 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.

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.

- 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.



Pandemic Response Oversight

The economic disruptions caused by the COVID-19 pandemic resulted in an abrupt shock to financial markets and affected many credit channels relied on by households, businesses, and state and local governments. In response, 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 has continued to play a vital role throughout the pandemic by enforcing federal consumer protection laws and protecting consumers from abuse.

We are closely coordinating with the U.S. Government Accountability Office; PRAC, which coordinates IG community oversight of the federal government’s COVID-19 pandemic response efforts; the Special Inspector General for Pandemic Recovery; the SBA Office of Inspector General; the U.S. Department of Justice (DOJ); and other OIGs to ensure robust oversight of the Board’s pandemic response activities, and we are overseeing the CFPB’s pandemic response activities through our own reviews, to efficiently deploy resources where they are most needed.

Inspector General Bialek continues to serve on PRAC; he is a member of the PRAC Financial Sector Oversight Subcommittee and serves as the vice chair of the PRAC Investigations Subcommittee.

Status Updates for Completed, Initiated, and Planned Work

In 2020, we initiated an ongoing pandemic response monitoring effort for risk assessment purposes and as part of our audit planning activities. We primarily focus on the Board’s pandemic response lending programs, which helps to inform our selection of prospective audit and evaluation topics. This monitoring effort is generally focused on the following topics:

- governance and controls to ensure consistent execution of the Board’s programs by the Reserve Banks designated to put them into action, as well as vendor activities to execute program objectives
- coordination activities among the Reserve Banks or the designated program manager to execute, monitor, and improve that execution over time
- data aggregation and validation, particularly before program-related information is shared with the public or congressional stakeholders
- whether pandemic response lending efforts served the intended communities

Although CFPB programs and operations are not directly funded by the CARES Act or tasked with CARES Act requirements, the agency plays a vital role in protecting consumers from pandemic-related consumer financial fraud and abuse. In this regard, we actively oversee the CFPB’s supervisory activity and monitoring of consumer complaints.

The audits and evaluations we have planned or initiated based on these activities and their status are outlined below.

Evaluation of the Federal Reserve System’s Vendor Selection and Management Processes Related to the Federal Reserve Bank of New York’s Emergency Lending Programs

We issued this report in April 2023; see the [summary](#) below.

Evaluations of the Federal Reserve System’s Loan Purchase and Administration for Its MSLP

The Board established the MSLP to facilitate lending to small and medium-sized for-profit and nonprofit organizations. To do so, the Federal Reserve Bank of Boston (FRB Boston) purchased 1,830 loans worth \$17.5 billion from banks and lenders, the majority of which were purchased in the last 2 months of the program. To handle this increased activity, FRB Boston implemented an expedited loan purchase process for certain lenders. FRB Boston is now in the process of administering the loans, including assessing overall credit risk and identifying substandard loans. To assist with managing the program, FRB Boston contracted with vendors for a variety of these purchase and administration functions, including purchase intake, credit administration, loan workout, and other services. We are conducting a two-phase assessment of the MSLP loan purchase and administration processes, including the design and operating effectiveness of internal controls. We completed our loan purchase evaluation in July 2023; see the [summary](#) below. We expect to complete our loan administration evaluation in the next semiannual reporting period.

Evaluation of the Federal Reserve System’s Paycheck Protection Program Liquidity Facility

The Board established the Paycheck Protection Program Liquidity Facility (PPPLF) to extend credit to financial institutions that originate loans through the SBA’s guaranteed PPP, taking the PPP loans as collateral. The PPPLF, managed by the Federal Reserve Bank of Minneapolis and operated out of the 12 Reserve Banks, distributed billions of dollars to eligible lenders. We will assess the effectiveness of the Federal Reserve System’s internal controls for the PPPLF processes related to (1) identifying and managing

risk and unresolved loans, (2) addressing nonpayment, and (3) detecting and mitigating fraudulent collateral. We began scoping this evaluation in the second quarter of 2023.

Audit of the CFPB’s Consumer Response Operations

The CFPB uses consumer complaints to help inform the agency’s supervision, enforcement, and policymaking activities. With an increase in consumer complaints during the COVID-19 pandemic, the Office of Consumer Response faces an operational risk with respect to its effectiveness in reviewing and monitoring consumer complaints. We plan to assess the effectiveness of the CFPB’s processes for reviewing and monitoring company responses to consumer complaints. This audit is in the fieldwork phase.

2023 Audit of the CFPB’s Information Security Program

FISMA requires us to perform an annual independent evaluation of the CFPB’s information security program, to include testing the effectiveness of controls for select systems. As part of our 2023 FISMA audit, we contracted with an independent accounting firm to test the effectiveness of selected security controls for the CFPB’s consumer response system. This system is used by the CFPB to collect, respond to, and refer consumer inquiries and complaints concerning consumer financial products and services. As noted above, the consumer response system is dealing with a higher volume of consumer complaints since the onset of the COVID-19 pandemic. We completed our information security program audit in September 2023; see the [summary](#) below. We plan to issue a separate, restricted memorandum on the results of the testing of the consumer response system in the next reporting period.

Pandemic-Related 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 OIGs. Since the start of the pandemic, our work has resulted in 157 full investigations; 93 arrests; 83 convictions; and nearly \$194 million in criminal fines, restitution, and special assessments. During this reporting period, we opened 14 full investigations; made 15 arrests; had 18 convictions; and recovered over \$124 million in criminal fines, restitution, and special assessments. 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 Hybrid Work and Workforce Planning, Updating the Human Capital System, and Advancing Diversity Initiatives
- Remaining Adaptable While Supervising Financial Institutions
- Enhancing Oversight of Cybersecurity at Supervised Financial Institutions and Service Providers
- Ensuring an Effective Information Security Program
- Evolving With Financial Sector Innovations
- Monitoring COVID-19 Pandemic Emergency Lending Facilities and Underlying Loan Portfolios
- Ensuring That Physical Infrastructure Effectively Meets Mission Needs

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

- Ensuring an Effective Information Security Program
- Managing Human Capital to Maintain a Talented, Diverse, Inclusive, and Engaged Workforce
- Continuing to Refine the Supervision and Enforcement Strategy
- Managing Consumer Complaints

See our website for our full [management challenges reports](#) to the Board and the CFPB.



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. Our audits are performed in accordance with *Government Auditing Standards*, which is 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. Our evaluations are performed according to *Quality Standards for Inspection and Evaluation*, which is 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

Following Established Processes Helped FRB New York and the Board Reduce Risks Associated With Lending Facility Contracts

2023-FMIC-B-005

April 17, 2023

The Federal Reserve Bank of New York (FRB New York) contracted with vendors to operate certain emergency lending facilities supporting businesses and state and local governments during the COVID-19 pandemic. We assessed the System’s vendor selection and management processes for lending facilities operated by FRB New York.

FRB New York generally followed established processes for selecting and managing vendors, while the Board provided oversight. Doing so helped foster transparency and consistency, mitigate risks and

conflicts of interest, and confirm that expected services were delivered. In January 2023, FRB New York took additional steps to reduce risks associated with future lending facility contracts by clarifying the vendor selection processes and identifying lessons learned applicable to lending facility acquisitions.

Our report does not contain recommendations.

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

2023-SR-B-006

April 26, 2023

Following multiple incidents involving senior System officials, the Federal Open Market Committee (FOMC) adopted a new personal investment and trading policy that prohibits covered individuals from purchasing individual securities, restricts active trading, and revises certain public reporting and disclosure requirements. We assessed the design and effectiveness of this policy as well as the Board’s and the Reserve Banks’ approach to monitoring personal investment and trading activities for potential conflicts of interest.

