Office of Inspector General

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

Semiannual Report to Congress

April 1, 2021–September 30, 2021

OIG

Semiannual Report to Congress

April 1, 2021–September 30, 2021

Office of Inspector General

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

Message From the Inspector General

This summer marked my 10-year anniversary as the inspector general for the Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection. Over the past decade, we have issued 225 reports containing 411 recommendations to the Board and 314 recommendations to the Bureau. Our Office of Investigations opened 357 cases and closed 249 cases, and our investigative work resulted in 118 arrests and $7.2 billion in criminal fines, restitution, forfeiture, civil judgments, and monetary recoveries. As I look back on the past decade, I am proud of our many accomplishments and am especially grateful for the extraordinary resilience and dedication the OIG staff have demonstrated over these years.

Throughout my time as inspector general, information security has been a growing concern. Federal agencies have seen breaches of sensitive data and an increase in information security incidents. These threats can create significant operational risk, disrupt critical services, and ultimately affect financial stability. Indeed, several of the major management challenges we have identified for the Board and the Bureau in recent years relate to information security.

We have produced more than 80 information technology (IT)–related reports and memorandums during my tenure, including annual audits of each agency, pursuant to the Federal Information Security Modernization Act of 2014 (FISMA), to determine the effectiveness of the agencies' information security policies, procedures, and processes. During this reporting period, we examined the Bureau's implementation of Splunk, a software platform used for monitoring, searching, and analyzing real-time machine-generated data critical to the Bureau's IT security environment. We also evaluated the progress made by the Board in maturating its enterprise risk management program and the agency's adoption of cloud computing systems.

We have started using scanning tools to identify vulnerabilities and ensure proper information security configurations and have increasingly employed data analytics in many aspects of our oversight work. In this reporting period, for example, we used data analytics to identify potentially unusual transactions in our audit of the Board's payroll controls and determined that the Board's payroll controls are generally effective. We also are using data analytics to better understand certain IT risks to address FISMA review

requirements more efficiently, and we used data analytics to identify improvements in the accuracy and transparency of the Board's public reporting under the Coronavirus Aid, Relief, and Economic Security Act.

Our Office of Investigations has grown significantly in the past decade. We opened field offices in Chicago, Miami, New York City, and San Francisco and have strengthened our relationships with other federal law enforcement agencies, including U.S. attorney's offices throughout the country and state and local law enforcement. We also created the Special Investigations Unit, which focuses on internal investigations of Board and Bureau employees, and modernized the Electronic Crimes Unit.

The pandemic resulted in a massive increase in our investigative case load. In 2018, we had 60 investigations open; currently, 146 are open, 92 of which involve alleged fraud against one or more of the Board's pandemic lending facilities. In the past 6 months, we closed 18 investigations and resolved 239 hotline complaints, and our work resulted in 24 matters for prosecutorial consideration; 27 convictions; and $6.5 million in criminal fines, restitution, and special assessments.

Diversity, equity, and inclusion (DE&I) has become an increasingly salient and essential aspect of our work over the past decade. We have taken many significant steps to expand and promote DE&I initiatives as an organization during my tenure, including establishing our DE&I Committee in 2014, incorporating DE&I principles into our strategic plan, offering a variety of DE&I trainings, hosting listening events, and developing a DE&I competency for use in performance management. I look forward to making further progress in this area.

I continue to serve on the Pandemic Response Accountability Committee, which coordinates inspector general community oversight of the federal government's COVID-19 pandemic response efforts. In addition, our office has planned and initiated a variety of projects related to the Federal Reserve's lending facilities that were established in response to the pandemic. This reporting period, we issued two memorandums as part of our ongoing evaluation of third-party cybersecurity risk management processes for vendors supporting the Main Street Lending Program and the Secondary Market Corporate Credit Facility. More information about our ongoing pandemic response oversight work is available in the Pandemic Response Oversight section of this report.

Finally, we recently welcomed new leadership to the Bureau, as Rohit Chopra was confirmed as director. We look forward to working with Director Chopra and his team as we provide independent oversight to improve the Bureau's programs and operations and to prevent and detect fraud, waste, and abuse.

As I reflect on the past decade and look to the future, I feel profound gratitude for the tremendous flexibility of the OIG staff, who have remained steadfastly committed to our mission, vision, and values despite the many personal and professional challenges they have faced in recent years. They have exemplified commitment, resourcefulness, and professionalism, and I am immensely proud of the work we have accomplished. I look forward to continuing to work together to achieve our vitally important mission.

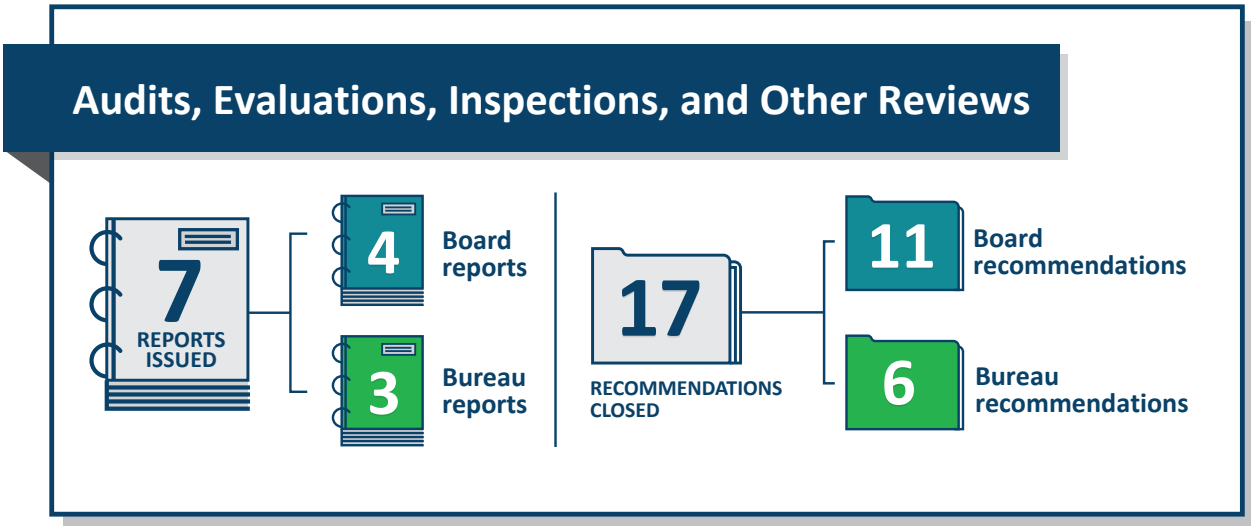
Sincerely,

Mark Bialek
Inspector General
October 29, 2021

Contents

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 Bureau of Consumer Financial Protection. The following are highlights, in chronological order, of our work during this semiannual reporting period.



The Board's Publicly Reported Data for the Main Street Lending Program and the Secondary Market Corporate Credit Facility

We identified several inaccurate city and state data points affecting a limited number of published loan transactions for the Main Street Lending Program (MSLP) as well as Secondary Market Corporate Credit Facility (SMCCF) transactions that appear to have been documented twice in each of the publicly reported transaction-specific disclosures published from January through April 2021.

The Bureau's Controls for Issuing and Managing Interagency Agreements

The Bureau can improve existing interagency agreement (IAA) guidance and internal controls, enforce internal controls to ensure compliance with IAA policies and procedures, and ensure the completeness of reports containing IAA data.

The Board's Payroll Controls

The Board's payroll controls are generally effective in ensuring compliance with applicable laws, regulations, policies, and procedures.

The Board's Implementation of Enterprise Risk Management

The Board continues to take steps to develop and implement an enterprise risk management (ERM) program; however, we identified opportunities to enhance the agency's planning, governance, and implementation of its ERM program and processes.

Former Board Employee Sentenced for Theft of Government Property

Former Board employee Venkatesh Rao was sentenced to 1 year of supervised probation and a $2,500 fine for theft of government property. He removed proprietary information used by the Board to conduct bank stress tests and stored the materials at his home.

Florida Resident Sentenced for $3.9 Million Paycheck Protection Program Fraud

Florida resident David T. Hines was sentenced to more than 6 years in prison for wire fraud. He obtained $3.9 million in Paycheck Protection Program (PPP) loans by falsifying payroll information and submitting bogus Internal Revenue Service (IRS) forms. Hines was also ordered to forfeit $3.4 million as well as the $318,000 Lamborghini luxury car he bought for himself using the loan proceeds.

