Office of Inspector General

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

Semiannual Report to Congress

October 1, 2021–March 31, 2022

OIG

Semiannual Report to Congress

October 1, 2021–March 31, 2022

Office of Inspector General

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

Message From the Inspector General

We recently marked 2 years since the initial COVID-19 pandemic shutdown, and our nation is approaching the tragic milestone of 1 million American lives lost. The human cost of this pandemic—the illness, trauma, grief, and other disruptions to our lives—has been virtually unthinkable. The effects of the pandemic continue to be felt throughout the economy, including through supply chain challenges, constraints in the labor supply, and inflation.

We continue to actively monitor the Board of Governors of the Federal Reserve System's pandemic-related lending programs. In a recent report, we assessed the Board's processes for collecting, aggregating, validating, and reporting data related to its Coronavirus Aid, Relief, and Economic Security (CARES) Act lending programs and found that the Board meets its CARES Act reporting requirements, voluntarily reports transaction-specific data, and publishes complete and accurate data. In addition, in an ongoing evaluation, we are assessing third-party cybersecurity risk management processes for vendors supporting the Main Street Lending Program and the Secondary Market Corporate Credit Facility. We are also conducting fieldwork in support of an evaluation to assess the Federal Reserve System's vendor selection and management processes related to the Federal Reserve Bank of New York's emergency lending programs. Finally, an evaluation of the System's loan purchase and administration for the Main Street Lending Program is in the planning stage.

Our Office of Investigations is investigating numerous cases of fraud related to the emergency lending programs established in response to the pandemic. In a recently indicted case, for example, a chief executive officer and primary owner of a company allegedly used false representations and documents to fraudulently obtain approval for his company to be a nonbank Paycheck Protection Program (PPP) lender. The indictment alleges that his company then obtained about $932 million in capital and issued $823 million in PPP loans, earning more than $71 million in lender fees. According to the indictment, he also obtained a PPP loan of over $283,000 for his company through alleged false statements about employees and wages using documents containing the alleged forged signature of the company's tax preparer.

Overall, our Office of Investigations closed 28 investigations and resolved 84 hotline complaints. Our work resulted in 23 referrals for criminal prosecution; 24 arrests; 20 indictments; 16 criminal informations; 20 convictions; and over $22 million in criminal fines, restitution, and special assessments.

I continue to serve on the Pandemic Response Accountability Committee (PRAC), which coordinates inspector general community oversight of the federal government's COVID-19 pandemic response efforts, and I also continue to participate in the PRAC Financial Sector Workgroup. In addition, we are working directly with the PRAC fraud task force to help protect the integrity of pandemic relief programs.

Great strides have been made over the past 2 years in COVID-19 detection, vaccines, and treatment, and many organizations, including our office, the Board, and the Bureau of Consumer Financial Protection, have returned to the office or are planning a return to the office. We have initiated evaluations of the Board's and the Bureau's return-to-office plans to examine specific controls related to vaccination requirements for visitors and contractors; building access protocols for employees, visitors, and contractors; facility cleaning and air filtration standards; and social distancing protocols and signage.

In other work during this reporting period, we assessed the Board's and the Federal Reserve Banks' consumer compliance examination and enforcement action issuance processes for unfair or deceptive acts or practices and fair lending matters, and we found that the Board can improve the efficiency and effectiveness of certain aspects of these processes. We also identified ways the Board can enhance its personnel security program, such as by defining specific objectives to measure program performance. We found that the Board's contract modification process related to renovation projects is generally effective.

We also evaluated the Bureau Division of Supervision, Enforcement and Fair Lending's (SEFL) approach to supervising nondepository institutions, such as mortgage lenders, debt collectors, and student loan servicers, and found that the Bureau can further enhance certain aspects of its approach to supervising these institutions. In addition, we conducted an evaluation of the design and effectiveness of SEFL's internal Quality Management Program for supervision activities.

Information security continues to be a priority. In a recent evaluation, we considered ways the Board can strengthen inventory and cybersecurity life cycle processes for cloud systems. We also published our annual information security audit for each agency we oversee, as required by the Federal Information Security Modernization Act of 2014.

Another area of interest is the relationship between financial institutions, financial stability, and climate change. Although assessing and managing climate-related risks presents several challenges, System supervisors are responsible for ensuring that supervised institutions operate in a safe and sound manner and can continue to provide financial services to their customers in the face of all types of risk, including those related to climate change. We are beginning work to evaluate the Board's supervisory approaches for climate risks to financial institutions.

These are uncertain times—not only because of the pandemic and its effects on the economy, but also given recent geopolitical events. Amid this uncertainty, I feel deeply grateful for the Office of Inspector General staff. None of us could have known that the pandemic would last this long or be this deadly and disruptive, yet they have handled the evolving challenges with creativity, resilience, and steadfast determination. I'm hopeful that we will have opportunities for in-person collaboration in the coming months, and I'm confident that no matter where we are located, we will continue to fulfill our mission of providing robust independent oversight.

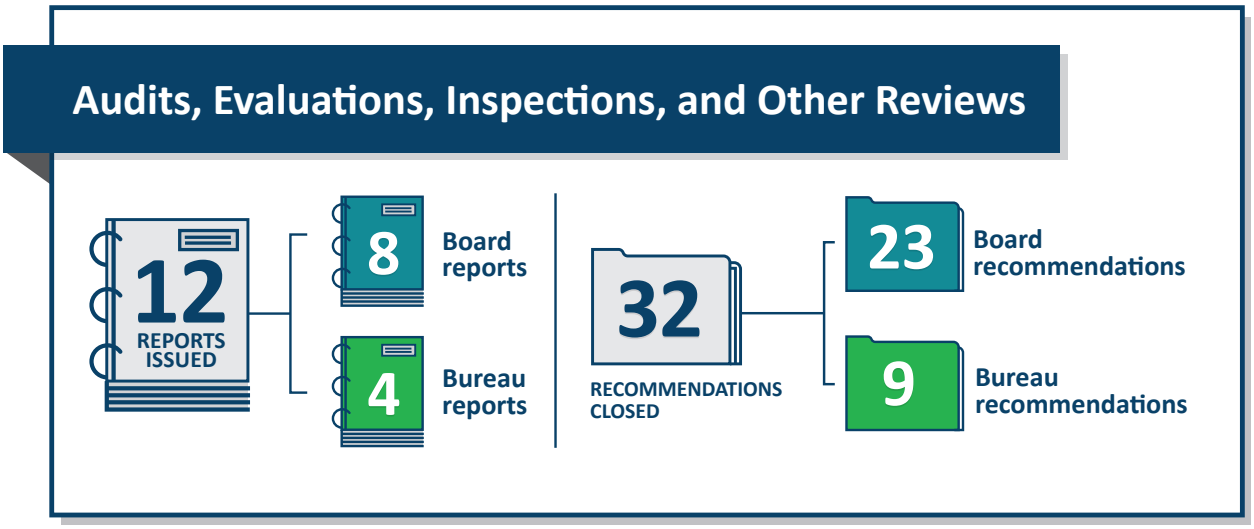
Sincerely,

Mark Bialek
Inspector General
April 29, 2022

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 Consumer Compliance Examination and Enforcement Action Issuance Processes

The Board can enhance the efficiency and effectiveness of its and the Federal Reserve Banks' consumer compliance examination and enforcement action issuance processes for unfair or deceptive acts or practices (UDAP) and fair lending matters.