We determined that the Board can further enhance the new FOMC personal investment and trading policy. Specifically, requirements that apply to senior FOMC officials can be extended to additional staff based on the risk presented by their access to confidential FOMC information, ethics programs can be strengthened to make reviews of financial disclosure reports more uniform and to enforce consequences for policy violations, and the information individuals provide in their financial disclosure reports can be verified for completeness and accuracy.

Our report contains six recommendations to strengthen the Board’s and the Reserve Banks’ approach to monitoring personal investment and trading activities for possible conflicts of interest. The Board concurred with our recommendations.

Board Purchase Card Program Controls Are Generally Effective and Can Be Further Strengthened

2023-FMIC-B-007

May 8, 2023

The Board’s purchase card program, which streamlines the purchase of certain goods and services, had more than \$6.5 million in transactions from 2020 through 2021. We assessed whether the purchase card program controls ensure that applicable laws, rules, regulations, policies, and procedures are followed and prevent and detect fraud and misuse.

We found that the Board’s purchase card program controls are generally effective. However, approving officials could review and approve transaction logs more timely.

Our report contains a recommendation to help ensure that authorizing officials review and approve transaction logs in a timely manner. The Board partially concurred with our recommendation.

The Board Can Enhance Its Procedures and Controls for Protecting Confidential Information in Supervision Central

2023-SR-B-009

June 14, 2023

While supervising and examining banking organizations, Reserve Bank examiners collect sensitive, nonpublic information, including personally identifiable information. The loss or misuse of this information could harm Board operations and bank customers. We assessed the Board’s and the Reserve Banks’ controls for protecting such information in certain examination applications used for supervising community and regional banks.

We found that examiners do not consistently use a process to help purge sensitive documents that are not required to be retained. In addition, some examiners may have access to more sensitive personally identifiable information than is necessary for their job duties.

Our report includes two recommendations to help the Board better protect sensitive, nonpublic information. The Board concurred with our recommendations.

Results of Scoping of the Evaluation of the Board and Reserve Banks’ Cybersecurity Incident Response Process for Supervised Institutions

2023-SR-B-010

June 26, 2023

Cybersecurity risks present significant and dynamic challenges to financial institutions. A significant cybersecurity incident at a Board-supervised financial institution could disrupt its operations and ultimately affect financial stability. We evaluated the Board and Reserve Banks’ process for responding to cybersecurity incidents at supervised financial institutions.

During our scoping activities, we found that the Board’s guidance documents do not clearly describe the mission or governance structure of the cybersecurity incident response process. In addition, the Board and Reserve Banks’ responses to cybersecurity incidents have not consistently followed the process described in guidance, and some staff were unclear of their roles and responsibilities in the process, highlighting the need for enhanced training.

Our report includes six recommendations to enhance the effectiveness of the Board and Reserve Banks’ process for responding to cybersecurity incidents at supervised institutions. The Board concurred with our recommendations.

The Board and FRB Boston Generally Followed Their Process for Purchasing MSLP Loan Participations but Can Formally Document Some Key Processes

2023-FMIC-B-011

July 17, 2023

The Board authorized the MSLP during the COVID-19 pandemic to support lending to businesses and nonprofits. Through the MSLP, lenders issued about \$17.5 billion in loans. To encourage the flow of credit, the MSLP, which is administered by FRB Boston, purchased loan participations—a share of loan values—from lenders. We evaluated the Board and FRB Boston’s process for purchasing MSLP loan participations.

All the loans we reviewed had complete and properly executed documentation, with reviews of lender-submitted documents generally performed as required. However, some key processes were not formally documented, which can lead to loss of institutional knowledge or inconsistency in process.

Our report contains a recommendation to help the Board and FRB Boston ensure consistency in their process for determining whether loans were purchased based on inaccurate borrower certifications. The Board and FRB Boston concurred with our recommendation.

The Board’s Approach to Climate Risk Supervision at Financial Institutions

July 31, 2023

In this OIG Insights paper, we noted that the Board is in the early stages of its supervisory work to assess climate-related financial risk to the safety and soundness of financial institutions. The Board is developing guidance on climate-related financial risk management for the largest financial institutions and has begun a pilot program to understand firms’ financial positions under various plausible climate scenarios. However, uncertainty about the timing and magnitude of the effects of climate change and the lack of quality data about climate risks pose challenges for supervisors and financial institutions.

Calendar Years 2020–2022 Risk Assessment of the Board’s Government Travel Card Program

September 13, 2023

We conducted a risk assessment of the Board’s government travel card (GTC) program to determine the necessary frequency and scope of GTC audits. The results of the risk assessment show that the risk of illegal, improper, or erroneous use in the Board’s GTC program is *low*.

A risk level of *low* means that illegal, improper, or erroneous use is unlikely to occur and that such an occurrence would be expected to have a minimal effect on current operations and long-term objectives.

Nonetheless, the Board’s Travel section should continue to take appropriate actions to ensure proper oversight of its program.

Material Loss Review of Silicon Valley Bank

2023-SR-B-013

September 25, 2023

SVB—which once had over \$200 billion in total assets—failed in March 2023. SVB went into receivership and cost the DIF an estimated \$16.1 billion. In accordance with the requirements of section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Act, we conducted a material loss review to determine why SVB’s failure resulted in a material loss to the DIF; to assess the Board’s and FRB San Francisco’s supervision during our period of review, January 2018 through March 2023; and to make recommendations, as appropriate.

SVB failed for several reasons. It was vulnerable to the business cycles of its customer base—concentrated in science and technology—with a high share of uninsured deposits and large, irregular cash flows. SVB also invested a large portion of deposits in securities with long-term maturities and experienced significant unrealized losses on those securities as interest rates rose. Further, SVB’s management and board failed to manage the risks of the bank’s rapid, unchecked growth and concentrations. Finally, management’s ineffective communication about the bank’s intent to raise capital, coupled with news of Silvergate Bank’s liquidation, led to a \$40 billion run on deposits with additional withdrawal requests totaling \$100 billion that SVB could not meet.

The Board and FRB San Francisco were responsible for ensuring that SVB conducted its business activities in a safe and sound manner. However, their supervisory approach did not evolve with SVB’s growth and increased complexity—for example, there were insufficient examiner resources, and examiners lacked requisite expertise supervising a large, complex institution. Further, the Board and FRB San Francisco did not effectively transition SVB between supervisory portfolios. Finally, examiners did not closely scrutinize the risks that rising interest rates posed to SVB’s investments.

Our report includes seven recommendations to improve banking organization supervisory processes. The Board concurred with our recommendations.

Review of the Supervision of Silvergate Bank

2023-SR-B-014R

September 27, 2023

In March 2023, Silvergate Bank’s holding company announced its intent to voluntarily liquidate the bank. Silvergate’s concentration in crypto industry deposit customers, rapid growth, and multilayered funding risks led to the bank’s voluntary liquidation. We initiated this evaluation in March 2023 on a discretionary

basis following the voluntary liquidation announcement. We assessed the Board’s and FRB San Francisco’s supervision of Silvergate. The scope of our evaluation included supervisory activities conducted from 2013 to 2023 related to Silvergate’s change in business strategy, deposit growth, concentrated business activities, and governance and risk management practices.

We found that the Board and FRB San Francisco considered requiring Silvergate to file an application under Regulation H as it evolved to a novel business model focused on the crypto industry, but did not. Regulation H requires state member banks to obtain approval from the Board before changing the general character of their business. In addition, we found that examiners should have escalated concerns through stronger, earlier, and more-decisive supervisory action; we identified ways in which FRB San Francisco could have strengthened the process to transition Silvergate from the community banking organization portfolio to the regional banking organization portfolio; we found that the Board’s examiner guidance does not include information that could have helped examiners address the risks associated with Silvergate’s business model and deposit composition; and we found that the Board does not have guidance for examiners supervising banks projecting or experiencing significant, rapid growth and does not have guidance on how examiners should assess whether a bank’s risk management capabilities and key control functions have evolved with that growth.