Introduction

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

In accordance with the Inspector General Act of 1978, as amended (5 U.S.C. app. 3), 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 Bureau programs and operations
- help prevent and detect fraud, waste, abuse, and mismanagement in Board and Bureau programs and operations
- review existing and proposed legislation and regulations to make recommendations about possible improvements to Board and Bureau programs and operations
- keep the Board of Governors, the Bureau 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 in order to detect and prevent fraud, waste, abuse, and mismanagement and 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 Bureau'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 Federal Reserve Bank and of the Board. The Board performs the accounting function for the Federal Financial Institutions Examination Council (FFIEC), and we oversee the annual financial statement audits of the Board and of the FFIEC.[1] Under the Dodd-Frank Wall Street Reform and Consumer Protection Act, the U.S. Government Accountability Office performs the financial statement audit of the Bureau.
- The Digital Accountability and Transparency Act of 2014 (DATA Act; 31 U.S.C. § 6101 note) requires agencies to report financial and payment data in accordance with data standards established by the U.S. Department of the Treasury and the Office of Management and Budget (OMB). The Bureau has determined that its Consumer Financial Civil Penalty Fund is subject to the DATA Act and that only one specific DATA Act requirement, section 3(b), applies to the Bureau Fund. The DATA Act requires us to review a statistically valid sample of the data submitted by the agency and report on its completeness, timeliness, quality, and accuracy and on the agency's implementation and use of the data standards.
- 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 Bureau 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 Bureau'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 Wall Street Reform and Consumer Protection 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

1. The FFIEC is a formal interagency body empowered (1) to 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 Bureau and (2) to make recommendations to promote uniformity in the supervision of financial institutions.

apply to the broader financial sector and ways to improve financial oversight.[2] Additionally, CIGFO must report annually about the IGs' concerns and recommendations, as well as issues that may apply to the broader financial sector. CIGFO can also convene a working group of its members to evaluate the effectiveness and internal operations of the Financial Stability Oversight Council, which was created by the Dodd-Frank Act and is charged with identifying threats to the nation's financial stability, promoting market discipline, and responding to emerging risks to the stability of the nation's financial system.

- Section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Act (12 U.S.C. § 1831o(k)), outlines certain review and reporting obligations for our office when a state member bank failure occurs. The nature of those review and reporting requirements depends on the size of the loss to the Deposit Insurance Fund.
- The Federal Reserve Act, as amended by the USA PATRIOT Act of 2001 (12 U.S.C. § 248(q)), grants the Board certain federal law enforcement authorities. We perform the external oversight function for the Board's law enforcement program.

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

Pandemic Response Oversight

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 that ensure liquidity in financial markets and provide lending support to various sectors of the economy. In addition, the Bureau 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 U.S. Small Business Administration (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 to efficiently deploy resources where they are most needed.

Inspector General Bialek continues to serve on PRAC and is an active member of the PRAC Financial Sector Workgroup.

Updated OIG Management Challenges

Because of the importance of the Board's pandemic response measures, in March 2021 we identified a new management challenge—Designing and Operationalizing Emergency Lending Programs to Address the Economic Effects of the COVID-19 Pandemic. We also identified issues related to the pandemic response that ripple through many of our previously identified challenges, particularly those related to governance, information security, workforce safety, and financial institution supervision.

The Bureau plays a vital role in enforcing federal consumer protection laws and protecting consumers from abuse, especially during challenging economic times. We have adapted aspects of the Bureau's management challenges to highlight the operational challenges presented by the pandemic response. Specifically, our Bureau management challenges highlight the operational challenges presented by ensuring employee safety during the pandemic, adapting the Bureau's financial institution oversight strategy and program, and managing an increase in consumer complaint activity during the pandemic.

Ongoing Monitoring Activities and Ongoing and Planned Audits and Evaluations

In 2020, we initiated an ongoing Board pandemic response monitoring effort for risk assessment purposes and to help inform our selection of potential audit and evaluation topics. This monitoring effort 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
- the monitoring and tracking of unique features associated with specific programs, such as
    - the forgiveness of PPP loans and its effect on the security interests under the Paycheck Protection Program Liquidity Facility
    - the limits associated with the Primary Market Corporate Credit Facility and the SMCCF
    - Treasury's equity investments in specific CARES Act programs

Our ongoing monitoring efforts also covered

- measures taken to encourage financial institutions to lend in a manner consistent with the spirit and intent of specific lending programs, such as the PPP
- the Board's efforts to review community banking organizations' participation in pandemic response programs to confirm that participation is commensurate with an institution's governance, risk management, and internal control capabilities
- the extent to which pandemic response lending efforts reach intended recipients and serve intended communities
- the MSLP, with a focus on risks that emerge as the program progresses throughout its life cycle

Finally, although Bureau 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 Bureau's supervisory activity and monitoring of consumer complaints.

Based on our ongoing monitoring effort, we are planning or have initiated the following pandemic response–related projects.

Audit of the Board's Data Collection, Aggregation, Validation, and Reporting Processes for Its CARES Act Lending Programs

The CARES Act and the Federal Reserve Act require the Board to report certain information related to its lending programs. In addition to meeting its statutory reporting requirements, the Board has committed to transparency and accountability by reporting additional information on a monthly basis for some CARES Act–funded lending programs. Such additional information includes names and details of the participants in each program; the amounts borrowed and the interest rate charged; and overall costs, revenues, and fees for each program. We are assessing the Board's processes for collecting, aggregating, and reporting lending information related to its CARES Act programs, including the data validation processes it uses to ensure that the information is accurate and complete.

Evaluation of Third-Party Cybersecurity Risk Management Processes for Vendors Supporting the MSLP and the SMCCF

To support the implementation of specific programs and facilities, the Reserve Banks have contracted with third-party vendors for various services, such as administrative, custodial, legal, design, and investment management services. These vendors provide data generated from the operations and management of the facilities to the Reserve Banks, who then provide the data to the Board. We are evaluating the effectiveness of (1) the risk management processes designed to ensure that effective information security and data integrity controls are implemented by third parties supporting the administration of the MSLP and the SMCCF and (2) select security controls managed by the Reserve Banks for selected systems that process and maintain MSLP and SMCCF data.

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

Many of the Federal Reserve System's emergency lending programs use vendors to establish and operate the programs, and some use multiple vendors. The Federal Reserve Bank of New York (FRB New York) awarded some of these contracts noncompetitively because of the exigent circumstances, and other contracts pose potential conflict-of-interest risks to the System. In addition, the reliance on vendors highlights the importance of FRB New York's monitoring of vendor performance. We plan to assess the System's vendor selection and management processes related to FRB New York's emergency lending programs.

Evaluation of the Federal Reserve System's Loan Purchase and Administration for Its Main Street Lending Program

The System established the MSLP to facilitate lending to small and medium-sized for-profit and nonprofit organizations. To do so, the System purchased $17.5 billion in 1,830 loans from banks and lenders, the majority of which were purchased in the last 2 months of the program. To handle the increase in volume, the Federal Reserve Bank of Boston implemented an expedited loan purchase process for certain lenders. The Federal Reserve Bank of 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, the System contracted with vendors for a variety of these purchase and administration functions, including purchase intake, credit administration, loan workout, and other services. We plan to initiate a project to assess the MSLP loan purchase and administration processes. Our work will specifically cover the expedited loan purchase process, the receipt of required borrower financial information, relevant internal controls, and vendor reliance across the program.

Audit of the Bureau's Consumer Response Operations

The Bureau uses consumer complaints to help inform the agency's supervision activities, enforce federal consumer financial laws, and write rules and regulations. With an increase in consumer complaints as a result of the COVID-19 pandemic and a recent organizational shift to the newly created Division of Consumer Education and External Affairs, Consumer Response faces an operational risk with respect to the timeliness with which it can respond to consumer complaints. We plan to assess the Bureau's effectiveness and timeliness in responding to consumer complaints.

Information Technology Reviews

Our Office of Information Technology is engaged in work on several aspects related to the Board's pandemic response. For example, as part of the evaluation of third-party cybersecurity risk management processes noted above, the office has conducted analytical testing of publicly reported transaction disclosure data for the MSLP and the SMCCF and issued memorandums to the Board in this area. In addition, the Office of Information Technology is expanding the testing of information technology (IT) systems and data involved in the Board's pandemic response.

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, the office has leveraged our relationships with various federal law enforcement organizations,

U.S. attorney's offices, and components of the DOJ. Our investigators regularly meet and coordinate with our law enforcement partners through the PRAC Investigations Committee and the PRAC Task Force and have established an effective coordination and information sharing process with the Special Inspector General for Pandemic Response.

Our recent investigative results and recoveries are described in the Investigations section.

Audits, Evaluations, Inspections, and Other Reviews

Audits assess aspects of the economy, efficiency, and effectiveness of Board and Bureau 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 Bureau'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 and inspections also assess aspects of the economy, efficiency, and effectiveness of Board and Bureau 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. Inspections are often narrowly focused on particular issues or topics and provide time-critical analyses. Our evaluations and inspections 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

Results of Analytical Testing of the Board's Publicly Reported Data for the Main Street Lending Program

April 14, 2021

In response to the economic effects of the COVID-19 pandemic, the Board established several emergency lending programs and facilities to provide loans to employers, certain businesses, and communities across the country. The Board established the MSLP to support lending to small and medium-sized for-profit

businesses and nonprofit organizations that were unable to access the PPP or that required additional financial support after receiving a PPP loan. The MSLP ended on January 8, 2021.

In February 2021, we announced an evaluation of third-party cybersecurity risk management processes for vendors supporting the MSLP and the SMCCF. During our planning work for this evaluation, we checked the accuracy and completeness of specific demographic data to identify invalid city-state combinations. We also determined the accuracy of specific MSLP transaction disclosure data.

We identified several inaccurate city and state data points affecting a limited number of published loan transactions for the MSLP. After informing Board and System officials of these inaccuracies, they took immediate steps to address them and to update the Board's public reporting.

Our final report for this evaluation may include recommendations related to the issues described in this memorandum.