The Board's Information Security Program

The Board's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. The Board has opportunities to mature its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

The Bureau's Information Security Program

The Bureau's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. The Bureau has opportunities 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's Approach to Supervising Nondepository Institutions

The Bureau applies consistent examination procedures to depository and nondepository institutions and uses the same approach to follow up on Matters Requiring Attention but can further improve its approach to supervising nondepository institutions.

The Board's Personnel Security Program

The Board can enhance its personnel security program and strengthen processes and controls for completing background investigations and granting security clearances for employees and contractors.

The Board's Coronavirus Aid, Relief, and Economic Security Act Lending Program Data Processes

The Board meets its Coronavirus Aid, Relief, and Economic Security (CARES) Act reporting requirements, voluntarily reports transaction-specific data, and generally publishes complete and accurate data, but can enhance transparency and reduce the potential to report immaterial inaccuracies in the transaction-specific data.

Many of our investigations during this semiannual reporting period concern fraud related to the Federal Reserve's pandemic response efforts, including the Main Street Lending Program (MSLP), which supported lending to small and medium-sized for-profit and nonprofit organizations in sound financial condition prior to the COVID-19 pandemic, and the Paycheck Protection Program Liquidity Facility, which extended credit to eligible financial institutions and took Paycheck Protection Program (PPP) loans guaranteed by the U.S. Small Business Administration (SBA) as collateral. In addition, our office also conducted investigations in support of our membership on the Pandemic Response Accountability Committee (PRAC).

Chief Executive Officer of PPP Lender MBE Capital Partners Charged in New York in Nearly $1 Billion PPP Loan and Lender Fraud

Rafael Martinez, chief executive officer (CEO) and primary owner of MBE Capital Partners, was charged with numerous crimes for his alleged role in a major PPP fraud scheme. According to the allegations, Martinez made false representations to the SBA to obtain $932 million in capital and issue $823 million in PPP loans to more than 36,000 businesses, which netted over $71 million in lender fees.

Former Bank Executives Pleaded Guilty in Iowa, Sentenced to Prison, for Fraud That Caused Over $4.5 Million in Federal Losses

Former bank executives Larry Henson, Andrew Erpelding, and Susan McLaughlin and former lending service provider president Michael Slater pleaded guilty after fraudulently obtaining SBA-guaranteed loans. When the loans defaulted, they shifted over $4.5 million in losses to the SBA.

Oklahoma Resident Convicted for Fraudulently Applying for $5.4 Million in PPP Loans

Olusola Ojo was found guilty by jury of bank fraud conspiracy, bank fraud, and aggravated identity theft for fraudulently applying for $5.4 million in PPP loans from multiple banks. He and his conspirators, spouses Ibanga and Teosha Etuk, created fake businesses and falsified payrolls, employee counts, taxes paid, ownership details, and their relationships with one another. They received nearly $1 million from the banks.

Massachusetts Owner of Information Technology Services Company Convicted in $2 Million PPP Fraud

Elijah Majak Buoi, owner of information technology (IT) services company Sosuda Tech LLC, was convicted for filing six fraudulent PPP loan applications seeking more than $13 million. In the applications, he misrepresented employee counts and payroll expenses and submitted fraudulent Internal Revenue Service (IRS) tax forms. In reality, his company had no U.S.-based employees or payroll. The government has recovered nearly all of the $2 million Buoi obtained.

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 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 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. 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 to ensure liquidity in financial markets and to 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 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.

Status Updates for Completed, Initiated, and Planned Work

In our prior semiannual report, we outlined our audit planning and risk identification activities related to pandemic oversight. Those activities included creating a management challenge related to the Board's emergency lending programs to help inform our audit planning activities. In our management challenges documents issued in March 2021, 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. In addition, we adapted aspects of the Bureau's management challenges to highlight the operational challenges presented by the pandemic response.

In 2020, we initiated an ongoing Board pandemic response monitoring effort for risk assessment purposes and as part of our audit planning activities, to help inform our future selection of prospective 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
- whether pandemic response lending efforts served the intended communities

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 these planning activities, we have initiated the audits and evaluations outlined below and describe the current status of those audits and evaluations.

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

We issued this report in March 2022; see the summary below.

Evaluation of Third-Party Cybersecurity Risk Management Processes for Vendors Supporting the MSLP and the Secondary Market Corporate Credit Facility

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 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 Secondary Market Corporate Credit Facility (SMCCF). This project is in the reporting phase.

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 compressed time frames available to create the programs, 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 are assessing the System's vendor selection and management processes related to FRB New York's emergency lending programs. This evaluation is in the fieldwork phase.

Evaluation of the System's Loan Purchase and Administration for Its MSLP

The Board established the MSLP to facilitate lending to small and medium-sized for-profit and nonprofit organizations. To do so, the Federal Reserve Bank of Boston 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 Reserve Bank 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 Federal Reserve Bank of Boston 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 assess the MSLP loan purchase and administration processes, including the design, implementation, and operating effectiveness of internal controls.

Evaluation of the Board's and the Bureau's Return-to-Office Plans

We have initiated separate return-to-office evaluations at the Board and the Bureau. After an extended period of full-time telework because of the COVID-19 pandemic, the Board and the Bureau have begun implementing multiphase return-to-office plans. We have initiated limited-scope reviews of certain aspects of the agencies' return-to-office plans. Specifically, we plan to evaluate each agency's controls related to the following: facility cleaning and air filtration standards; social distancing protocols and signage; building access protocols for employees, visitors, and contractors; and vaccination requirements for visitors and contractors.

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.

IT 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 has performed data analytics of MSLP borrower and financial information, which is being considered in the scope of the evaluation of the System's loan purchase and administration for the MSLP.