Our report contains 12 recommendations to enhance supervisory processes based on lessons learned from Silvergate’s voluntary liquidation. The Board concurred with our recommendations. Given Silvergate’s status as an open institution and the confidential supervisory and trade secret information described in our report, our full report is restricted.

2023 Audit of the Board’s Information Security Program

2023-IT-B-015

September 29, 2023

The Office of Management and Budget’s fiscal year 2023–2024 guidance for FISMA reporting directs IGs to evaluate the maturity level (from a low of 1 to a high of 5) of their agency’s information security program for fiscal year 2023. In accordance with FISMA requirements, we assessed the effectiveness of the Board’s (1) security controls and techniques for selected information systems and (2) information security policies, procedures, standards, and guidelines.

The Board’s information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. Since our review last year, we found that the Board has taken steps to strengthen its information security program, for example, by expanding the coverage of its vulnerability disclosure program to include all internet-accessible systems and by strengthening its supply chain risk management program through improved documentation of its processes.

However, the Board can strengthen its information security program in the *identify* and *protect* function areas. Specifically, the Board should define its cybersecurity risk tolerance, complete its cybersecurity risk register, define its process for consistently inventorying and documenting necessary attributes for its web application and third-party systems, strengthen mobile device security, and update and review its privacy impact assessments.

Seven recommendations from our prior FISMA audit reports remain open. This report contains seven new recommendations. The Board concurred with our recommendations.

Consumer Financial Protection Bureau

Report on the Independent Audit of the CFPB’s Agile Systems/Software Development Life Cycle Processes

2023-IT-C-008

May 31, 2023

We contracted with an independent public accounting firm to conduct a performance audit of the CFPB’s Agile systems/software development life cycle processes. We reviewed and monitored the work of the contractor to ensure compliance with the contract and generally accepted government auditing standards.

The contractor found that the CFPB’s information security program effectively integrates cybersecurity requirements into its software development life cycle processes and will be further strengthened once efforts to improve privileged user and software inventory management processes are completed.

The report did not include recommendations.

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

September 13, 2023

We conducted a risk assessment of the CFPB’s GTC program to determine the necessary frequency and scope of GTC audits. The results of the risk assessment show that the risk of illegal, improper, or erroneous use in the CFPB’s GTC program is *low*.

A risk level of *low* means that illegal, improper, or erroneous use is unlikely to occur and that such an occurrence would be expected to have a minimal effect on current operations and long-term objectives. Nonetheless, the CFPB’s Office of Travel and Relocation should continue to take appropriate actions to ensure proper oversight of its program.

The CFPB Can Improve Its Controls for Exercising Contract Options

2023-FMIC-C-012

September 18, 2023

Contract options allow federal agencies to add supplies or services to existing contracts. The CFPB obligated \$88 million for contract options from July 2019 to June 2021. We assessed the CFPB’s controls for exercising contract options to ensure compliance with applicable laws, regulations, and internal policies and procedures.

Our audit found that the CFPB did not consistently document that all *Federal Acquisition Regulation* requirements were met before exercising options. The agency also did not always exercise options before the associated contracts expired or notify the contractors of the option extension within contract-required time frames.

After receiving a draft of our report, the CFPB took steps to address these findings; therefore, our final report does not include recommendations.

2023 Audit of the CFPB’s Information Security Program

2023-IT-C-016

September 29, 2023

The Office of Management and Budget’s fiscal year 2023–2024 guidance for FISMA reporting directs IGs to evaluate the maturity level (from a low of 1 to a high of 5) of their agency’s information security program for fiscal year 2023. We contracted with an independent contractor who, in accordance with FISMA requirements, assessed the effectiveness of the CFPB’s (1) security controls and techniques for selected information systems and (2) information security policies, procedures, standards, and guidelines.

The independent contractor found that the CFPB’s information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. In addition, the contractor noted the CFPB has strengthened its information security program, for example, by maturing its information security continuous monitoring and supply chain risk management processes and working to meet the zero-trust architecture requirements.

However, the contractor identified new opportunities to strengthen the CFPB’s information security program in the area of contingency planning. Specifically, the CFPB can improve its continuity of operations processes by ensuring that it conducts and maintains an enterprise business impact analysis and can maintain resilience by ensuring that it schedules and performs contingency plan testing at least annually for all its systems. In addition, the CFPB should continue its prior efforts regarding data loss prevention and software asset management to ensure that its program remains effective.

The CFPB has taken sufficient actions to close prior OIG FISMA audit recommendations related to its account management, risk management, configuration management, and identity and access management. This report includes one new recommendation designed to strengthen the CFPB’s information security program with regard to contingency planning. The CFPB concurred with our recommendation.



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) OIG 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

In March 2023, the California Department of Financial Protection and Innovation closed SVB, a state member bank located in Santa Clara, California, and supervised by FRB San Francisco. The Department of Financial Protection and Innovation appointed the FDIC as receiver. As of December 31, 2022, SVB had total assets of approximately \$209 billion. On March 14, 2023, we initiated an engagement addressing the supervision of SVB. In May 2023, the FDIC estimated that the loss to the DIF would be approximately \$16.1 billion, which exceeds the statutory threshold requiring us to conduct a material loss review. We completed our [material loss review of SVB](#) during this reporting period.

In July 2023, the Kansas Office of the State Bank Commissioner closed Heartland Tri-State Bank, a state member bank located in Elkhart, Kansas, and supervised by the Federal Reserve Bank of Kansas City. The Office of the State Bank Commissioner appointed the FDIC as receiver. At the time of its failure, Heartland had total assets of approximately \$122 million. We received notice that the estimated loss to the DIF exceeds the statutory definition of a material loss. Accordingly, our engagement is a material loss review.

Nonmaterial Loss Reviews

The Federal Deposit Insurance Act, as amended, requires that we semiannually report certain information on 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 is required to 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 and savings and loan holding companies and state-chartered banks that are members of the System, known as *state member banks*. Under delegated authority from the Board, the Reserve Banks supervise bank and savings and loan holding companies and state member banks, and the Board's Division of Supervision and Regulation oversees the Reserve Banks' supervisory activities. Our investigations typically involve allegations that senior bank or holding company 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 in a manner that may have affected the CFPB's ability to carry out its supervisory responsibilities. 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 SBA as collateral. In addition, our office also conducted investigations in support of our membership on PRAC. Our office is also part of the DOJ's COVID-19 Fraud Enforcement Task Force.

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

Former First NBC Bank President Sentenced in Louisiana to 14 Years in Prison and \$214 Million Restitution for Fraud That Caused Bank’s Failure

For his role in a fraud scheme leading to the failure of the \$5 billion First NBC Bank, Ashton J. Ryan Jr., former president and CEO, was sentenced to 170 months in prison after being convicted of all 46 counts against him, including bank fraud, conspiracy to commit bank fraud, and making false entries in bank records. He was also sentenced to 3 years of supervised released and ordered to pay \$214 million in restitution. Based in New Orleans, the bank was a subsidiary of the Board-supervised First NBC Bank Holding Company. The bank’s failure cost the FDIC’s DIF just under \$1 billion.

In the long-running scheme, Ryan and several other executives conspired with borrowers to defraud the bank. The executives extended loans to the borrowers, who were unable to repay the loans, and then extended new loans to the borrowers to cover the existing loans. Ryan and the executives enriched themselves through fees earned on the loans while concealing their actions—and the true financial condition of the bank—from the board of directors and outside auditors and examiners. By the time the bank collapsed, these bogus loans totaled hundreds of millions of dollars.

We conducted this investigation with the Federal Bureau of Investigation (FBI) and the FDIC OIG. The U.S. Attorney’s Office for the Eastern District of Louisiana prosecuted.