The Board's Payroll Controls Are Generally Effective

2021-FMIC-B-008 **June 7, 2021**

The Federal Reserve Act grants the Board broad authority over employment matters, including employee compensation. Under this authority, the Board has designed and implemented its own compensation and benefits programs. From January 1, 2019, through March 31, 2020, the Board processed $498.5 million in payments to 3,112 Board employees. We assessed the effectiveness of certain payroll internal controls designed to ensure compliance with applicable laws, regulations, policies, and procedures.

The Board's payroll controls are generally effective in ensuring compliance with applicable laws, regulations, policies, and procedures. We used data analytics to identify potentially unusual transactions and to test categories such as premium pay, salary adjustments, tax withholdings, and payroll deductions and additions. We identified one instance in which the Board did not comply with its compensation policy. In that instance, an employee's base salary exceeded the applicable salary maximum for 5 months. After becoming aware of our finding, Payroll implemented a control to determine whether any employee's annual base salary exceeds their applicable salary maximum. We observed the execution of the control and found it to be effective.

We made no recommendations.

Results of Analytical Testing of the Board's Publicly Reported Data for the Secondary Market Corporate Credit Facility

July 14, 2021

In response to the economic effects of the COVID-19 pandemic, the Board established several emergency lending programs and facilities to provide loans to employers, certain businesses, and communities across the country. The Board established two facilities to support credit to large employers: the Primary Market Corporate Credit Facility for new bond and loan issuance and the SMCCF to provide liquidity for outstanding corporate bonds. The Board designed the SMCCF to create a portfolio that tracked a broad, diversified market index of U.S. corporate bonds.

In February 2021, we announced an evaluation of third-party cybersecurity risk management processes for vendors supporting the MSLP and the SMCCF. During our planning work for this evaluation, we identified transactions that appeared to have been documented twice in each of the SMCCF transaction-specific disclosures published from January through April 2021. In addition, we identified instances in each of the publicly reported transaction-specific disclosures published from January through April 2021 in which transactions for partial bond redemptions were not clearly labeled and did not include redemption amounts.

After informing Board and FRB New York officials of these duplicate entries, they took immediate steps to strengthen internal review processes to ensure that these transactions are appropriately recorded in the SMCCF public disclosure data.

We offered two items for management's immediate consideration. Our final report for this evaluation may include recommendations related to these issues.

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

2021-IT-B-011 **September 15, 2021**

To better manage the full spectrum of internal and external risks, federal agencies, including the Board, are increasingly implementing ERM. ERM refers to an agencywide approach to addressing significant risks by considering them as an interrelated portfolio rather than within silos. We assessed the effectiveness of the Board's ongoing efforts to plan, develop, and integrate ERM processes across the agency. Specifically, this evaluation focused on (1) the establishment of supporting ERM governance and operational structures and (2) steps taken to cultivate a risk culture that aligns the risk management program with the Board's mission, vision, strategy, and values.

The Board continues to take steps to develop and implement an ERM program. The agency is performing several foundational ERM activities within the Office of the Chief Operating Officer with the goal of establishing core ERM capabilities before agencywide rollout. Further, the Board has established an interim risk committee to serve as a temporary forum for enterprise risk discussions. However, the Board can enhance the planning, governance, and implementation of its ERM program and processes.

Our report includes recommendations and items for management's consideration related to the foundational aspects of the Board's ERM program. The Board concurred with our recommendations.

Bureau of Consumer Financial Protection

Independent Accountants' Report on the Bureau's Fiscal Year 2020 Compliance With the Payment Integrity Information Act of 2019

2021-FMIC-C-007 April 28, 2021

The PIIA requires agency heads to periodically review and identify all programs and activities that may be susceptible to significant improper payments. In addition, each fiscal year the IG of each agency is required to determine and report on whether the agency is in compliance with the act. We contracted with an independent public accounting firm to audit the Bureau's compliance with the PIIA as it relates to the Civil Penalty Fund for fiscal year 2020. The contract required the audit to be performed in accordance with *Government Auditing Standards* issued by the comptroller general of the United States. We reviewed and monitored the work of the firm to ensure compliance with the contract and *Government Auditing Standards*.

The firm determined that the Bureau complied with the two applicable requirements of the PIIA for fiscal year 2020 as they relate to the Civil Penalty Fund. Specifically, the Bureau published and posted on its website an annual financial statement for the most recent fiscal year, and it conducted a program-specific risk assessment in conformance with section 3352(a) of the PIIA. The other four PIIA requirements are not applicable to the Civil Penalty Fund because the Bureau has determined that the fund is not susceptible to significant improper payments. The firm made no recommendations in its report.

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

2021-FMIC-C-009 July 21, 2021

The Bureau uses IAAs to procure certain goods or services from other government agencies. During fiscal year 2019, the obligated value of its active IAAs totaled some $320 million. We assessed the design and

operating effectiveness of the Bureau's controls for issuing and managing IAAs, including compliance with relevant laws and regulations.

The Bureau's Office of the Chief Procurement Officer and Office of the Chief Financial Officer can improve controls for issuing and managing IAAs. We found that the Bureau's guidance does not clearly and formally describe IAA responsibilities. In addition, the offices did not consistently identify and document the correct statutory authority for issuing IAAs, nor did they follow relevant *Federal Acquisition Regulation* requirements. Further, invoice approvers did not consistently review IAA billings in accordance with the relevant Bureau policy, and the Bureau did not consistently deobligate excess funding on IAAs in a timely manner. Finally, a Procurement report used to satisfy internal and external stakeholder IAA information needs did not contain complete data.

We made recommendations to improve existing IAA guidance and internal controls, to enforce internal controls to ensure compliance with IAA policies and procedures, and to ensure the completeness of reports containing IAA data. The Bureau concurred with our recommendations.

Evaluation of the Bureau's Implementation of Splunk

2021-IT-C-010R **September 8, 2021**

Splunk is a software platform used for monitoring, searching, and analyzing real-time machine-generated data and is often used by organizations as their primary security information and event management application. We examined the Bureau's implementation of Splunk to assess the system's compliance with FISMA and the information security policies, procedures, standards, and guidelines of the Bureau.

The Bureau's implementation of Splunk generally adheres to security best practices, the agency's information security policies and procedures, and FISMA. However, the Bureau can strengthen the effectiveness of controls implemented for Splunk in the areas of risk management, access controls, and configuration management.

Our report includes recommendations and matters for management consideration designed to increase the effectiveness of controls in these areas. The Bureau concurred with our recommendations.

Failed State Member Bank Reviews

Section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Act, requires that we review and report within 6 months on Board-supervised financial institutions whose failure results in a material loss to the Deposit Insurance Fund. Section 38(k) also requires that we (1) semiannually report certain information on financial institutions that incur nonmaterial losses to the Deposit Insurance Fund and (2) conduct an in-depth review of any nonmaterial losses to the Deposit Insurance Fund that exhibit unusual circumstances. No state member bank failures occurred during this reporting period.

Investigations

Our Office of Investigations investigates criminal, civil, and administrative wrongdoing by Board and Bureau employees as well as alleged misconduct or criminal activity that affects the Board's or the Bureau'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*.

During this period, the Office of Investigations met with officials at both the Board and the Bureau to discuss investigative operations and the investigative process. The office also met with counterparts at other financial regulatory agency OIGs to discuss matters of mutual interest, joint investigative operations, joint training opportunities, and hotline operations.

Board of Governors of the Federal Reserve System

The Board is responsible for consolidated supervision of bank holding companies, including financial holding companies formed under the Gramm-Leach-Bliley Act. The Board also supervises state-chartered banks that are members of the System (state member banks). Under delegated authority from the Board, the Reserve Banks supervise bank holding companies and state member banks, and the Board's Division of Supervision and Regulation oversees the Reserve Banks' supervisory activities.

Our office's investigations concerning bank holding companies and state member banks typically involve allegations that senior officials falsified financial records, lied to or misled examiners, or obstructed examinations in a manner that may have hindered the Board's ability to carry out its supervisory operations. Such activity may result in criminal violations, including false statements or obstruction of bank examinations. The following are examples from this reporting period of investigations into matters affecting the Board's ability to carry out its supervisory responsibilities.

Former Board Employee Sentenced for Theft of Government Property

Venkatesh Rao, of Maryland, was sentenced to 1 year of supervised probation, a criminal fine of $2,500, and a special assessment of $25 for theft of government property from the Board, his former employer.

In 2019, the Board notified Rao that his work performance was unsatisfactory, and Rao decided to voluntarily separate from the Board. Before separating, Rao entered a Board building in Washington, DC, approximately 16 times during weekends; he printed more than 50 restricted government documents from his workstation and bypassed Board restrictions on emailing and making electronic copies of restricted materials. Rao removed the restricted documents, which contained proprietary information used by the Board to conduct bank stress tests, from the building and stored the materials at his home.

This case was investigated by our office. It was prosecuted by the U.S. Attorney's Office for the District of Maryland.

Former Bank Teller in Missouri Sentenced to Prison for Embezzling Funds From an Elderly Customer's Account

Missouri resident Anthony Vaughn, a former bank teller at Commerce Bank, a state member bank, was sentenced to 44 months in prison, followed by 5 years of supervised release, after pleading guilty to one count of bank fraud and one count of aggravated identity theft for embezzling funds from an elderly customer's account. The defendant was also ordered to pay $39,559 in restitution and a $200 special assessment. He will be prohibited from working in the banking industry.