Pandemic-Related Investigations

Our Office of Investigations is dedicated to identifying and investigating potential fraud related to the lending facilities that are central to the Board's pandemic response. In conducting our work in this area, we have leveraged our relationships with various federal law enforcement organizations, U.S. attorney's offices, PRAC, and other OIGs. Since the start of the pandemic, our work has resulted in 95 full investigations; 48 arrests; 30 convictions; and over $24.2 million in criminal fines, restitution, and special assessments.

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

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

The Board Can Improve the Efficiency and Effectiveness of Certain Aspects of Its Consumer Compliance Examination and Enforcement Action Issuance Processes

2021-SR-B-012 **October 6, 2021**

The Board delegates to each Reserve Bank the authority to supervise certain financial institutions located within the Reserve Bank's district. Reserve Bank consumer compliance examination staff help execute the Board's consumer compliance supervision program, and the Board's Division of Consumer and Community

Affairs (DCCA) oversees these delegated responsibilities. DCCA's *Consumer Compliance Handbook* describes UDAP and fair lending as two of the most significant consumer compliance risk areas for financial institutions. We assessed the efficiency and effectiveness of the Board's and the Reserve Banks' consumer compliance examination and enforcement action issuance processes, including the processes pertaining to UDAP and fair lending matters.

DCCA can improve the efficiency and effectiveness of the UDAP review processes by developing formal performance goals and target time frames, establishing criteria for when DCCA must review a potential UDAP matter, and providing guidance and training to Reserve Bank consumer compliance supervision personnel. Although DCCA has recently made efforts to improve the timeliness of the fair lending review processes by establishing new performance measures and targets as well as refining the criteria for delegating certain fair lending reviews to the Reserve Banks, DCCA can further enhance these processes by developing additional training to help acclimate Reserve Bank staff and examiners to their newly delegated roles and responsibilities. In addition, DCCA should assess the staffing structure and approach of its Fair Lending Enforcement and UDAP Enforcement sections. Finally, DCCA can enhance transparency in the UDAP and fair lending examination and enforcement action issuance processes by clarifying expectations for communicating with key stakeholders.

Our report contains recommendations designed to enhance the efficiency and effectiveness of the Board's and the Reserve Banks' consumer compliance examination and enforcement action issuance processes for UDAP and fair lending matters. The Board concurred with our recommendations.

2021 Audit of the Board's Information Security Program

2021-IT-B-014 **October 29, 2021**

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 continues to operate effectively at a level-4 (*managed and measurable*) maturity. Since our review last year, the Board has taken several steps to strengthen its information security program. Nonetheless, the agency 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.

This year, we noted opportunities for improvement related to system-level plans of action and milestones (POA&Ms), documented system-level risk acceptances, and the implementation of the Board's software and license asset management processes for one of the agency's divisions. Similar to our previous FISMA

audits, a consistent theme we noted is that the decentralization of IT services results in an incomplete view of the risks affecting the Board's security posture.

The Board has taken sufficient action to close 8 of the 15 recommendations from our prior FISMA audits that remained open at the start of this audit. This report contains 2 new recommendations designed to strengthen the Board's information security program in the area of cybersecurity risk management. The Board concurred with our recommendations.

The Board Can Enhance Its Personnel Security Program

2022-MO-B-001 **January 31, 2022**

The Board's Personnel Security Services (PSS) section conducts background investigations to determine an individual's suitability to be employed and grants security clearances to individuals with a need to access classified information. We assessed the efficiency and effectiveness of the Board's process and controls for completing background investigations and granting security clearances for employees and contractors.

The Board can enhance its personnel security program. Specifically, PSS has not defined objectives or risk tolerances to measure program performance and did not consistently follow its processes for documenting position risk designations for the background investigations initiated during our scope. PSS conducted the appropriate investigations for contractors but did not always conduct investigations at the appropriate tier for Board employees.

In addition, PSS did not have a process to reconcile data in its case management system, did not perform periodic reviews to ensure the accuracy of reinvestigation due dates in the case management system, and did not always approve security clearance access request forms in a timely manner.

Lastly, we found that PSS did not have processes to document its annual validation of a clearance holder's need for continued access to classified information and did not always document the validation attempt prior to initiating a reinvestigation.

Our report contains recommendations designed to enhance the Board's personnel security program and strengthen processes and controls for completing background investigations and granting security clearances for employees and contractors. The Board generally concurred with our recommendations.

The Board's Contract Modification Process Related to Renovation Projects Is Generally Effective

2022-FMIC-B-002 **February 2, 2022**

The Board is planning and managing major renovations of all four buildings it owns. These multiyear projects pose financial and operational risks, such as overpayment for services and schedule delays. We reviewed the Board's contract modification process related to its renovation projects to ensure compliance with its relevant process, policy, and guidance. The modifications within our scope totaled approximately $42 million.

The Board complied with its change order process by using contractors to mitigate schedule delays and financial risks associated with renovation projects. The Board also complied with policy requirements and generally complied with guidance related to its review process for renovation contract modifications. However, in five instances, the Board issued modifications without completing the relevant forms or obtaining the appropriate approvals because of administrative oversights.

Our report does not contain any recommendations because the Board replaced its manual process for completing the forms and obtaining approvals with an electronic process that included automatic reminders and approval status tracking.

Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2021 and 2020, and Independent Auditors' Report

2022-FMIC-B-003 **February 24, 2022**

The Board performs the accounting function for the FFIEC, and we contract with an independent public accounting firm to annually audit the financial statements of the FFIEC. The contract requires the audits to be performed in accordance with auditing standards generally accepted in the United States and in accordance with the auditing standards applicable to financial audits in *Government Auditing Standards*, issued by the comptroller general of the United States. We reviewed and monitored the work of the independent public accounting firm to ensure compliance with applicable standards and the contract.

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the FFIEC as of December 31, 2021 and 2020, and the results of operations and cash flows for those years in conformity with accounting principles generally accepted in the United States. The auditors' report on internal control over financial reporting and on compliance and other matters disclosed no instances of noncompliance or other matters.

The Board Has Effective Processes to Collect, Aggregate, Validate, and Report CARES Act Lending Program Data

2022-FMIC-B-004 **February 28, 2022**

The COVID-19 pandemic disrupted economic activity in the United States, which affected many sectors of the financial system. In response to the pandemic, the Board established lending programs under the CARES Act to support state and local governments and businesses of all sizes. The Board is required by statute to report on any outstanding loan or guarantee programs once every 30 days. We assessed the Board's processes for collecting, aggregating, validating, and reporting data related to its CARES Act lending programs.