CEO of PPP Lender MBE Capital Sentenced in New York to 54 Months in Prison and Restitution for \$823 Million PPP Fraud

Rafael Martinez, CEO and primary owner of MBE Capital Partners, was sentenced to 54 months in prison for conspiracy to commit wire fraud in connection with an \$823 million PPP loan and lender fraud scheme. He was also sentenced to 3 years of supervised release and ordered to pay over \$71 million in restitution and forfeit nearly \$45 million along with multiple properties and luxury vehicles.

Martinez used false representations and documents to fraudulently obtain SBA approval for his company, MBE Capital Partners, to be a nonbank PPP lender. After MBE was approved, Martinez issued \$823 million in PPP loans to about 36,600 businesses. Those loans earned Martinez over \$71 million in lender fees. In addition, Martinez schemed to obtain a PPP loan of over \$283,000 for MBE through false statements about employees and wages using the forged signature of MBE’s tax preparer. Martinez spent the proceeds from his criminal conduct on, among other things, a \$10 million villa in the Dominican Republic; a \$3.5 million mansion in New Jersey; a chartered jet service; and several luxury vehicles, including a Bentley, a BMW, a Ferrari, a Mercedes-Benz, and a Porsche.

We conducted this investigation with the Internal Revenue Service (IRS) Criminal Investigation (CI) and the SBA OIG. The U.S. Attorney’s Office for the Southern District of New York prosecuted.

Texas Man Sentenced to Over 2 Years in Prison for Money Laundering Conspiracy

Joshua Roberts, a Texas resident and citizen of Ghana and the United Kingdom, was sentenced to 2 years and 3 months in prison, followed by 3 years of supervised release, and ordered to pay over \$831,000 in restitution for conspiracy to commit money laundering. Roberts's prison sentence will run concurrently with a sentence he is serving for related crimes in a Georgia case.

Roberts established a sham company to launder funds gained through criminal activity. The funds were derived from a sophisticated scam that compromised legitimate business or personal email accounts to conduct unauthorized fund transfers. One of the attempted targets was a Board vendor. His coconspirators were sentenced in a previous reporting period: Peggy McDowell Brown, of Kentucky, was sentenced to 2 years of probation and ordered to pay over \$831,000 in restitution, and Olajide Samuel Agbaniyaka, of Georgia, was sentenced to 3 years and 1 month in prison, followed by 2 years of supervised release, and ordered to pay over \$1.1 million in restitution.

We investigated this case with Homeland Security Investigations. The U.S. Attorney's Office for the Western District of Kentucky prosecuted.

Florida Man Sentenced to Prison and Restitution for \$2.5 Million COVID-Relief Fraud

Vinicius Santana, a Florida resident and owner of Massachusetts-based painting company Complete Home Care, was sentenced to 29 months in prison, followed by 3 years of supervised release, and ordered to pay restitution of \$2.5 million for filing fraudulent applications to obtain \$2.5 million in PPP loan funds.

Santana submitted four PPP loan applications on behalf of his painting business. The first three applications, in which Santana allegedly listed five employees and an average monthly payroll between \$10,000 and \$18,000, were denied. In the fourth application, Santana allegedly falsely claimed to have 154 employees and an average monthly payroll of \$1 million. The fourth application was approved, and a bank issued Santana's company a \$2.5 million loan. After receiving the funds, Santana allegedly misused the loan proceeds to buy cars and invest in cryptocurrency.

We investigated this case with the FBI, the FDIC OIG, and the U.S. Postal Inspection Service. The U.S. Attorney's Office for the District of Massachusetts prosecuted.

Former Louisiana Assistant District Attorney and Two Associates Convicted for Defrauding First NBC Bank

Glenn E. Diaz, former St. Bernard Parish assistant district attorney, and two associates, Peter J. Jenevein and Mark S. Grelle, were convicted of dozens of bank fraud and money laundering charges for defrauding First NBC Bank out of more than \$550,000. The counts carry sentences of up to 30 years in prison and 3 years of supervised release, plus fines up to the greater of \$1 million or twice the gain to the defendants or losses to the victims.

Diaz, Jenevein, and Grelle conspired to defraud First NBC Bank through a series of false invoices for work purportedly done at a Florida warehouse owned by Diaz. A customer of First NBC Bank, Diaz had been overdrawing his checking account for purported business expenses but was instead depositing these overdrafts into his personal account at another bank. After First NBC Bank officers began requiring Diaz to prove that the funds were used for business expenses, Diaz had Jenevein provide invoices for work performed by Grelle’s company, Grelle Underground Services LLC. The defendants also sent fraudulent documents to First NBC Bank to support the disbursements of money from the bank that purportedly reimbursed Diaz for additional fraudulent business costs. Bank officers approved the overdrafts based on these invoices and supporting materials. However, after Diaz wrote the check to Grelle’s company, Grelle would then write a check back to Diaz. Diaz would deposit the money into his personal account and use it for personal and business expenditures unrelated to the Florida warehouse project. In total, Diaz, Jenevein, and Grelle executed 17 round-trip transactions.

We conducted this investigation with the FBI and the FDIC OIG. The U.S. Attorney’s Office for the Eastern District of Louisiana is prosecuting.

CEO of California Residential Reentry Home Convicted for \$34 Million PPP Fraud and Other Crimes

Attila Colar, former CEO of All Hands on Deck, was convicted of 44 counts involving a \$34 million in PPP fraud and other schemes. All Hands on Deck is a residential reentry home in California for individuals who are on probation or parole, are homeless, or have mild mental illness. The counts—which include conspiracy, bank fraud, wire fraud, aggravated identity theft, obstruction, and witness tampering—carry sentences of up to 30 years in prison and fines up to \$1 million.

Colar submitted multiple PPP loan applications on behalf of All Hands on Deck that were false or misleading. He substantially overstated payroll, claiming as many as 81 employees when in fact he was the only salaried employee. He also submitted multiple fraudulent PPP loan applications in the name of other, bogus companies. He used the identities of two individuals living in his residential reentry facility, claiming they were CEOs of companies with million-dollar payrolls. In all, Colar submitted 16 fraudulent

PPP loan applications seeking over \$34 million. In another scheme, Colar fraudulently induced a company to refer parolees to All Hands on Deck using falsified fire inspection clearance reports, a false letter of recommendation, false security clearance documents, and false or misleading information about its staff.

We conducted this investigation with the FBI, the IRS CI, the SBA OIG, and the U.S. Treasury Inspector General for Tax Administration. The U.S. Attorney’s Office for the Northern District of California is prosecuting.

New York Brothers Pleaded Guilty to \$7.6 Million PPP Relief Fraud

Larry Jordan and Sutukh El, brothers who own multiple businesses, submitted fraudulent applications in a scheme to obtain \$7.6 million in PPP loans. Both pleaded guilty to conspiracy to commit bank fraud and wire fraud, while Jordan also pleaded guilty to bank fraud and engaging in monetary transactions in criminally derived property. The counts carry sentences of up to 30 years in prison and fines up to \$1 million.

Jordan and El submitted eight fraudulent PPP loan applications on behalf of their companies. They made numerous false statements about their businesses and submitted fake documents, including bogus federal tax filings and payroll information, to support the applications. They then used the loan proceeds for personal investments, expenses, and home improvements.

We conducted this investigation with the FBI, the FDIC OIG, the Federal Housing Finance Agency OIG, and the SBA OIG. The DOJ and the U.S. Attorney’s Office for the Western District of New York are prosecuting.

Social Media Influencer Pleaded Guilty in Maryland to \$1.2 Million PPP and Economic Injury Disaster Loan Fraud Scheme

Denish Sahadevan, of Maryland, pleaded guilty to wire fraud, aggravated identity theft, and money laundering in a \$1.2 million PPP and Economic Injury Disaster Loan (EIDL) fraud scheme. The charges carry up to 20 years in prison. Sahadevan will be required to pay at least \$429,000 in restitution; he will also forfeit a gold, physical Bitcoin and about \$17,000 in cash, proceeds from the scheme that were seized during a search of his residence.