Vaughn was embezzling money from an elderly customer's accounts and possessed several check cards issued in the victim's name, which Vaughn printed at a local bank branch. He used the cards on more than 100 occasions for his personal benefit. He also transferred funds to his wife's account from the victim's account, used the victim's funds to buy furniture and plane tickets, and forged several checks up to $30,000 in the victim's name. Vaughn used his position at the bank to create a trail of false entries to cover up his activities. During the investigation, it was discovered that the former bank teller had earlier been involved in similar fraudulent activities while working at two other financial institutions. The total loss to all victims was over $100,000.

This case was investigated by our office and the Federal Deposit Insurance Corporation (FDIC) OIG. It was prosecuted by the U.S. Attorney's Office for the Eastern District of Missouri.

Former Managing Director and Two Former Loan Officers Pleaded Guilty in Widespread Bank Fraud Scheme

Former employees of a Michigan financial institution—YiHou Han, managing director of residential lending, and Hao Liang "Frank" Hu and Amy Lu, loan officers—pleaded guilty to participating in a conspiracy to originate fraudulent residential mortgage loan applications through the bank's low-documentation Advantage Loan Program. The bank's holding company is supervised by the Board.

From 2011 to 2019, the trio falsified and caused to be falsified borrowers' income and debt-to-income ratios, job titles, employment histories, and supporting documents, among other things. As part of the scheme, they instructed borrowers to fabricate deposit histories and to transfer funds to third parties who would then transfer the funds back to the borrowers as gifts to conceal the true source of the funds. They also knowingly facilitated the approval of loans to borrowers involved in money laundering and tax evasion. As part of the plea, Han admitted that her fraudulent actions were encouraged by members of the bank's senior management to increase the bank's revenue and the coconspirators' personal commissions. In sum, the scheme resulted in 2,471 Advantage loans and more than $876 million in credit extended by the bank. Han, Hu, and Lu received about $6.9 million in commissions.

This case was investigated by our office, the Federal Bureau of Investigation (FBI), the FDIC OIG, and the U.S. Postal Inspection Service. It is being prosecuted by the DOJ Criminal Division's Fraud Section.

Former Bank Teller in Arkansas Pleaded Guilty to Bank Fraud for Embezzling Funds From an Elderly Customer's Account

Arkansas resident Rashaud Brown, a former bank teller, pleaded guilty to one count of bank fraud for his role in embezzling funds from Arvest Bank, a state member bank, and from an elderly customer's account. He had been indicted by a federal grand jury in the Eastern District of Arkansas for 1 count of embezzlement by a bank official and 11 counts of bank fraud. As part of the plea agreement, the defendant will be prohibited from working in the banking industry.

Brown engaged in 11 fraudulent cash withdrawals from the elderly victim's account. Brown used his position at the bank to create a trail of false entries in an attempt to cover up his fraudulent activity.

This case was investigated by our office. It is being prosecuted by the U.S. Attorney's Office for the Eastern District of Arkansas.

Former Bank Teller in Arkansas Indicted for Embezzling Funds

Pamela Cooper, a former official vault teller at the Premier Bank of Arkansas, a state member bank, was indicted by a grand jury with one count of theft, embezzlement, or misapplication by a bank officer or employee. 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 the defendant willfully embezzled some $314,000 from the bank by removing money from the vault and concealing the activity by falsifying bank documents. If convicted, the defendant faces a maximum sentence of 30 years in prison and a $1 million fine.

This case was investigated by our office and the FBI. It is being prosecuted by the U.S. Attorney's Office for the Eastern District of Arkansas.

Florida Resident Sentenced for $3.9 Million PPP Fraud

Florida resident David T. Hines was sentenced to more than 6 years in prison for wire fraud after fraudulently obtaining some $3.9 million in PPP loans. The court ordered Hines to forfeit $3.4 million as well as the $318,000 Lamborghini luxury car he bought for himself using the loan proceeds.

Hines submitted multiple PPP applications to an insured financial institution on behalf of different companies, claiming to have had dozens of employees and millions of dollars in monthly payroll. In addition to submitting false and fraudulent IRS forms to support the applications, Hines also helped others obtain fraudulent PPP loans. The financial institution approved and funded about $3.9 million in loans. Within days of receiving the PPP funds, Hines bought a 2020 Lamborghini Huracán, which he registered jointly in his name and in the name of one of his companies. Soon after, he failed to make the payroll payments he claimed on his loan applications. He did, however, make purchases at luxury retailers and resorts in Miami Beach.

This case was investigated by our office, the FDIC OIG, the IRS Criminal Investigation (IRS CI), the SBA OIG, and the U.S. Postal Inspection Service. It was prosecuted by the DOJ and the U.S. Attorney's Office for the Southern District of Florida.

Oklahoma Resident Sentenced to Prison for PPP Fraud

Rafael Maturino of Oklahoma was sentenced to 1 year and 1 day in prison, followed by 3 years of supervised release, after pleading guilty to bank fraud in a scheme to defraud the First Bank of Owasso by applying for a PPP loan under false pretenses. He was also ordered to pay $97,800 in restitution and a $100 special assessment.

Maturino applied for a PPP loan on behalf of Maturino Enterprises Inc., a company he claimed to own and operate. He submitted forms that misrepresented the company's payroll spending, number of employees, and taxes paid. He also admitted to misrepresenting how the loan would be used, claiming that the funds would go toward retaining workers; maintaining payroll; or making mortgage interest, lease, and utility payments, as specified under PPP rules.

This case was investigated by our office, the FBI, and the SBA OIG. It was prosecuted by the U.S. Attorney's Office for the Northern District of Oklahoma.

Oklahoma Residents Pleaded Guilty, Sentenced to Prison, for Attempted $5.4 Million PPP Fraud

Three individuals in Oklahoma pleaded guilty to charges including bank fraud, aggravated identity theft, and false statements to a financial institution for allegedly conspiring to fraudulently obtain over $5.4 million in PPP loans. Ibanga Etuk was sentenced to 4 years in prison, was ordered to pay $168,000 in restitution, and will be removed from the United States following his sentencing. His wife, Teosha Etuk, was sentenced to 1 year and 1 day in prison and ordered to pay $150,000 in restitution. Adewale Matthew Abel is awaiting sentencing. Olusola Ojo, also implicated in the fraud, is awaiting trial after being charged with bank fraud, bank fraud conspiracy, and aggravated identity theft, as reported in our previous semiannual report to Congress; 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 Etuks and Ojo allegedly created 12 fictitious business entities to fraudulently apply for about 22 PPP loans using false information about payroll spending, number of employees, taxes paid, details of business ownership, and their relationships with one another. All four defendants submitted multiple applications for the same businesses to more than 12 banks without disclosing to those banks that they were submitting duplicative applications. They conspired to obtain over $5.4 million in loans and received close to $1 million from the banks.

This case was investigated by our office, the FBI, and the SBA OIG. It is being prosecuted by the U.S. Attorney's Office for the Northern District of Oklahoma.

Oklahoma Resident Pleaded Guilty After Fraudulently Applying for PPP Loans

Adam Winston James of Oklahoma pleaded guilty to aggravated identity theft in a scheme to defraud Regent Bank when applying for a PPP loan.

James applied for a PPP loan on behalf of Velocity Innovations LLC, a company he claimed to own and operate. As part of the application, he used the identities of at least seven people without their knowledge, fraudulently claiming that those individuals were employees of Velocity Innovations LLC. James received $125,900 from Regent Bank as a result of the scheme.

This case was investigated by our office, the FBI, and the SBA OIG. It was prosecuted by the U.S. Attorney's Office for the Northern District of Oklahoma.

Two California Siblings Pleaded Guilty to Separate Pandemic Relief Fraud Schemes Netting Over $2 million

Caesar Oskan and Ester Ozkar, siblings from California, pleaded guilty to making false statements to a financial institution in separate schemes to defraud the federal government of pandemic relief funds.

The siblings each submitted fraudulent applications to multiple banks to obtain about $2.2 million in PPP loans and Economic Injury Disaster Loans. Oskan admitted that he submitted 27 fraudulent applications, backdating documents to reflect earlier creation dates for the entities so that the entities could qualify for the loans. He further created fake IRS tax documents that contained false statements about the number of employees, payroll costs, and wages paid. Separately, Ozkar admitted that he submitted 14 fraudulent applications using the same methods.

This case was investigated by our office, the FBI, the IRS CI, the U.S. Treasury Inspector General for Tax Administration, the SBA OIG, and the U.S. Secret Service. It is being prosecuted by the U.S. Attorney's Office for the Northern District of California.

New York and Florida Resident Charged in $3.8 Million PPP Fraud Scheme

Gregory J. Blotnick, a dual New York and Florida resident, was charged with eight counts of wire fraud and six counts of money laundering for his alleged role in fraudulently obtaining $3.8 million in PPP loans. The fact that a defendant has been charged with a crime is merely an accusation, and a defendant is presumed innocent until and unless proven guilty.