The Board meets its CARES Act reporting requirements; voluntarily reports transaction-specific data; and publishes complete and accurate data, with the exception of some immaterial inaccuracies. Although the Board established and documented processes for collecting, aggregating, validating, and reporting CARES Act lending program data, it can improve the documentation of a key decision related to how it gains assurance that the publicly reported transaction-specific data are accurate and complete.

While the Board's decision to publish transaction-specific data exceeded applicable statutory requirements for publishing aggregate-level data on the lending programs, we identified additional opportunities to enhance transparency and reduce the potential to report immaterial inaccuracies in the supplemental data, which would further the Board's long-term objective to increase the public's understanding of its activities.

Our report contains recommendations designed to help the Board quickly establish processes for reporting on lending programs under similar future circumstances. The Board concurred with our recommendations, and one recommendation was closed, based on actions taken by the Board, upon issuance of this report.

Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2021 and 2020, and Independent Auditors' Report

2022-FMIC-B-005 **March 3, 2022**

We contracted with an independent public accounting firm to audit the financial statements of the Board and to audit the Board's internal control over financial reporting. The contract requires the audits of the financial statements to be performed in accordance with the auditing standards generally accepted in the United States; the standards applicable to financial audits in *Government Auditing Standards*, issued by the comptroller general of the United States; and the auditing standards of the Public Company Accounting

Oversight Board. The contract also requires the audit of internal control over financial reporting to be performed in accordance with the attestation standards established by the American Institute of Certified Public Accountants and with the auditing standards of the Public Company Accounting Oversight Board. We reviewed and monitored the work of the independent public accounting firm to ensure compliance with applicable standards and the contract.

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the Board as of December 31, 2021 and 2020, and the results of its operations and its cash flows for those years in conformity with accounting principles generally accepted in the United States. Also, in the auditors' opinion, the Board maintained, in all material respects, effective internal control over financial reporting as of December 31, 2021, based on the criteria established in *Internal Control—Integrated Framework* by the Committee of Sponsoring Organizations of the Treadway Commission. The auditors' report on compliance and other matters disclosed no instances of noncompliance or other matters.

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

2022-IT-B-006 **March 23, 2022**

The Board is increasingly using internet-based computing services (commonly referred to as *cloud services* or *cloud technologies*) and has developed a cloud strategy that emphasizes solutions that support business capabilities and opportunities for the efficient execution of the Board's mission. Pursuant to FISMA, we evaluated the effectiveness of the Board's life cycle processes for ensuring that cybersecurity risks are adequately managed for cloud systems in use.

We found that the Board has established an information systems security life cycle that is intended to ensure that cybersecurity risks for all systems, including those that are cloud based, are adequately managed. However, we found that the Board's security life cycle processes are not consistently implemented for select cloud systems across the agency. Specifically, life cycle processes in the areas of assessing security controls, authorizing information systems, and monitoring security controls were not consistently performed.

Our report includes recommendations designed to strengthen the Board's cloud system inventory and cybersecurity life cycle processes, as well as matters for management consideration. The Board concurred with our recommendations.

Bureau of Consumer Financial Protection

Independent Auditors' Report on the Bureau's Fiscal Year 2021 Compliance With the Digital Accountability and Transparency Act of 2014

2021-FMIC-C-013 **October 27, 2021**

The DATA Act requires IGs to periodically provide Congress with an assessment of the completeness, accuracy, timeliness, and quality of a statistical sample of spending data submitted by their agency and the agency's implementation and use of the applicable data standards. We contracted with an independent certified public accounting firm to audit the Bureau's fiscal year 2021 compliance with DATA Act requirements. We reviewed and monitored the work of the contractor to ensure compliance with the contract and applicable auditing standards.

The contractor determined that the data it sampled from the data the Bureau reported to USAspending.gov were complete, accurate, and timely. The contractor rated the quality of the data as excellent based on the Quality Scorecard designed to provide governmentwide consistency in the measurement of quality. The Bureau also implemented and used governmentwide financial data standards as established by the Office of Management and Budget and Treasury, as applicable, and presented required elements in accordance with standards.

2021 Audit of the Bureau's Information Security Program

2021-IT-C-015 **October 29, 2021**

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 continues to operate effectively at a level-4 (*managed and measurable*) maturity. Since our review last year, the Bureau has taken several steps to strengthen its information security program. Nonetheless, similar to our previous FISMA audits, 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.

This year, we identified opportunities to improve the Bureau's enterprise cybersecurity risk management processes, POA&M process for technical vulnerabilities, and configuration management plan.

The Bureau has taken sufficient actions to close 2 of the 11 recommendations from our prior FISMA audits that were open at the start of this audit. This report includes 3 new recommendations designed to

strengthen the Bureau's information security program in the areas of risk and configuration management. The Bureau concurred with our recommendations.

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

2021-SR-C-016 **November 1, 2021**

Within the Bureau's Division of Supervision, Enforcement and Fair Lending (SEFL), the Office of Supervision Examinations (OSE) is responsible for supervising and examining institutions' compliance with federal consumer financial laws. OSE's Oversight team is responsible for developing and supporting the supervision program and manages the Quality Management Program (QMP) for supervision activities. We assessed the design and effectiveness of SEFL's QMP for supervision activities.

SEFL can improve the effectiveness of its QMP for supervision activities by finalizing the updates to existing and draft QMP policies, procedures, and guidance and considering increasing SEFL leadership involvement in formal program oversight. Additionally, OSE should enhance aspects of the QMP's quality control review processes, assess the program's current staffing level and structure, formalize its training program, and enhance the reporting and distribution of its quality assurance results.

Our report contains recommendations designed to enhance the effectiveness of SEFL's QMP for supervision activities. The Bureau concurred with our recommendations.

The Bureau Can Further Enhance Certain Aspects of Its Approach to Supervising Nondepository Institutions

2021-SR-C-017 **December 8, 2021**

The Bureau's SEFL is responsible for ensuring compliance with federal consumer financial laws by supervising market participants and initiating enforcement actions when appropriate. The Dodd-Frank Act authorizes the Bureau to supervise depository institutions and their affiliates with more than $10 billion in total assets and certain nondepository institutions. We assessed SEFL's approach to supervising nondepository institutions.