Sahadevan submitted fraudulent PPP and EIDL applications on behalf of four Maryland entities he controlled. He created bogus documents, such as tax forms and bank statements, for the applications. He also used the identifying information of a tax preparer he knew, without that person’s knowledge or agreement, to legitimize the tax forms. Sahadevan applied for about 71 PPP loans totaling more than \$941,000 and successfully obtained about \$146,000. He also applied for and received 8 EIDLs totaling

more than \$283,000. Sahadevan then laundered the money by purchasing and trading securities and cryptocurrency, settling personal debts, and making payments to his girlfriend.

We conducted this investigation with the FBI. The U.S. Attorney’s Office for the District of Maryland is prosecuting.

Bank Teller Pleaded Guilty to Stealing Nearly \$90,000 Deposited by Georgia Convenience Store

Kayla Monroe Evans pleaded guilty to skimming nearly \$90,000 from a Georgia convenience store’s deposits while working as a teller at Synovus Bank, a state member bank. She faces up to 30 years in prison, along with substantial fines and restitution, followed by up to 3 years of supervised release.

For nearly 2 years, Evans handled the convenience store’s deposits. An auditor for the store began noticing substantial differences between the amount of cash presented to the bank compared with the amount actually deposited. The investigation discovered that Evans was frequently skimming large amounts of cash from the deposits for her personal use, stealing almost \$90,000 in total. As part of her plea, Evans agreed to pay restitution for the full loss to the store and to never seek employment in any financial institution.

We conducted this investigation with the Candler County Sheriff’s Office, the District Attorney’s Office for the Middle Judicial Circuit, and the Georgia Bureau of Investigation. The U.S. Attorney’s Office for the Southern District of Georgia is prosecuting.

Two Loan Brokers and a Loan Officer Pleaded Guilty in Massachusetts to Bank Fraud Conspiracy

Ted Capodilupo and Joseph Masci, operators of a loan brokerage business, pleaded guilty to conspiracy to commit bank fraud against a Massachusetts-based bank and the SBA. Brian Ferris, a loan officer at the bank, also pleaded guilty to conspiracy to commit bank fraud. The charges carry up to 30 years in prison and 5 years of supervised release; a fine of up to \$1 million or twice the defendants’ gain or victims’ loss, whichever is greater; restitution; and forfeiture.

Capodilupo, Masci, and Ferris agreed to defraud the bank and the SBA by submitting fraudulent loan applications to the bank, which administered the SBA’s small business express loan program. Capodilupo and Masci submitted dozens of fraudulent applications on behalf of borrowers who were ineligible for traditional business loans. They misrepresented, among other things, the identity of the real loan recipients and the businesses the loans were sought for, and they falsified documents supporting the applications. Capodilupo and Masci charged borrowers fees for obtaining these fraudulent loans. Ferris,

who worked as a loan officer at the bank, caused the bank to issue the loans in exchange for a kickback of about \$500 per loan. The scheme generated about \$270,000 in fees for Capodilupo and Masci. Many of the loans ultimately defaulted, resulting in substantial losses to the bank.

We conducted this investigation with the FBI, the FDIC OIG, and the SBA OIG. The U.S. Attorney’s Office for the District of Massachusetts is prosecuting.

Kansas City Bank Manager Indicted for \$12.4 Million PPP Fraud and Unemployment Benefits Fraud

Anthony Omar Brockman, a former bank branch manager, was indicted for accepting gifts in exchange for facilitating a \$12.4 million PPP loan fraud scheme. He was also charged for a scheme to receive over \$11,000 in unemployment benefits. 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.

The indictment alleges that Brockman facilitated fraudulent PPP loan applications for Tod Ray Keilholz, the owner of TRK Construction and three other Missouri businesses. Keilholz was charged separately for his role in a more than \$27.1 million bank fraud scheme that included over \$12.4 million in PPP loans. In exchange for his help securing the loans, Brockman accepted a new Chevrolet Tahoe and National Football League playoff tickets, which Keilholz bought with his fraudulently gained loan proceeds. Further, Brockman signed an affidavit gifting the vehicle to Rich Boy Prep, a charity of which his wife was the CEO, but instead sold the vehicle.

We conducted this investigation with the FBI, the FDIC OIG, the IRS CI, the SBA OIG, and the U.S. Treasury Inspector General for Tax Administration. The U.S. Attorney’s Office for the Western District of Missouri is prosecuting.

Tax Officer, Five Others, Charged in California for Multimillion Dollar PPP Fraud

Six individuals face a variety of charges for alleged schemes to fraudulently obtain millions of dollars in PPP loans. Frank Mosley, a former IRS revenue officer and current City of Oakland tax enforcement officer; his brother Reginald Mosley; Marcus Wilborn; Aaron Boren; and Scott Conway were charged with conspiracy to commit bank fraud, which carries up to 30 years in prison. Frank and Reginald Mosley were also charged with aiding and advising in the filing of false tax returns, which carries up to 3 years in prison. Kenya Ellis was charged in a separate case with bank fraud, which carries up to 30 years in prison. The defendants may also be ordered to pay restitution and additional assessments and required to serve periods of supervised release. 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, Frank and Reginald Mosley submitted a fraudulent PPP loan application for Forward Thinking Investors, which they controlled. After receiving over \$1 million in loan proceeds, Reginald Mosley recruited acquaintances, including Wilborn, Boren, and Conway, to submit additional fraudulent applications. They submitted applications on behalf of four entities they claimed had dozens of employees and monthly payrolls up to \$430,000. However, the entities were merely shell companies with no payroll expenses. The defendants received some \$3 million in loan proceeds, which they then used for significant personal expenses, personal credit cards, personal investments, and distributions to their family members. Frank and Reginald Mosley also filed fraudulent tax returns with the IRS in an attempt to cover up their scheme. Ellis allegedly aided and advised Frank and Reginald Mosley and others in submitting fraudulent PPP loan applications, while fraudulently obtaining for herself more than \$296,000 in PPP and other COVID-related loans.

We conducted this investigation with the IRS CI and the SBA OIG. The U.S. Attorney’s Office for the Northern District of California is prosecuting.