Blotnick allegedly submitted eight fraudulent PPP loan applications to several lenders on behalf of seven purported businesses. The applications contained fraudulent representations, including bogus federal tax returns for entities with no history of wages paid during the relevant time period. Blotnick also fabricated the existence of employees listed in purported payroll expense sheets submitted to the various financial institutions. Based on these alleged misrepresentations, the lenders approved Blotnick's PPP loan applications and provided his purported business with about $3.8 million in loans. Blotnick then transferred most of the proceeds into a brokerage account and lost most of the money in stock trading.

The case was investigated by our office, the FDIC OIG, the Federal Housing Finance Agency OIG, the IRS CI, and the U.S. Social Security Administration OIG. It is being prosecuted by the U.S. Attorney's Office for the District of New Jersey.

Two Texas Residents and One Oregon Resident Charged With Fraud Scheme to Obtain Over $14 Million in PPP Loans

Apocalypse Bella, Mackenzy Toussaint, and Amos Mundendi were charged with participating in a fraud scheme to obtain over $14 million in PPP loans. Bella, an Oregon resident, and Toussaint and Mundendi, both of Texas, were charged with one count of conspiracy, one count of major fraud against the United States, and one count of wire fraud and wire fraud conspiracy. 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, Bella, Toussaint, and Mundendi were involved in an extensive scheme to prepare and submit fraudulent applications to the SBA and to at least one company that processes PPP loan applications. The defendants devised and executed the scheme by conspiring with individuals who own, operate, or otherwise are affiliated with multiple businesses. They coordinated or directly submitted applications containing false information, such as the number of employees, to maximize the loan amounts. The scheme resulted in the approval of $4 million in loans to two companies in New York. However, the funds were deposited in a series of bank accounts located in the United States and elsewhere, including accounts controlled by Toussaint and Bella.

This case was investigated by our office, the FBI, the IRS CI, and the SBA OIG. It is being prosecuted by the U.S. Attorney's Office for the Southern District of New York.

Three Oklahoma Residents Charged With PPP Fraud

Aleta Necole Thomas, Pepper Jones, and Katrina West, all of Oklahoma, were charged with multiple counts of false statements to a financial institution and aggravated identity theft in a scheme to fraudulently obtain PPP loans. The fact that a defendant has been charged with a crime is merely an accusation, and a defendant is presumed innocent until and unless proven guilty.

The defendants, acting together and separately, are alleged to have fraudulently applied for and received over $795,000 in PPP loans under bogus businesses such as Lead Us Kids Home Daycare, Lead Us Kids Daycare II, Coming Correction Community Ministries, and Coming Correct Community Ministries II.

This case was investigated by our office, the FBI, the SBA OIG, and the U.S. Treasury Inspector General for Tax Administration. It is being prosecuted by the U.S. Attorney's Office for the Northern District of Oklahoma.

Bureau of Consumer Financial Protection

Title X of the Dodd-Frank Act created the Bureau to implement and enforce federal consumer financial law. The Bureau 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. Additionally, with certain exceptions, the Bureau's enforcement jurisdiction generally extends to individuals or entities that are engaging or have engaged in conduct that violates federal consumer financial law.

Our investigations concerning the Bureau's responsibilities typically involve allegations that company directors or officers provided falsified business data and financial records to the Bureau, lied to or misled examiners, or obstructed examinations in a manner that may have affected the Bureau's ability to carry out its supervisory responsibilities. Such activity may result in criminal violations, such as false statements or obstruction of examinations.

No publicly reportable developments in our Bureau-related investigations occurred during this reporting period.

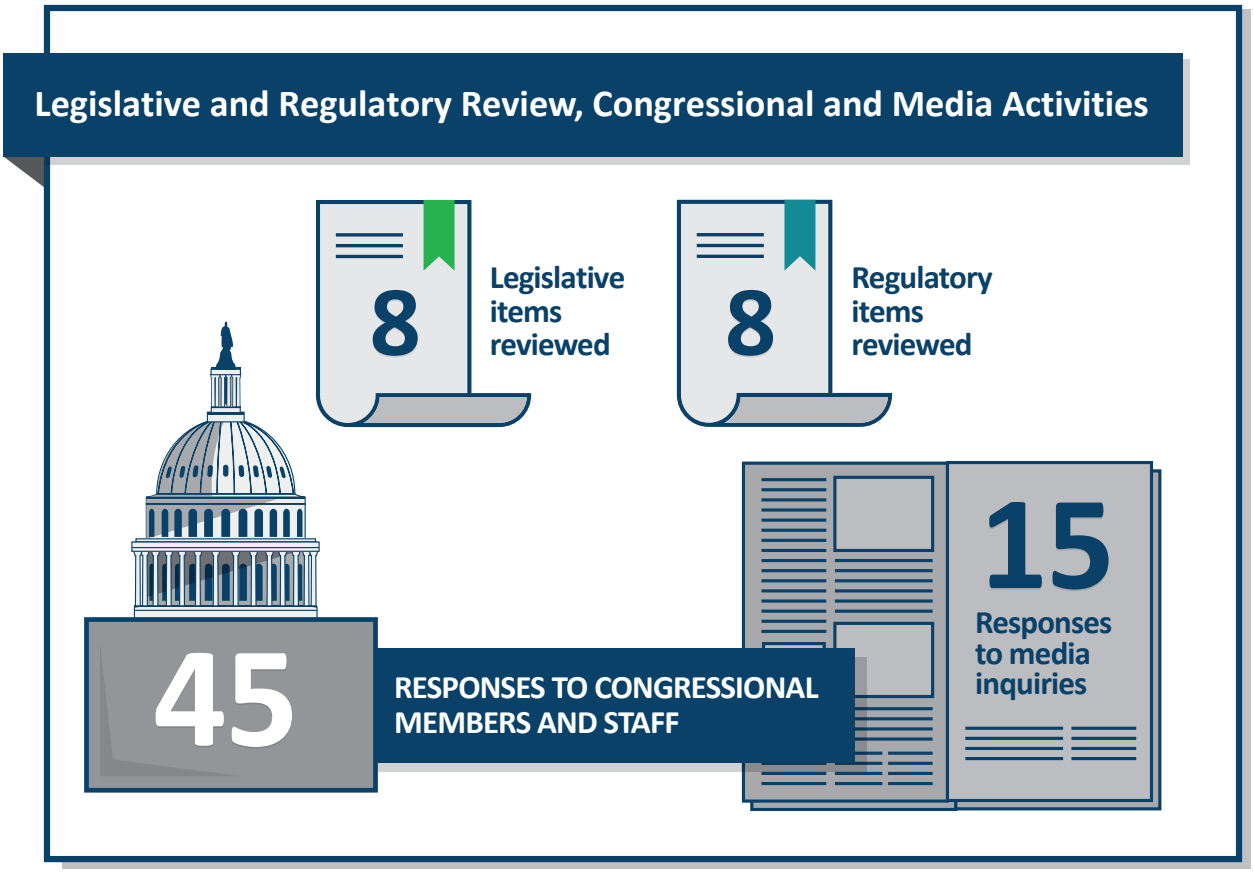
Hotline

The OIG Hotline helps people report fraud, waste, abuse, and mismanagement related to the programs or operations of the Board and the Bureau. 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 229 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 Bureau. We refer such complaints to the appropriate federal agency for evaluation and resolution.

We continue to receive many 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 Bureau'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 is the independent legal counsel to the IG and OIG staff. Legal Services provides comprehensive legal advice, research, counseling, analysis, and representation in support of our audits, investigations, inspections, and evaluations as well as other professional, management, and administrative functions. Legal Services also keeps the IG and OIG staff aware of recent legal developments that may affect us, the Board, or the Bureau.

In accordance with section 4(a)(2) of the Inspector General Act of 1978, as amended, Legal Services 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 Bureau's programs and operations. During this reporting period, Legal Services reviewed 8 legislative items and 8 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 45 responses to congressional members and staff concerning the Board and the Bureau. Additionally, we responded to 15 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 20,000 reports, detailing for fiscal year 2021 alone $54.6 billion in potential savings and over 6,000 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 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, and Inclusion Work Group. The Diversity, Equity, and Inclusion Work Group works to affirm, advance, and augment CIGIE's commitment to promote a diverse, equitable, and inclusive 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 Institutions Oversight Subcommittee.

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

Our Legal Services 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, as amended, 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 October 2020, the OIG for the National Archives and Records Administration completed a peer review of our audit organization. We received a peer review rating of *pass*.
- In August 2019, the OIG for the Tennessee Valley Authority 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.

See our website for peer review reports of our organization.