SEFL applies consistent examination procedures to depository and nondepository institutions and uses the same approach to follow up on Matters Requiring Attention. These approaches help to ensure that the Bureau consistently supervises these two types of financial institutions. SEFL can, however, further improve its approach to supervising nondepository institutions. Specifically, SEFL has issued consumer compliance ratings to nondepository institutions less frequently than to depository institutions and faces challenges gathering information to identify the total population of nondepository institutions within

the Bureau's jurisdiction. We also found that limited staffing levels in SEFL's OSE constrain the Bureau's ability to examine nondepository institutions. Lastly, SEFL's guidance lacked definitions for tracking certain examination data, and we identified inconsistent and missing data in SEFL's system of record.

Our report contains recommendations designed to further enhance the Bureau's approach to supervising nondepository institutions. 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 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.

Many of our investigations during this semiannual reporting period concern fraud related to the Federal Reserve's pandemic response efforts, including the MSLP, which supported lending to small and medium-sized for-profit and nonprofit organizations in sound financial condition prior to the COVID-19 pandemic, and the Paycheck Protection Program Liquidity Facility, which extended credit to eligible financial institutions and took PPP loans guaranteed by the SBA as collateral. In addition, our office also conducted investigations in support of our membership on PRAC.

The following are examples from this reporting period of investigations into matters affecting the Board's ability to carry out its supervisory responsibilities.

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

Arkansas resident Rashaud Brown, a former bank teller, was sentenced to 4 weekends in jail followed by 3 years of supervised release. He was also ordered to pay $2,000 in restitution and a $100 special assessment. Brown previously pleaded guilty to one count of bank fraud for his role in embezzling funds from an elderly customer's account while Brown was employed at Arvest Bank, a state member bank. As part of the plea agreement, Brown is prohibited from working in the banking industry.

Brown engaged in 11 fraudulent cash withdrawals from the elderly victim's account. He 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 was prosecuted by the U.S. Attorney's Office for the Eastern District of Arkansas.

Former Bank Executives Pleaded Guilty in Iowa, Sentenced to Prison, for Fraud That Caused Over $4.5 Million in Federal Losses

Larry Henson, Andrew Erpelding, and Susan McLaughlin, former executives of now-defunct Valley Bank in Moline, Illinois, and Michael Slater, former president of Iowa-based lending service provider Vital Financial Services, pleaded guilty to conspiracy to commit wire fraud affecting a financial institution for their roles in a scheme to defraud the SBA in connection with its programs to guarantee loans made to small businesses. Henson was sentenced to 9 months in prison followed by 5 years of supervised release. Henson was also ordered to pay $4.5 million in restitution and a $100 special assessment. Erpelding, McLaughlin, and Slater face maximum penalties of 30 years in prison.

The four coconspirators fraudulently obtained loan guarantees from the SBA on behalf of Valley Bank borrowers despite knowing that the loans did not meet SBA guidelines and requirements. They did so in part by altering loan payment histories, renaming businesses, and hiding previous loan defaults. When the fraudulently guaranteed loans defaulted, the coconspirators caused the submission of reimbursement requests to the SBA to purchase the defaulted loans from investors and lending institutions, thereby shifting the majority of losses to the SBA. In all, they attempted to obtain guarantees on over $14 million in loans, were successful in obtaining guarantees on over $9 million in loans, and caused the SBA losses of over $4.5 million.

This case was investigated by our office, the Federal Bureau of Investigation (FBI), the Federal Deposit Insurance Corporation (FDIC) OIG, the Federal Housing Finance Agency (FHFA) OIG, and the SBA OIG. It is being prosecuted by the DOJ Criminal Division and the U.S. Attorney's Office for the Southern District of Iowa.

Three Charged With Financial Crimes While Employed at North Dakota Banks

Brady Torgerson was charged with bank fraud, misapplication of bank funds, making false entries in bank records, and aggravated identity theft while employed at two North Dakota financial institutions. Brent Torgerson and Kelly Huffman were each charged with misapplication of bank funds while employed at the North Dakota financial institutions. 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, Brady Torgerson engaged in a scheme to defraud both financial intuitions by issuing bank funds to individuals not entitled to the funds, failing to register banking transactions, creating fraudulent loan obligations, and taking actions to conceal his activities. Brent Torgerson, Brady's father, misapplied bank funds by issuing a $724,558 cashier's check to his son without obtaining promissory notes and other necessary financial paperwork. Huffman misapplied bank funds by unlawfully issuing a $125,649 check advance at Brady Torgerson's request.

This case was investigated by our office, the FDIC OIG, and the FHFA OIG. It is being prosecuted by the U.S. Attorney's Office for the District of North Dakota.

Two Loan Brokers and One Loan Officer Charged in Massachusetts Bank Fraud Scheme

Ted Capodilupo, Joseph Masci, and Brian Ferris were charged with and have agreed to plead guilty to one count each of conspiracy to commit bank fraud in connection with a scheme to defraud the SBA and a Massachusetts bank. The bank is a subsidiary of Berkshire Hills Bancorp Inc., a bank holding company supervised by the Board. 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, Capodilupo, Masci, and Ferris agreed to defraud the bank and the SBA by submitting fraudulent loan applications to the bank to secure SBA-guaranteed loans. Capodilupo and Masci, who operated a loan brokerage business, submitted dozens of fraudulent applications on behalf of borrowers ineligible for traditional business loans. The defendants misrepresented the identities of the real loan recipients and the businesses for which the loans were sought. Capodilupo and Masci also fabricated federal tax forms, falsified applicant signatures, and falsely indicated that no broker had

assisted in preparing or referring the applications. Capodilupo and Masci charged borrowers fees for obtaining these fraudulent loans; the scheme generated about $270,000 in fees for Capodilupo and Masci. Ferris, who worked as a loan officer at the bank, caused the bank to issue the loans and received a $500 kickback from Capodilupo and Masci for each loan. Many of the loans ultimately defaulted, resulting in substantial losses to the bank.

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

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

Glenn E. Diaz, former St. Bernard Parish assistant district attorney, and two associates, Peter J. Jenevein and Mark S. Grelle, were indicted for bank fraud, conspiracy to commit bank fraud, and money laundering related to their alleged defrauding of First NBC Bank, the New Orleans–based bank that failed in April 2017. The bank was a subsidiary of First NBC Bank Holding Company, a Board-supervised bank holding company. 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 19-count indictment, from at least April 2016 through December 20, 2016, Diaz, Jenevein, and Grelle conspired to defraud First NBC Bank through a series of false invoices for work purportedly done at a Florida warehouse owned by Diaz. Diaz, a customer of First NBC Bank, had been overdrawing his checking account for purported business expenses but was instead depositing these overdrafts into his personal account at another bank. After First NBC Bank officers began requiring Diaz to prove that the funds were used for business expenses, Diaz had Jenevein provide invoices for work performed by Grelle's company, Grelle Underground Services LLC. Bank officers approved the overdrafts based on these invoices. However, after Diaz wrote the check to Grelle's company, Grelle would then write a check back to Diaz. Diaz would then deposit the money into his personal account and use it for personal and business expenditures unrelated to the Florida warehouse project. In total, Diaz, Jenevein, and Grelle executed 17 round-trip transactions that defrauded First NBC Bank of $345,841.