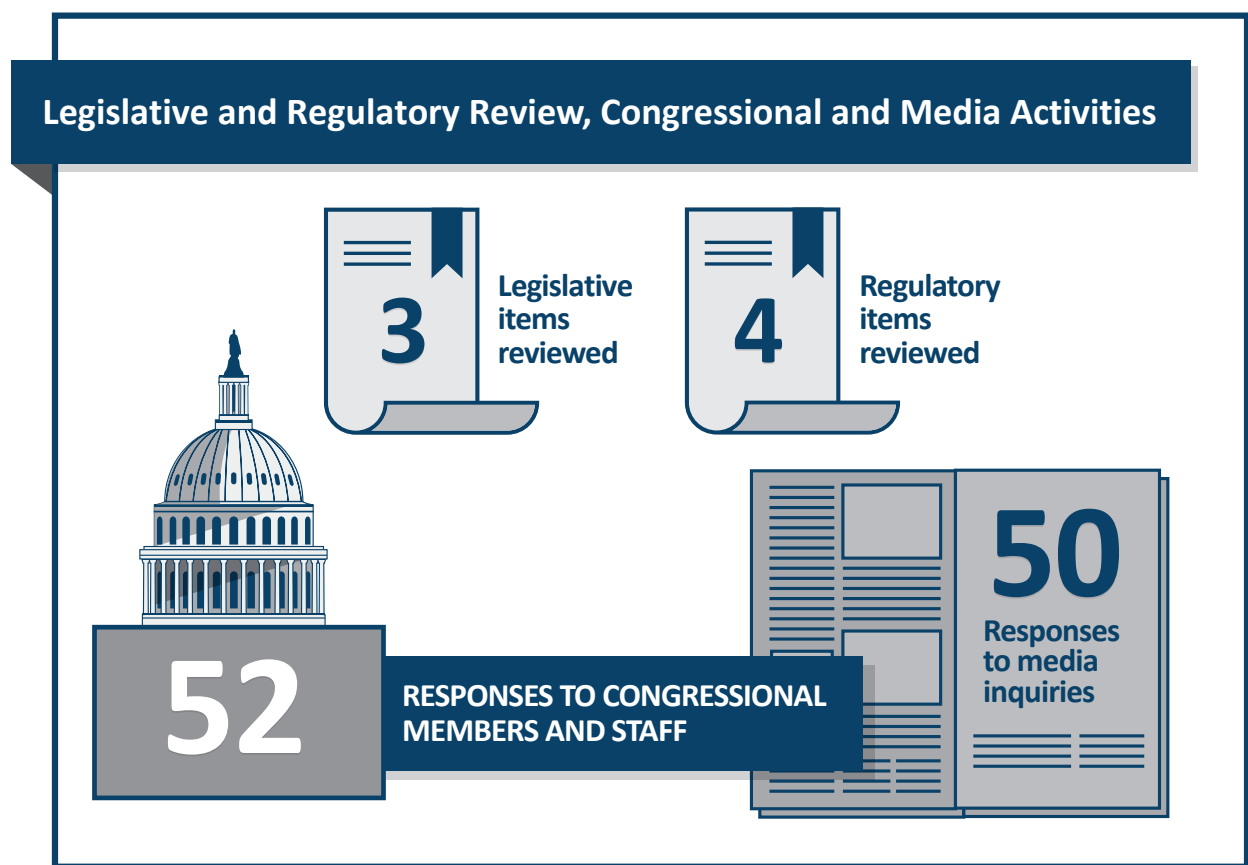
Hotline

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 by phone, [web form](#), fax, or 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 206 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. During this reporting period, OLS reviewed three legislative items and four regulatory items.

Congressional and Media Activities

We communicate and coordinate with various congressional committees on issues of mutual interest. During this reporting period, we provided 52 responses to congressional members and staff concerning the Board and the CFPB. Additionally, we responded to 50 media inquiries.

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 is a searchable website containing the latest public reports from federal OIGs. It provides access to over 27,000 reports, detailing for fiscal year 2023 alone around \$79 billion in potential savings and around 5,300 recommendations to improve programs across the federal government.

The IG serves as a member of CIGIE’s Legislation Committee and Technology Committee and is the vice chair of the Investigations Committee. The Legislation Committee is the central point of information for legislative initiatives and congressional activities that may affect the OIG community. The Technology Committee facilitates effective information technology (IT) audits, evaluations, and investigations and provides a forum for the expression of the OIG community’s perspective on governmentwide IT operations. The Investigations Committee advises the OIG community on issues involving criminal investigations, criminal investigations personnel, and criminal investigative guidelines. The IG is also a member of CIGIE’s Diversity, Equity, Inclusion, and Accessibility Work Group. The work group works to affirm, advance, and augment CIGIE’s commitment to promote a diverse, equitable, inclusive, and accessible workforce and workplace environment throughout the OIG community.

In addition, the IG serves on CIGIE’s PRAC, which coordinates oversight of federal funds authorized by the CARES Act and the COVID-19 pandemic response. The IG is the vice chair of the PRAC Investigations Subcommittee and is a member of the PRAC Financial Sector Oversight Subcommittee.

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 and are current members of the Federal Audit Executive Council’s Quality Assurance Work Group.



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 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 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 therein and our internal policies and procedures.
- 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*.
- In September 2023, we completed an evaluation peer review of the SBA OIG and reported that the organization generally complied with Blue Book requirements.

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
Following Established Processes Helped FRB New York and the Board Reduce Risks Associated With Lending Facility Contracts	Evaluation
The Board Can Further Enhance the Design and Effectiveness of the FOMC's Investment and Trading Rules	Evaluation
Board Purchase Card Program Controls Are Generally Effective and Can Be Further Strengthened	Audit
The Board Can Enhance Its Procedures and Controls for Protecting Confidential Information in Supervision Central	Evaluation
Results of Scoping of the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions	Evaluation
The Board and FRB Boston Generally Followed Their Process for Purchasing MSLP Loan Participations but Can Formally Document Some Key Processes	Evaluation
The Board's Approach to Climate Risk Supervision at Financial Institutions	Insights
Calendar Years 2020–2022 Risk Assessment of the Board's Government Travel Card Program	Risk assessment
Material Loss Review of Silicon Valley Bank	Evaluation
Review of the Supervision of Silvergate Bank	Evaluation
2023 Audit of the Board's Information Security Program	Audit
Total number of audit reports: 2	
Total number of evaluation reports: 7	
Total number of other 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 of recommendations		
		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	09/23	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	01/23	7	1
2017 Audit of the Board's Information Security Program	10/17	9	9	0	09/23	8	1
Security Control Review of the Board's Public Website (nonpublic)	03/18	7	7	0	05/23	6	1
Security Control Review of the Board Division of Research and Statistics' General Support System (nonpublic)	09/18	9	9	0	05/23	9	0
2018 Audit of the Board's Information Security Program	10/18	6	6	0	09/23	5	1
The Board Can Strengthen Information Technology Governance	11/18	6	6	0	05/23	6	0
2019 Audit of the Board's Information Security Program	10/19	6	6	0	09/23	4	2

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Board’s Oversight of Its Designated Financial Market Utility Supervision Program Is Generally Effective, but Certain Program Aspects Can Be Improved	03/20	6	6	0	09/23	5	1
2020 Audit of the Board’s Information Security Program	11/20	4	4	0	09/23	3	1
The Board’s Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced	09/21	3	3	0	06/22	1	2
The Board Can Enhance Its Personnel Security Program	01/22	6	6	0	08/23	6	0
The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems	03/22	3	3	0	05/23	0	3
Testing Results for the Board’s Software and License Asset Management Processes (nonpublic)	06/22	1	1	0	05/23	0	1
Security Control Review of the Board’s Secure Document System (nonpublic)	06/22	1	1	0	05/23	1	0
2022 Audit of the Board’s Information Security Program	09/22	1	1	0	09/23	0	1

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Board Can Enhance the Effectiveness of Certain Aspects of Its Model Risk Management Processes for the SR/HC-SABR and BETR Models	12/22	7	7	0	06/23	7	0
The Board Can Enhance Certain Governance Processes Related to Reviewing and Approving Supervisory Proposals	12/22	9	9	0	08/23	2	7
The Board Can Enhance Enterprise Practices for Data Management Roles and Responsibilities	01/23	5	5	0	08/23	2	3
The Board Can Further Enhance the Design and Effectiveness of the FOMC's Investment and Trading Rules	04/23	6	6	0	n.a.	0	6
Board Purchase Card Program Controls Are Generally Effective and Can Be Further Strengthened	05/23	1	1 ^a	0	07/23	1	0
The Board Can Enhance Its Procedures and Controls for Protecting Confidential Information in Supervision Central	06/23	2	2	0	09/23	0	2
Results of Scoping of the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions	06/23	6	6	0	n.a.	0	6

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Board and FRB Boston Generally Followed Their Process for Purchasing MSLP Loan Participations but Can Formally Document Some Key Processes	07/23	1	1	0	n.a.	0	1
Material Loss Review of Silicon Valley Bank	09/23	7	7	0	n.a.	0	7
Review of the Supervision of Silvergate Bank (nonpublic)	09/23	12	12	0	n.a.	0	12
2023 Audit of the Board's Information Security Program	09/23	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.