Appendix A: Statistical Tables

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

Report title	Type of report
Results of Analytical Testing of the Board's Publicly Reported Data for the Main Street Lending Program	Analytical testing
The Board's Payroll Controls Are Generally Effective	Audit
Results of Analytical Testing of the Board's Publicly Reported Data for the Secondary Market Corporate Credit Facility	Analytical testing
The Board's Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced	Evaluation
Total number of audit reports: 1 Total number of evaluation reports: 1 Total number of other reviews: 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
The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control	09/13	1	1	0	09/21	1	0
2016 Audit of the Board's Information Security Program	11/16	9	9	0	11/20	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	08/21	7	1
2017 Audit of the Board's Information Security Program	10/17	9	9	0	11/20	5	4
The Board's Organizational Governance System Can Be Strengthened	12/17	14	14	0	08/21	13	1
Security Control Review of the Board's Public Website (nonpublic)	03/18	7	7	0	06/20	4	3
Security Control Review of the Board Division of Research and Statistics' General Support System (nonpublic)	09/18	9	9	0	03/20	7	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
2018 Audit of the Board's Information Security Program	10/18	6	6	0	11/20	5	1
The Board Can Strengthen Information Technology Governance	11/18	6	6	0	06/20	3	3
The Board Can Enhance Its Internal Enforcement Action Issuance and Termination Processes by Clarifying the Processes, Addressing Inefficiencies, and Improving Transparency	09/19	6	6	0	07/21	4	2
The Board's Law Enforcement Operations Bureau Can Improve Internal Processes	09/19	6	6	0	07/21	4	2
2019 Audit of the Board's Information Security Program	10/19	6	6	0	11/20	1	5
The Board Should Finalize Guidance to Clearly Define Those Considered Senior Examiners and Subject to the Associated Postemployment Restriction	03/20	1	1	0	08/21	1	0
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	09/21	1	5

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 Certain Aspects of Its Enforcement Action Monitoring Practices	03/20	1	1	0	09/21	1	0
The Board Can Further Enhance the Design and Implementation of Its Operating Budget Process	03/20	2	2	0	07/21	2	0
The Board Can Strengthen Its Oversight of the Protective Services Unit and Improve Controls for Certain Protective Services Unit Processes	03/20	6	6	0	06/21	6	0
The Board Can Improve Its Contract Administration Processes	03/20	13	13	0	07/21	13	0
The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced	09/20	10	10	0	09/21	6	4
2020 Audit of the Board's Information Security Program	11/20	4	4	0	n.a.	0	4
The Board Economics Divisions Can Enhance Some of Their Planning Processes for Economic Analysis	02/21	6	6	0	n.a.	0	6
The Board Can Improve the Management of Its Renovation Projects	03/21	2	2	0	09/21	0	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 Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced	09/21	3	3	0	n.a.	0	3

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

n.a. not applicable.

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

Report title	Type of report
Independent Accountants' Report on the Bureau's Fiscal Year 2020 Compliance With the Payment Integrity Information Act of 2019	Audit
The Bureau Can Improve Its Controls for Issuing and Managing Interagency Agreements	Audit
Evaluation of the Bureau's Implementation of Splunk	Evaluation
Total number of audit reports: 2 Total number of evaluation reports: 1	

Table A-4. OIG Reports to the Bureau 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	11/20	2	1
2017 Audit of the CFPB's Information Security Program	10/17	7	7	0	11/20	5	2
The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data	01/18	11	11	0	09/21	9	2
Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program	02/18	2	2	0	01/20	1	1
2018 Audit of the Bureau's Information Security Program	10/18	4	4	0	11/20	1	3
Technical Testing Results for the Bureau's SQL Server Environment (nonpublic)	05/19	5	5	0	05/21	4	1
The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP	07/19	3	3	0	03/21	0	3
2019 Audit of the Bureau's Information Security Program	10/19	7	7	0	11/20	3	4
Testing Results for the Bureau's Plan of Action and Milestones Process	04/20	2	2	0	03/21	0	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
Technical Testing Results for the Bureau's Legal Enclave (nonpublic)	07/20	4	4	0	03/21	0	4
Results of Scoping and Suspension of the Evaluation of the Bureau's Personnel Security Program	08/20	3	3	0	09/21	2	1
2020 Audit of the Bureau's Information Security Program	11/20	1	1	0	n.a.	0	1
The Bureau Can Strengthen Its Hiring Practices and Can Continue Its Efforts to Cultivate a Diverse Workforce	03/21	10	10	0	n.a.	0	10
The Bureau Can Improve Its Controls for Issuing and Managing Interagency Agreements	07/21	6	6	0	n.a.	0	6
Evaluation of the Bureau's Implementation of Splunk (nonpublic)	09/21	4	4	0	n.a.	0	4

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

n.a. not applicable.

Table A-5. Audit, Inspection, and Evaluation Reports Issued to the Board and the Bureau 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 Bureau 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, inspection, 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	125
Investigations opened during the reporting period	39
Investigations closed during the reporting period	18
Investigations open at end of the reporting period	146
Investigative results for the reporting period	
Persons referred to DOJ prosecutors	23
Persons referred to state/local prosecutors	1
Declinations received	12
Joint investigations	127
Reports of investigation issued	1
Oral and/or written reprimands	0
Terminations of employment	0
Arrests	15
Suspensions	0
Debarments	0
Prohibitions from banking industry	3
Indictments	15
Criminal informations	9
Criminal complaints	4
Convictions	27
Civil actions	$0

See notes at end of table.

Investigative actions	Number or dollar value[a]
Administrative monetary recoveries and reimbursements	$0
Civil judgments	$0
Criminal fines, restitution, and special assessments	$6,544,200
Forfeiture	$0

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	30
Complaints received during reporting period	229
Total complaints for reporting period	259
Complaints resolved during reporting period	239
Complaints pending	20

Appendix B: Inspector General Empowerment Act of 2016 Requirements

The Inspector General Empowerment Act of 2016 amended section 5 of the Inspector General Act of 1978 by adding reporting requirements that must be included in OIG semiannual reports to Congress. These additional reporting requirements include summaries of certain audits, inspections, and evaluations; investigative statistics; summaries of investigations of senior government employees and the name of the senior government official, if already made public by the OIG; whistleblower retaliation statistics; summaries of interference with OIG independence; and summaries of closed audits, evaluations, inspections, and investigations that were not publicly disclosed. Our response to these requirements is below.

Summaries of each audit, inspection, and evaluation report issued to the Board or the Bureau for which no agency comment was returned within 60 days of receiving the report or for which no management decision has been made by the end of the reporting period.

- We have no such instances to report.

Summaries of each audit, inspection, and evaluation report issued to the Board or the Bureau for which there are outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.

- 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 that involves a senior government employee in which allegations of misconduct were substantiated, 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 instances 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.

A detailed description of any attempt by the Board or the Bureau to interfere with the independence of the OIG, including (1) through budget constraints designed to limit OIG capabilities and (2) incidents when the 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.

- We have no such attempts 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 closed our audit of the Board's compliance with the Open, Public, Electronic and Necessary (OPEN) Government Data Act in the final weeks of the reporting period and disclosed its closure in our October 1, 2021, *Work Plan*. OMB is responsible for providing federal agencies with guidance to facilitate the implementation of the OPEN Government Data Act's requirements. We planned to use the OMB implementation guidance to assess the Board's compliance with the act. During scoping, we learned that a majority of the OPEN Government Data Act requirements that are applicable to the Board are covered under OMB's phase 2 implementation guidance, which has not been issued. The lack of phase 2 guidance limits our ability to fully assess and determine whether the Board is in compliance with the act.

Appendix C: Summaries of Reports With Outstanding Unimplemented Recommendations

The Inspector General Empowerment Act of 2016 requires that we provide summaries of each audit, inspection, and evaluation report issued to the Board or the Bureau for which there are outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.

Board of Governors of the Federal Reserve System

Table C-1. Reports to the Board With Unimplemented Recommendations, by Calendar Year

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2016	1	1
2017	3	6
2018	4	9
2019	3	9
2020	3	13
2021 [a]	3	11

Note: Because the Board is primarily a regulatory and policymaking agency, 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.

a. Through September 30, 2021.

2016 Audit of the Board's Information Security Program

2016-IT-B-013 **November 10, 2016**

Total number of recommendations: 9
Recommendations open: 1

In accordance with FISMA requirements, we reviewed the Board's information security program. Specifically, we evaluated the effectiveness of the Board's (1) security controls and techniques and (2) information security policies, procedures, and practices.

We found that the Board had taken several steps to mature its information security program to ensure that the program was consistent with FISMA requirements. However, we identified several improvements needed in the Board's information security program in the areas of risk management, identity and access management, security and privacy training, and incident response. Specifically, we found that the Board could have strengthened its risk management program by ensuring that Board divisions were consistently implementing the organization's risk management processes related to security controls assessment, security planning, and authorization. In addition, we found instances of Board sensitive information that was not appropriately restricted within the organization's enterprisewide collaboration tool. We also noted that the Board had not evaluated the effectiveness of its security and privacy awareness training program in 2016. Finally, we found that the Board could have strengthened its incident response capabilities.

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

We assessed (1) the Board's current cybersecurity oversight approach and governance structure, (2) the current examination practices for financial market utilities and multiregional data processing servicer (MDPS) firms for which the Board has oversight responsibilities, and (3) the Board's ongoing initiative for the future state of cybersecurity oversight. We found that the Division of Supervision and Regulation could improve the oversight of MDPS firms by (1) enforcing a reporting requirement in the Bank Service Company Act, (2) considering the implementation of an enhanced governance structure for these firms, (3) providing additional guidance on the supervisory expectations for these firms, and (4) ensuring that the division's intelligence and incident management function is aware of the technologies used by MDPS firms. We also identified opportunities to improve the recruiting, retention, tracking, and succession

planning of cybersecurity resources, as well as opportunities to enhance the internal communications about cybersecurity-related risks.