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

Oklahoma Resident Sentenced to Prison for Fraudulently Applying for PPP Loans

Adam Winston James of Oklahoma was sentenced to 2 years in prison followed by 1 year of supervised release for aggravated identity theft in a scheme to defraud Regent Bank when applying for a PPP loan. He was also ordered to pay $25,906 in restitution and a $100 special assessment.

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.

Oklahoma Resident Convicted for Fraudulently Applying for $5.4 Million in PPP Loans

Olusola Ojo was found guilty of one count of bank fraud conspiracy, two counts of bank fraud, and one count of aggravated identity theft following a jury trial and was immediately taken into custody until sentencing. His coconspirators, spouses Ibanga and Teosha Etuk, were sentenced to prison as reported in our previous semiannual report to Congress.

Ojo and the Etuks created 12 fictitious businesses to fraudulently apply for duplicative PPP loans from multiple banks. To support their applications, the trio falsified payroll spending, employee counts, taxes paid, ownership details, and the coconspirators' relationships with one another. They conspired to obtain $5.4 million in loans and ultimately received $995,385 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.

Massachusetts Owner of IT Services Company Convicted in $2 Million PPP Fraud

Elijah Majak Buoi, owner of IT services company Sosuda Tech LLC, was convicted of four counts of wire fraud and one count of making a false statement to a financial institution in connection with filing fraudulent PPP loan applications seeking more than $13 million. For the wire fraud charge, Buoi faces up to 20 years in prison and 3 years of supervised release as well as a fine of up to $250,000 or twice the gross gain or loss from the offense. For the making a false statement to a financial institution charge, Buoi

faces up to 30 years in prison and 3 years of supervised release as well as a fine of up to $250,000 or twice the gross gain or loss from the offense.

Buoi submitted six fraudulent PPP loan applications on behalf of his company to four SBA-approved lenders. In each loan application, Buoi misrepresented employee counts and payroll expenses and submitted fraudulent IRS tax forms. In reality, Sosuda Tech was a startup company with no U.S.-based employees or payroll. As a result of his scheme, Buoi obtained a $2 million PPP loan. The government recovered nearly $2 million of the loan funds.

The case was investigated by our office, the FBI, the FDIC OIG, and IRS–Criminal Investigation. It is being prosecuted by the U.S. Attorney's Office for the District of Massachusetts and the DOJ Criminal Division.

New York–Florida Resident Pleaded Guilty in $6.8 Million PPP Fraud

Gregory J. Blotnick, a dual New York and Florida resident, pleaded guilty to one count of wire fraud and one count of money laundering for his role in a scheme to fraudulently obtain over $6.8 million in PPP loans. He faces up to 30 years in prison.

From April 2020 through March 2021, Blotnick submitted 21 fraudulent PPP loan applications to 13 lenders on behalf of 9 purported businesses that he controlled. Blotnick falsified various information to the lenders, including employee counts, federal tax returns, and payroll documentation. Based on these misrepresentations, the lenders approved Blotnick's PPP loan applications and provided his purported business with about $4.6 million in loans. Blotnick then transferred most of the funds to brokerage accounts and lost more than $3 million in stock trades.

The case was investigated by our office, the FDIC OIG, the FHFA OIG, IRS–Criminal Investigation, and the U.S. Social Security Administration (SSA) OIG. It is being prosecuted by the U.S. Attorney's Office for the District of New Jersey.

Three Oklahoma Residents Pleaded Guilty in PPP Fraud

Three Oklahoma residents pleaded guilty to charges stemming from a scheme in which they fraudulently obtained nearly $800,000 in PPP loans. Aleta Necole Thomas, the leader of the scheme, pleaded guilty to two counts of false statement to a financial institution and faces up to 30 years in prison and up to a $1 million fine. Katrina West and Pepper Jones each pleaded guilty to one count of false statement and face up to 5 years in prison and a fine of up to $10,000. In total, the defendants have agreed to pay $795,159 in restitution, of which nearly $210,000 has already been seized.

Using a bogus business to obtain PPP loans for herself, Thomas submitted false information to two financial institutions, Cross River Bank and First Electronic Bank. Thomas forged bank statements and IRS forms

to support the claim that Coming Correct Community Ministry had 26 employees and contractors and average monthly payroll expenses of $35,000. West and Jones similarly used bogus businesses to obtain loans from two other financial institutions, Fountainhead Commercial Capital and Harvest Small Finance LLC, respectively.

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

Oklahoma Business Owner Pleaded Guilty in MSLP Fraud

Jill Nicole Ford pleaded guilty to bank fraud and money laundering related to a loan obtained through the MSLP. Ford agreed to pay $252,143 in restitution and a $200 special assessment. Ford also faces up to 30 years in prison and a $1 million fine for the bank fraud charge and up to 10 years in prison and a $250,000 fine for the money laundering charge, which may be followed by up to 5 years of supervised release.

Ford claimed that the MSLP loan she obtained for her business, Oliver & Olivia Apparel, Inc., would be used for working capital and employee payroll. Instead, Ford laundered the loan proceeds by using them to pay for construction of her personal home. She also used the funds to purchase a luxury SUV for personal use.

This case was investigated by our office, the FBI, IRS–Criminal Investigation, the SBA OIG, the Special Inspector General for Pandemic Recovery, and the U.S. Secret Service. It is being prosecuted by the U.S. Attorney's Office for the Western District of Oklahoma.

Kentucky Businessowner Pleaded Guilty to Wire Fraud in Connection With $1.3 Million PPP Fraud

Randall "Rocky" Blankenship Jr., owner of several business entities, pleaded guilty to a conspiracy to commit wire fraud to obtain PPP loans from two Kentucky banks under false pretenses. He agreed to pay restitution of $1.3 million and faces up to 20 years in prison, a $250,000 fine, and 3 years of supervised release.