^a The Board partially concurred with this recommendation.

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

Report title	Type of report
Report on the Independent Audit of the CFPB’s Agile Systems/Software Development Life Cycle Processes	Audit
Fiscal Years 2020–2022 Risk Assessment of the CFPB’s Government Travel Card Program	Risk assessment
The CFPB Can Improve Its Controls for Exercising Contract Options	Audit
2023 Audit of the CFPB’s Information Security Program	Audit
Total number of audit reports: 3	
Total number of evaluation reports: 0	
Total number of other 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 of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
2014 Audit of the CFPB's Information Security Program	11/14	3	3	0	09/23	2	1
2017 Audit of the CFPB's Information Security Program	10/17	7	7	0	09/23	6	1
The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data	01/18	11	11	0	08/23	10	1
2018 Audit of the Bureau's Information Security Program	10/18	4	4	0	09/23	2	2
2019 Audit of the Bureau's Information Security Program	10/19	7	7	0	09/23	7	0
Technical Testing Results for the Bureau's Legal Enclave (nonpublic)	07/20	4	4	0	03/23	1	3
The Bureau Can Strengthen Its Hiring Practices and Can Continue Its Efforts to Cultivate a Diverse Workforce	03/21	10	10	0	09/23	5	5
The Bureau Can Improve Its Controls for Issuing and Managing Interagency Agreements	07/21	6	6	0	09/23	5	1
Evaluation of the Bureau's Implementation of Splunk (nonpublic)	09/21	4	4	0	03/23	1	3
2021 Audit of the Bureau's Information Security Program	10/21	3	3	0	09/23	3	0

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Bureau Can Improve Aspects of Its Quality Management Program for Supervision Activities	11/21	9	9	0	08/23	8	1
The CFPB Is Generally Prepared to Implement the OPEN Government Data Act and Can Take Additional Steps to Further Align With Related Requirements	09/22	2	2	0	09/23	2	0
2022 Audit of the CFPB’s Information Security Program	09/22	6	6	0	09/23	1	5
2023 Audit of the CFPB’s Information Security Program	09/23	1	1	0	n.a.	0	1

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 With Questioned Costs, Unsupported Costs, or Recommendations That Funds Be Put to Better Use During the Reporting Period

Reports	Number	Dollar value
With questioned costs, unsupported costs, or recommendations that funds be put to better use, regardless of whether a management decision had been made	0	\$0

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. In the event that an audit or evaluation report contains quantifiable information regarding questioned costs, unsupported costs, or recommendations that funds be put to better use, this table will be expanded.

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	179
Investigations opened during the reporting period	17
Investigations closed during the reporting period	28
Investigations open at end of the reporting period	168
Investigative results for the reporting period	
Persons referred to DOJ prosecutors	5
Persons referred to state/local prosecutors	0
Declinations received	6
Joint investigations	125
Reports of investigation issued	1
Oral and/or written reprimands	0
Terminations of employment	0
Arrests	19
Suspensions	0
Debarments	0
Prohibitions from banking industry	2
Indictments	14
Criminal informations	12
Criminal complaints	1
Convictions	27
Civil actions	\$0
Administrative monetary recoveries and reimbursements	\$0

See notes at end of table.

Investigative actions	Number or dollar value^a
Civil judgments	\$0
Criminal fines, restitution, and special assessments	\$349,612,570
Forfeiture	\$43,655,703

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

^a Metrics: These statistics were compiled from the OIG's 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	3
Complaints received during reporting period	206
Total complaints for reporting period	209
Complaints resolved during reporting period	196
Complaints pending	13



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 to include additional summaries and statistics for the reporting period. Our response to these requirements is below.

An identification of each recommendation made before the reporting period, for which corrective action has not been completed, including the potential cost savings associated with the recommendation.

- See [appendix C](#).

Statistical tables showing for the reporting period (1) the number of issued investigative reports, (2) the number of persons referred to the DOJ for criminal prosecution, (3) the number of persons referred to state and local authorities for criminal prosecution, and (4) the number of indictments and criminal informations that resulted from any prior referral to prosecuting authorities. Describe the metrics used to develop the data for these new statistical tables.

- See [table A-6](#).

A report on each investigation conducted by the OIG where allegations of misconduct were substantiated involving a senior government employee, which includes (1) the name of the senior government official, if already made public by the OIG; (2) a detailed description of the facts and circumstances of the investigation as well as the status and disposition of the matter; (3) whether the matter was referred to the DOJ and the date of the referral; and (4) whether the DOJ declined the referral and the date of such declination.

- We have no such investigations to report.

A detailed description of any instance of whistleblower retaliation, including information about the official found to have engaged in retaliation and what, if any, consequences the agency imposed to hold that official accountable.

- We have no such instances to report.

Information related to interference by the Board or the CFPB, including (1) a detailed description of any attempt by the Board or the CFPB to interfere with the independence of the OIG, such as through budget constraints designed to limit OIG capabilities and incidents when either agency has resisted or objected to OIG oversight activities or restricted or significantly delayed OIG access to information, including the justification of the establishment for such action, and (2) a summary of each report made to the Board of Governors or the CFPB director during the reporting period regarding unreasonable refusals or failures to provide information or assistance to the OIG.

- We have nothing to report.

Detailed descriptions of (1) inspections, evaluations, and audits conducted by the OIG that were closed and not disclosed to the public and (2) investigations conducted by the OIG involving a senior government employee that were closed and not disclosed to the public.

- We investigated allegations that a senior Board employee retaliated against an employee who had filed complaints with Employee Relations and the OIG by denying that employee a promotion opportunity. The investigation did not substantiate these claims. This investigation was closed.



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	2	2
2019	1	2
2020	2	2
2021	1	2
2022	4	12
2023 ^a	1	3

^a Through March 31, 2023.

2016 Audit of the Board’s Information Security Program

2016-IT-B-013

November 10, 2016

Total number of 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 number of 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.

2017 Audit of the Board’s Information Security Program

2017-IT-B-018

October 31, 2017

Total number of 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.

Security Control Review of the Board’s Public Website (nonpublic)

2018-IT-B-008R

March 21, 2018

Total number of recommendations: 7

Recommendations open: 1

The open recommendation relates to strengthening cybersecurity risk management processes.

2018 Audit of the Board’s Information Security Program

2018-IT-B-017

October 31, 2018

Total number of 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 number of 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’s Oversight of Its Designated Financial Market Utility Supervision Program Is Generally Effective, but Certain Program Aspects Can Be Improved

2020-FMIC-B-005

March 18, 2020

Total number of recommendations: 6

Recommendations open: 1

2. Define and document which parties at the division director and governor levels will have a role in reviewing and approving enforcement actions for designated financial market utilities.

2020 Audit of the Board’s Information Security Program

2020-IT-B-020

November 2, 2020

Total number of recommendations: 4

Recommendations open: 1

3. Ensure that the Board’s continuous monitoring processes include the security control requirements for applicable network devices.

The Board’s Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced

2021-IT-B-011

September 15, 2021

Total number of recommendations: 3

Recommendations open: 2

1. Work with Board divisions to conduct an assessment of the current risk management practices and risk culture across the agency and use the results to inform the direction of the Board’s enterprise risk management program.
2. Work with the administrative governor, as appropriate, to determine an optimal governance structure and associated reporting relationships for the agency’s enterprise risk management program and update the *Delegations of Administrative Authority* accordingly.