2017 Audit of the Board's Information Security Program

2017-IT-B-018 **October 31, 2017**

Total number of recommendations: 9
Recommendations open: 4

We evaluated the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. We followed U.S. Department of Homeland Security guidelines and evaluated the information security program's maturity level (from a low of 1 to a high of 5) across several areas.

The Board's information security program is operating at a level-3 maturity (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. Further, it has implemented an effective security training program that includes phishing exercises and associated performance metrics. However, the Board can mature its information security program to ensure that it is effective, or operating at level-4 maturity (*managed and measurable*). The lack of an agencywide risk-management governance structure and strategy as well as decentralized IT services result in an incomplete view of the risks affecting the security posture of the Board and impede its ability to implement an effective information security program. In addition, several security processes, such as configuration management and information security continuous monitoring, were not effectively implemented agencywide.

The Board's Organizational Governance System Can Be Strengthened

2017-FMIC-B-020 **December 11, 2017**

Total number of recommendations: 14
Recommendations open: 1

An organization's governance system determines how decisionmaking, accountability, controls, and behaviors help accomplish its objectives. Our evaluation (1) describes the current state of the Board's organizational governance structures and processes and (2) assesses the extent to which these structures and processes align with those of other relevant institutions and with governance principles.

The Board's core organizational governance structure aligns with benchmark institutions and selected governance principles, as does its public disclosure of governance documents. Nonetheless, the Board can strengthen its governance system by clarifying and regularly reviewing purposes, roles and responsibilities, authorities, and working procedures of its standing committees; enhancing the

orientation program for new governors and reviewing and formalizing the process for selecting dedicated advisors; setting clearer communication expectations and exploring additional opportunities for information sharing among governors; reviewing, communicating, and reinforcing the Board of Governors' expectations of the chief operating officer and the heads of the administrative functions; and establishing and documenting the Executive Committee's mission, protocols, and authorities.

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

2018-IT-B-008R **March 21, 2018**

Total number of recommendations: 7
Recommendations open: 3

We evaluated the adequacy of select information security controls for protecting the Board's public website from compromise. Overall, the information security controls that we tested were adequately designed and implemented. However, we identified opportunities for improvement in the areas of configuration management and risk management.

Security Control Review of the Board Division of Research and Statistics' General Support System (nonpublic)

2018-IT-B-015R **September 26, 2018**

Total number of recommendations: 9
Recommendations open: 2

We evaluated the effectiveness of select security controls and techniques for the Division of Research and Statistics' general support system, as well as the system's compliance with FISMA and Board information security policies, procedures, standards, and guidelines.

Overall, we found that the division has taken steps to implement information security controls for its general support system in accordance with FISMA and Board information security policies, procedures, standards, and guidelines. We identified opportunities for improvement in the implementation of the Board's information system security life cycle for the division's general support system to ensure that information security controls are effectively implemented, assessed, authorized, and monitored.

2018 Audit of the Board's Information Security Program

2018-IT-B-017 **October 31, 2018**

Total number of recommendations: 6
Recommendations open: 1

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Board. We evaluated the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Board's information security program is operating at a level-4 (*managed and measurable*) maturity, which indicates an overall effective level of security. The Board has opportunities to mature its information security program in FISMA domains across all five security functions outlined in the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

The Board Can Strengthen Information Technology Governance

2018-IT-B-020 **November 5, 2018**

Total number of recommendations: 6
Recommendations open: 3

The efficiency and effectiveness of the Board's agencywide information security program is contingent on enterprisewide visibility into IT operations. As part of our requirements under FISMA, we assessed whether the Board's current organizational structure and authorities support its IT needs—specifically, the organizational structure and authorities associated with security, privacy, capital planning, budgeting, and acquisition.

Overall, we found that certain aspects of the Board's organizational structure and authorities could inhibit the Board's achievement of its strategic objectives regarding technology as well as its achievement of an effective FISMA maturity rating. Although the Board has IT governance mechanisms in place, we found opportunities for improvement in the areas of security, budgeting, procurement, and capital planning.

The Board Can Enhance Its Internal Enforcement Action Issuance and Termination Processes by Clarifying the Processes, Addressing Inefficiencies, and Improving Transparency

2019-SR-B-013 **September 25, 2019**

Total number of recommendations: 6
Recommendations open: 2

We assessed the efficiency and effectiveness of the Board's and the Reserve Banks' enforcement action issuance and termination processes and practices.

We found that the Board and the Reserve Banks have implemented some effective practices to support the enforcement action issuance and termination processes; however, we identified opportunities for the Board to enhance these processes. Specifically, we found that the Board can clarify certain aspects of these internal processes, such as the steps in these processes, the Board stakeholders' roles and responsibilities, and the Board members' involvement. In addition, we found that the Board can (1) improve the timeliness and efficiency of its enforcement action issuance and termination processes and (2) increase transparency with respect to the status of ongoing enforcement actions.

The Board's Law Enforcement Operations Bureau Can Improve Internal Processes

2019-MO-B-014 **September 30, 2019**

Total number of recommendations: 6
Recommendations open: 2

We assessed whether the control environment in the Law Enforcement Unit's (LEU) Operations Bureau is operating effectively to support the LEU's mission as well as components of the Division of Management's strategic goals.

We found that the LEU's Operations Bureau can improve standards and processes associated with its control environment to better support the LEU's mission. Specifically, we found that the LEU did not document the roles, responsibilities, training qualifications, and reporting requirements after modifying its process for internal reviews. We also found that the LEU can better communicate its decisions and the rationale for changes affecting the Operations Bureau and can take further action to improve communication generally. Additionally, the LEU can better capitalize on professional development opportunities for officers and new supervisors. Lastly, the LEU should also strengthen its processes for determining shift and post assignments.

2019 Audit of the Board's Information Security Program

2019-IT-B-016 **October 31, 2019**

Total number of recommendations: 6
Recommendations open: 5

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Board. We evaluated the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Board's information security program is operating effectively at level 4 (*managed and measurable*). The Board has opportunities to mature its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

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: 5

We assessed the effectiveness of the Board's oversight of its designated financial market utility (DFMU) supervision program.

The Board has implemented practices and processes (1) to ensure governance over the DFMU supervision program, (2) to collaborate with other supervisory agencies in accordance with authorities provided in the Dodd-Frank Act, and (3) to conduct reviews of material changes filed by DFMUs that meet the Board's responsibilities under title VIII of the Dodd-Frank Act. However, we identified opportunities for the Board to enhance these practices and processes. Specifically, the Board should publish certain internal delegations of authority and define certain roles and responsibilities within the DFMU supervision program. The Board also can enhance its processes for collaborating with other supervisory agencies. Lastly, the Board can better prepare for emergency changes filed by the DFMUs for which it is the supervisory agency.

The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced

2020-SR-B-019 **September 30, 2020**

Total number of recommendations: 10
Recommendations open: 4

We assessed the effectiveness of the Board's cybersecurity supervision approach for Large Institution Supervision Coordinating Committee (LISCC) firms—the largest, most systemically important domestic and foreign financial institutions supervised by the Board.

The Board's approach to cybersecurity supervision of LISCC firms continues to evolve and can be enhanced. The Board can strengthen its governance of LISCC firm cybersecurity supervision by clarifying the roles and responsibilities of the groups involved in supervision and planning activities and better defining how cybersecurity supervisory activities inform relevant ratings. The Board can also enhance its approach to cybersecurity training to ensure examiners keep their skills up to date. Additionally, the Board can improve its guidance and training for reporting cybersecurity events.

2020 Audit of the Board's Information Security Program

2020-IT-B-020 **November 2, 2020**

Total number of recommendations: 4
Recommendations open: 4

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Board. We evaluated the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Board's information security program is operating effectively at level 4 (*managed and measurable*). The Board has opportunities to mature its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

The Board Economics Divisions Can Enhance Some of Their Planning Processes for Economic Analysis

2021-MO-B-001 **February 24, 2021**

Total number of recommendations: 6
Recommendations open: 6

The Board has four divisions that conduct economic analysis and independent research that support the Board's monetary policy goals established by Congress: maximum employment, stable prices, and moderate long-term interest rates. We evaluated the effectiveness of these divisions' planning processes.

The economics divisions can enhance some of their planning processes for their economic analysis activities by considering additional practices to improve transparency, communication, and monitoring. In addition, the economics divisions can benefit from developing a more structured approach to sharing processes and supporting practices with each other, as well as considering the value of an external evaluation of certain activities to support continuous improvement efforts.

The Board Can Improve the Management of Its Renovation Projects

2021-FMIC-B-004 **March 10, 2021**

Total number of recommendations: 2
Recommendations open: 2

The Board is planning and managing major renovations of all four buildings it owns. Its total renovation budget, as of June 2020, was $2.1 billion. We assessed the Board's process for planning and managing multiple renovation projects as well as procuring services under various renovation-related contracts.

The Board can improve its planning and managing of ongoing renovation projects as well as future large, complex, multidivision initiatives by developing a policy that outlines the required project planning components, including project governance; ensuring that contractors submit required progress reports and meeting minutes; and ensuring that the project team maintains a current approved schedule and documents any significant changes to the schedule in the project file.

The Board complied with its policies and procedures for conducting market research and awarding competitive contracts to bidders, which also aligned with industry and government practices.