Blankenship, with the help of a certified public accountant, created fake tax documents and payroll records indicating that his businesses—Blankenship RV Finance Solutions LLC, RSGG Properties LLC, RSGG Holdings LLC, and RSGG Investments LLC—had hundreds of thousands of dollars in quarterly payroll expenses. In reality, none of the entities had any payroll expenses. Blankenship then submitted four PPP loan applications through two Kentucky banks and, as a result, fraudulently obtained $1.3 million in loans. Blankenship used some of the funds for his recreational vehicle business (which had already received its

own PPP loan and was ineligible for additional loans at the time) and his personal use, including paying off casino debt and purchasing real estate.

This was a joint investigation by our office, the FBI, and the FDIC OIG. It is being prosecuted by the U.S. Attorney's Office for the Eastern District of Kentucky.

Las Vegas Resident Pleaded Guilty to PPP Fraud While on Pretrial Release for Attempted Robbery Charge

Keyawn Lloyd Cook Jr. of Nevada pleaded guilty to one count of wire fraud related to a scheme to defraud the SBA and a lender by filing fraudulent loan applications seeking over $100,000 in PPP loans. He faces up to 30 years in prison.

According to court documents and admissions made in court, Cook—while on pretrial release for an attempted robbery charge—submitted at least five fraudulent loan applications over a 15-month period for Economic Injury Disaster Loan (EIDL) and PPP funding. Cook submitted loan applications in the names of multiple nonexistent businesses claiming to operate in various industries. Cook falsely claimed to have between 9 and 12 employees in the applications for EIDL funding and, in his application for a $100,000 PPP loan, he falsely claimed gross revenues of $50,000 by a bogus barber shop. Separately, Cook was sentenced to 5 years in prison for his attempted robbery of an armored car employee in 2019.

This case was investigated by our office, the FBI, IRS–Criminal Investigation, and the SBA OIG. It is being prosecuted by the U.S. Attorney's Office for the District of Nevada.

CEO of PPP Lender MBE Capital Partners Charged in New York in Nearly $1 Billion PPP Loan and Lender Fraud

Rafael Martinez, CEO and primary owner of MBE Capital Partners, was charged with numerous counts for his alleged role in a PPP fraud scheme. Martinez was charged with one count of bank fraud, two counts of wire fraud, one count of making false statements to a bank, one count of making false statements, one count of making false statements to the SBA, and one count of aggravated identity theft. 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, Martinez used false representations and documents to fraudulently obtain the SBA's approval for his company, MBE Capital Partners LLC, to be a nonbank PPP lender. After MBE was approved, Martinez obtained about $932 million in capital and issued $823 million in PPP loans to about 36,600 businesses. Those loans earned Martinez over $71 million in lender fees. In addition, Martinez schemed to obtain a PPP loan of over $283,000 for MBE through false statements about employees and

wages using the forged signature of MBE's tax preparer. Martinez spent the proceeds from his criminal conduct on, among other things, a $10 million villa in the Dominican Republic; a $3.5 million mansion in New Jersey; a chartered jet service; and several luxury vehicles, including a Bentley, a BMW, a Ferrari, a Mercedes-Benz, and a Porsche.

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

Three New Jersey Residents Charged in $2.1 Million PPP and EIDL Fraud

Three New Jersey residents were charged for their alleged roles in fraudulently obtaining over $2.1 million in EIDL and PPP loans. Arlen G. Encarnacion was charged with 11 counts of bank fraud, 3 counts of wire fraud, and 2 counts of money laundering. Kent Encarnacion was charged with 1 count of bank fraud and 2 counts of money laundering. Jacquelyn Pena was charged with 3 counts of bank fraud and 2 counts of money laundering.

According to the allegations, Arlen Encarnacion submitted 11 fraudulent PPP loan applications to two lenders on behalf of nine purported businesses and three fraudulent EIDL applications to the SBA on behalf of three purported businesses. Kent Encarnacion submitted 1 fraudulent PPP loan application on behalf of a purported business to one lender and Pena submitted 3 fraudulent PPP loan applications to two lenders on behalf of three purported businesses. Using bogus tax documents and fabricated employees and wages, the defendants received about $2.1 million in federal COVID-19 emergency relief funds meant for distressed small businesses. Of this amount, Arlen Encarnacion received about $1.7 million, Kent Encarnacion about $156,000, and Pena about $335,000. The defendants then used the money for personal purchases, including real estate and a Lamborghini SUV.

The case was investigated by our office, the FDIC OIG, the FHFA OIG, IRS–Criminal Investigation, Homeland Security Investigations, the SSA OIG, and the U.S. Postal Inspection Service. It is being prosecuted by the U.S. Attorney's Office for the District of New Jersey.

New Jersey Resident Charged in $1 Million PPP and EIDL Fraud

Nivah Garcis was charged with one count of bank fraud and one count of money laundering for her alleged role in fraudulently obtaining over $1 million in EIDL and 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.

According to the allegations, Garcis submitted two fraudulent PPP loan applications to a lender on behalf of two purported businesses and three fraudulent EIDL applications to the SBA on behalf of three

purported businesses. The applications Garcis submitted each contained fraudulent representations to the lender and the SBA, including bogus IRS tax documents. Garcis also fabricated the existence of employees and wages. According to IRS records, none of the purported tax documents that Garcis submitted were ever filed with the IRS. Based on Garcis's misrepresentations, her loan applications were approved for about $1.1 million in federal COVID-19 emergency relief funds. Garcis then used the proceeds for various personal expenses, including a BMW SUV.

The case was investigated by our office, the FDIC OIG, the FHFA OIG, Homeland Security Investigations, IRS–Criminal Investigation, the SSA OIG, and the U.S. Postal Inspection Service. It is being prosecuted by the U.S. Attorney's Office for the District of New Jersey.

New Jersey Resident Charged in $860,000 EIDL and PPP Loan Fraud

Butherde Darius was charged with one count of bank fraud, one count of wire fraud, and four counts of money laundering for his alleged role in fraudulently obtaining over $860,000 in EIDL and 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.

According to the allegations, Darius submitted fraudulent EIDL and PPP loan applications on behalf of his purported business, Fabulous Appetizers LLC, to lenders and the SBA. According to IRS records, many of the purported tax documents Darius submitted were never filed with the IRS. Darius also fabricated the existence of employees and the revenue of his business. Based on these misrepresentations, Darius received about $862,000 in federal COVID-19 emergency relief funds. Darius then spent the proceeds on personal expenses, including hotels and airfare, and made cash withdrawals of over $58,000.

The case was investigated by our office, the FDIC OIG, the FHFA OIG, Homeland Security Investigations, IRS–Criminal Investigation, the SSA OIG, and the U.S. Postal Inspection Service. It is being prosecuted by the U.S. Attorney's Office for the District of New Jersey.