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

2022-IT-B-006

March 23, 2022

Total number of 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 Program 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 number of 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 number of recommendations: 1

Recommendations open: 1

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

The Board Can Enhance Certain Governance Processes Related to Reviewing and Approving Supervisory Proposals

2022-SR-B-017

December 7, 2022

Total number of recommendations: 9

Recommendations open: 7

1. Develop, in consultation with the Board of Governors, a dashboard or similar tool for Board members that forecasts planned supervisory policy and guidance proposals. As part of this effort, assign responsibilities for maintaining and updating the dashboard or tool and establish a frequency for distributing the dashboard or tool.
2. Update the Policy Issuance Processing Form template to provide guidance on how to document Board member and Board committee consultation on supervisory policy and guidance proposals.
3. Issue internal guidance on the process for soliciting public comment on supervisory policy and guidance proposals that defines
 - a. the types of supervisory proposals that should be submitted for public comment.
 - b. the options for soliciting public comment on a proposal.
 - c. the factors that should be considered when determining whether to seek comment and, if the Board decides to solicit public comment on a supervisory proposal, which option to use.
 - d. the approval process for whether and how to solicit public comment.

4. Update, in consultation with the Board of Governors, the director of the Division of Financial Stability, and the general counsel, the delegations of authority related to the stress testing program to clarify how actions should be delegated when there is no vice chair for supervision or Committee on Supervision and Regulation (CSR) chair.
5. Update, in consultation with the Board of Governors, the director of the Division of Supervision and Regulation, and the general counsel, the CSR charter to state how the committee should operate in the absence of a vice chair for supervision and a CSR chair, including specifying who is responsible for setting the strategic direction and priorities of the committee and developing committee meeting agendas.
6. Update, in consultation with the Board of Governors, the *Board Organization and Procedures* policy to state who will fill the role of oversight governor for the Division of Supervision and Regulation if the Board chair has not appointed one.
7. Establish a process to document CSR meetings, including describing what guidance or concurrence was provided to Board staff.

The Board Can Enhance Enterprise Practices for Data Management Roles and Responsibilities

2023-MO-B-001

January 18, 2023

Total number of recommendations: 5

Recommendations open: 3

2. Develop and obtain Board Data Council approval for a Boardwide policy to facilitate the adoption of the finalized data management roles and responsibilities.
3. Develop and provide training related to Boardwide data management roles and responsibilities to foster consistent messaging and expectations.
4. Develop guidance for creating and managing data inventories, including roles and responsibilities and metadata standards.

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
2014	1	1
2015	0	0
2016	0	0
2017	1	1
2018	2	3
2019	0	0
2020	1	3
2021	4	10
2022	1	5
2023 ^a	0	0

^a Through March 31, 2023.

2014 Audit of the CFPB's Information Security Program

2014-IT-C-020

November 14, 2014

Total number of recommendations: 3

Recommendations open: 1

3. Strengthen the CFPB's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database and application-level security configurations.

2017 Audit of the CFPB’s Information Security Program

2017-IT-C-019

October 31, 2017

Total number of recommendations: 7

Recommendations open: 1

1. Ensure that a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain an agencywide risk profile.

The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data

2018-MO-C-001

January 22, 2018

Total number of recommendations: 11

Recommendations open: 1

2. Finalize the building access system upgrade to ensure that personal identity verification badges and site badges are automatically deactivated in the building access system and that personal identity verification badges are automatically deactivated in the USAccess system upon an individual’s separation.

2018 Audit of the Bureau’s Information Security Program

2018-IT-C-018

October 31, 2018

Total number of recommendations: 4

Recommendations open: 2

1. Strengthen configuration management processes by
 - a. remediating configuration-related vulnerabilities in a timely manner.
 - b. ensuring that optimal resources are allocated to perform vulnerability remediation activities.
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 number of recommendations: 4****Recommendations open: 3**

The open recommendations relate to strengthening vulnerability management, configuration management, and testing processes.

The Bureau Can Strengthen Its Hiring Practices and Can Continue Its Efforts to Cultivate a Diverse Workforce**2021-MO-C-006****March 29, 2021****Total number of recommendations: 10****Recommendations open: 5**

1. Monitor the use of structured interviews and provide periodic reports tracking the use of structured interviews to senior CFPB officials, such as division and office leaders and the chief operating officer.
5. Align policy, procedure, and guidance documents with the actual practices related to identifying subject-matter experts early in the hiring process and requiring subject-matter expert signatures on combined rating sheets.
7. Implement automated system controls to ensure that key date fields are completed for all hiring actions in the Hiring Tracker database.
8. Update the *Measuring and Reporting Time to Hire* standard operating procedure to include
 - a. comprehensive guidance on documenting purposeful omissions in the Hiring Tracker data entry form.
 - b. Office of Human Capital practices for reviewing the Hiring Tracker database for accuracy and completeness.
9. Require training for staff responsible for entering information into the Hiring Tracker database on
 - a. using the Hiring Tracker data entry form and database.
 - b. the updated standard operating procedure so that practices align with established processes.

The Bureau Can Improve Its Controls for Issuing and Managing Interagency Agreements

2021-FMIC-C-009

July 21, 2021

Total number of recommendations: 6

Recommendations open: 1

1. Create or update existing interagency agreement (IAA) policies and procedures to establish clear expectations for issuing and managing IAAs. Ensure that expectations for the key activities in the IAA process are addressed, including
 - a. roles and responsibilities of relevant parties, including the Bureau of the Fiscal Service, Administrative Resource Center; the Office of the Chief Financial Officer; the Office of the Chief Procurement Officer; program offices; and invoice approvers.
 - b. training and certification requirements for invoice approvers.
 - c. developing and maintaining IAA agreement documents.
 - d. monitoring performance under the IAA.
 - e. approving Intra-Governmental Payment and Collections.
 - f. deobligating and closing IAAs.

Evaluation of the Bureau’s Implementation of Splunk (nonpublic)

2021-IT-C-010R

September 8, 2021

Total number of recommendations: 4

Recommendations open: 3

The open recommendations relate to strengthening risk management, access control, and hardware asset management processes.

The Bureau Can Improve Aspects of Its Quality Management Program for Supervision Activities

2021-SR-C-016

November 1, 2021

Total number of recommendations: 9

Recommendations open: 1

7. Assess the Quality Management Program’s current staffing level and structure to determine whether additional or dedicated resources are needed or whether the current 25 percent time allotment for conducting quality assurance reviews and the 2-week time allotment for quality control reviews

should be revised. Develop and implement plans to address the program’s staffing needs based on the results of the assessment.

2022 Audit of the CFPB’s Information Security Program

2022-IT-C-014

September 30, 2022

Total number of recommendations: 6

Recommendations open: 5

2. Ensure that the CFPB’s new data loss prevention tool is implemented and configured to monitor traffic across all network access points and environments, as applicable.
3. Ensure that policies and supporting procedures for developing and maintaining an enterprisewide software inventory are developed and maintained.
4. Ensure that an enterprisewide software inventory is conducted and maintained.
5. Ensure the development of policies and procedures for the performance and maintenance of an organizationwide business impact analysis.
6. Update the CFPB’s organizationwide business impact analysis and ensure that the results are used to make applicable changes to related contingency and continuity plans.



Abbreviations

CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CEO	chief executive officer
CI	Criminal Investigation
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CSR	Committee on Supervision and Regulation
DIF	Deposit Insurance Fund
DOJ	U.S. Department of Justice
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
FRB Boston	Federal Reserve Bank of Boston
FRB New York	Federal Reserve Bank of New York
FRB San Francisco	Federal Reserve Bank of San Francisco
GTC	government travel card
IAA	interagency agreement
IG	inspector general
IRS	Internal Revenue Service
IT	information technology
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

SBA U.S. Small Business Administration
SVB Silicon Valley Bank



Office of Inspector General

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

20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551
Phone: 202-973-5000 | Fax: 202-973-5044

OIG Hotline

oig.federalreserve.gov/hotline
oig.consumerfinance.gov/hotline

800-827-3340