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: 3

See the summary in the body of this report.

Bureau of Consumer Financial Protection

Table C-2. Reports to the Bureau With Unimplemented Recommendations, by Calendar Year

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2014	1	1
2015	0	0
2016	0	0
2017	1	2
2018	3	6
2019	3	8
2020	4	8
2021[a]	3	20

Note: Because the Bureau is primarily a regulatory and policymaking agency, 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.

a. Through September 30, 2021.

2014 Audit of the CFPB's Information Security Program

2014-IT-C-020 **November 14, 2014**

Total number of recommendations: 3
Recommendations open: 1

We found that the Bureau continued to take steps to mature its information security program and to ensure that it was consistent with the requirements of FISMA. Overall, we found that the Bureau's information security program was consistent with 9 of 11 information security areas. Although corrective actions were underway, further improvements were needed in security training and contingency planning. We found that the Bureau's information security program was generally consistent with the requirements for continuous monitoring, configuration management, and incident response; however, we identified opportunities to strengthen these areas through automation and centralization.

2017 Audit of the CFPB's Information Security Program

2017-IT-C-019 **October 31, 2017**

Total number of recommendations: 7
Recommendations open: 2

We evaluated the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. We followed U.S. Department of Homeland Security guidelines and evaluated the information security program's maturity level (from a low of 1 to a high of 5) across several areas.

The Bureau's overall information security program is operating at a level-3 maturity (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. However, the Bureau can mature its information security program to ensure that it is effective, or operating at level-4 maturity (*managed and measurable*). Specifically, the agency can strengthen its ongoing efforts to establish an ERM program by defining a risk appetite statement and associated risk tolerance levels and developing and maintaining an agencywide risk profile. It can also improve configuration monitoring processes for agency databases and applications, multifactor authentication for the internal network and systems, assessments of the effectiveness of security awareness and training activities, and incident response and contingency planning capabilities.

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: 2

The Bureau's offboarding process for employees and contractors covers, among other things, the return of property, records management, and ethics counseling on conflicts of interest. We determined whether the agency's controls over these aspects of offboarding effectively mitigate reputational and security risks.

Although the Bureau has offboarding controls related to conflicts of interest for executive employees' postemployment restrictions, the Bureau has opportunities to strengthen controls in other areas. Specifically, the agency did not always deactivate badges timely or record the status of badges for separating employees and contractors, did not consistently maintain IT asset documentation, did not always conduct records briefings, did not always maintain nondisclosure agreements for contractors, and did not accurately maintain certain separation and contractor data.

Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program

2018-IT-C-003 **February 14, 2018**

Total number of recommendations: 2
Recommendations open: 1

We contracted with a third party to conduct a performance audit of the Bureau's privacy program and its implementation.

Overall, the contractor found that the Bureau has substantially developed, documented, and implemented a privacy program that addresses applicable federal privacy requirements and security risks related to collecting, processing, handling, storing, and disseminating sensitive privacy data. Further, the contractor noted that the Bureau has documented privacy policies and procedures covering a wide range of topics, including privacy roles and responsibilities, privacy impact assessment and system of records notice management, training, breach notification and response, and monitoring and auditing.

2018 Audit of the Bureau's Information Security Program

2018-IT-C-018 **October 31, 2018**

Total number of recommendations: 4
Recommendations open: 3

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Bureau. We evaluated the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Bureau's information security program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level. The Bureau also has opportunities to mature its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program is effective.

Technical Testing Results for the Bureau's SQL Server Environment (nonpublic)

2019-IT-C-007R **May 22, 2019**

Total number of recommendations: 5
Recommendations open: 1

We identified that the security configurations for select SQL Server instances and databases were not aligned with established baselines and that significant weaknesses exist in controls for account management and configuration management. We believe that these continuing weaknesses heighten the risk of a breach of sensitive data maintained in the Bureau's SQL Server environment.

The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP

2019-IT-C-009 **July 17, 2019**

Total number of recommendations: 3
Recommendations open: 3

To meet our FISMA requirements, we determined whether the Bureau has implemented an effective life cycle process for deploying and managing Federal Risk and Authorization Management Program (FedRAMP) cloud systems, including ensuring that effective security controls are implemented.

We found that the Bureau has developed a life cycle process for deploying and managing security risks for Bureau systems, which include the FedRAMP cloud systems it uses. However, we found that the

process is not yet effective in ensuring that (1) risks are comprehensively assessed prior to deploying new cloud systems, (2) continuous monitoring is performed to identify security control weaknesses after deployment, and (3) electronic media sanitization renders sensitive Bureau data unrecoverable when cloud systems are decommissioned.

2019 Audit of the Bureau's Information Security Program

2019-IT-C-015 **October 31, 2019**

Total number of recommendations: 7
Recommendations open: 4

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Bureau. We evaluated the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Bureau's information security program is operating effectively at level 4 (*managed and measurable*). We identified opportunities for the Bureau to strengthen its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

Testing Results for the Bureau's Plan of Action and Milestones Process

2020-IT-C-014 **April 29, 2020**

Total number of recommendations: 2
Recommendations open: 2

As part of our 2019 audit of the Bureau's information security program, which we performed to meet FISMA requirements, we tested the Bureau's plan of action and milestones (POA&M) process, which the agency uses to document and remediate information security weaknesses.

We found that costs associated with remediating cybersecurity weaknesses listed in POA&Ms were not accurately accounted for. We also identified instances in which the status of cybersecurity weaknesses included in the Bureau's automated solution for POA&M management was inaccurate.

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

2020-IT-C-017R **July 22, 2020**

Total number of recommendations: 4
Recommendations open: 4

As part of our 2019 audit of the Bureau's information security program, which we performed to meet FISMA requirements, we tested technical controls for the agency's Legal Enclave.

We found a significant weakness on a device that controls access to the environment housing the Legal Enclave, resulting in several security vulnerabilities. Further, the Bureau had not appropriately tested contingency planning activities for the device. In addition, we identified several security misconfigurations and security weaknesses for technologies in the Legal Enclave, which increase the risk of unauthorized data access and system misuse. Although the Bureau was aware of several of these issues, it had not taken timely action to mitigate the risks; the Bureau had accepted specific risks related to certain vulnerabilities in the Legal Enclave but had not formally documented its rationale for these decisions.

Results of Scoping and Suspension of the Evaluation of the Bureau's Personnel Security Program

2020-MO-C-018 **August 17, 2020**

Total number of recommendations: 3
Recommendations open: 1

We initiated an evaluation to assess the efficiency and effectiveness of the Bureau's personnel security program. However, the Bureau recently completed an internal review of the program, which identified other areas for improvement, and the U.S. Office of Personnel Management launched a separate review in March 2020. Because the Bureau needs time to fully address the results from these additional reviews, we suspended our evaluation.

We found that the Personnel Security Office does not have measurable objectives to evaluate its performance related to reducing its adjudication backlog, nor does it have a plan with measurable objectives to manage the background investigation process going forward. In addition, we found that the Personnel Security Office does not have processes to reconcile its personnel security data.

2020 Audit of the Bureau's Information Security Program

2020-IT-C-021 **November 2, 2020**

Total number of recommendations: 1
Recommendations open: 1

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Bureau. We evaluated the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Bureau's information security program is operating effectively at level 4 (*managed and measurable*). We identified opportunities for the Bureau to strengthen its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

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: 10

The Bureau's human capital processes are the means to develop a talented, diverse, inclusive, and engaged workforce to support the agency's mission. We assessed the Bureau's compliance with its policies and procedures related to selected types of hiring, promotions, and other internal placements and identified any potential effects of those hiring practices on its workforce diversity.

The Bureau can strengthen its hiring processes and reduce risks associated with assessing applicants, documenting hiring actions, tracking hiring actions, and reporting excepted service positions. In addition, the Bureau's racial and ethnic diversity has increased as a percentage of its overall workforce in recent years, and we identified several practices that may help the agency continue to increase its workforce diversity.

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: 6

See the summary in the body of this report.

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

2021-IT-C-010R **September 8, 2021**

Total number of recommendations: 4
Recommendations open: 4

See the summary in the body of this report.

Abbreviations

CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CFPB	Consumer Financial Protection Bureau
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
DATA Act	Digital Accountability and Transparency Act of 2014
DE&I	diversity, equity, and inclusion
DFMU	designated financial market utility
DOJ	U.S. Department of Justice
ERM	enterprise risk management
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FedRAMP	Federal Risk and Authorization Management Program
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act of 2014
FRB New York	Federal Reserve Bank of New York
IAA	interagency agreement
IG	inspector general
IRS	Internal Revenue Service
IRS CI	Internal Revenue Service Criminal Investigation
IT	information technology
LEU	Law Enforcement Unit
LISCC	Large Institution Supervision Coordinating Committee
MDPS	multiregional data processing servicer
MSLP	Main Street Lending Program
OMB	Office of Management and Budget
OPEN	Open, Public, Electronic and Necessary
PIIA	Payment Integrity Information Act of 2019
POA&M	plan of action and milestones

PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
SBA	U.S. Small Business Administration
SMCCF	Secondary Market Corporate Credit Facility

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551
Phone: 202-973-5000 | Fax: 202-973-5044

OIG Hotline

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

800-827-3340