Texas Resident Indicted for Submitting Fraudulent PPP Loan Applications for Over $3 Million

Sinoj Kallamplackal Joseph of Texas was charged with seven counts of wire fraud and three counts of making false statements to a bank for his alleged participation in a scheme to file fraudulent applications seeking millions of dollars 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.

According to the allegations, Joseph submitted fraudulent applications for over $3 million in PPP loans to an SBA-approved lender in the names of MK Analytics LLC, Sanbi Solutions LLC, and KMS Traders Group

LLC. Joseph fabricated business records, including employee counts and payroll costs, and submitted other fraudulent documentation in support of the applications.

This case was investigated by our office, the FDIC OIG, IRS–Criminal Investigation, the Treasury Inspector General for Tax Administration, and the SBA OIG. It is being prosecuted by the U.S. Attorney's Office for the Eastern District of Texas.

Oklahoma Couple Charged for Attempted $2.7 Million PPP Loan Fraud

Spouses William Mark Sullivan and Michelle Cadman-Sullivan were each indicted by a federal grand jury in Oklahoma and charged with bank fraud conspiracy. In addition, Cadman-Sullivan was charged with four counts of aggravated identity theft. 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, the couple fraudulently applied for six PPP loans totaling more than $2.7 million at Arvest Bank in Tulsa, Oklahoma, and The Exchange Bank in Skiatook, Oklahoma. They created bogus businesses—Oaklahoma Paving LLC, U.S. Central Construction LLC, USA-1 Construction INC., and Oaklahoma Energy—and falsified on loan applications employee counts and payroll expenses. They also failed to disclose to the banks that they were submitting duplicative and overlapping applications. The couple obtained $742,927 in loans.

This case was investigated by our office and the SBA OIG. 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.

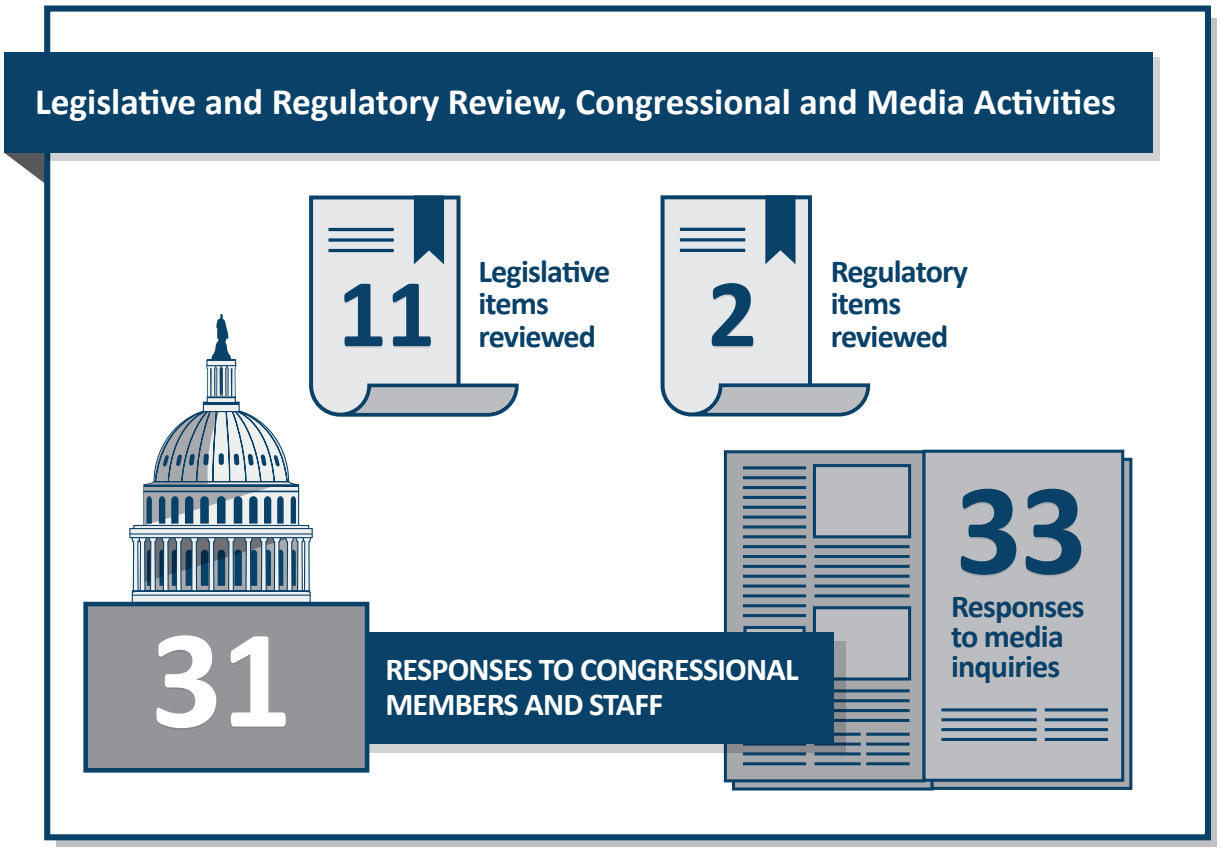
Hotline

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 72 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 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 11 legislative items and 2 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 31 responses to congressional members and staff concerning the Board and the Bureau. Additionally, we responded to 33 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 22,000 reports, detailing for fiscal year 2021 alone $62.7 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
The Board Can Improve the Efficiency and Effectiveness of Certain Aspects of Its Consumer Compliance Examination and Enforcement Action Issuance Processes	Evaluation
2021 Audit of the Board's Information Security Program	Audit
The Board Can Enhance Its Personnel Security Program	Evaluation
The Board's Contract Modification Process Related to Renovation Projects Is Generally Effective	Audit
Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2021 and 2020, and Independent Auditors' Report	Audit
The Board Has Effective Processes to Collect, Aggregate, Validate, and Report CARES Act Lending Program Data	Audit
Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2021 and 2020, and Independent Auditors' Report	Audit
The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems	Evaluation
Total number of audit reports: 5 Total number of evaluation reports: 3	

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

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
2016 Audit of the Board's Information Security Program	11/16	9	9	0	10/21	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	10/21	7	1
2017 Audit of the Board's Information Security Program	10/17	9	9	0	10/21	8	1
The Board's Organizational Governance System Can Be Strengthened	12/17	14	14	0	03/22	14	0
Security Control Review of the Board's Public Website (nonpublic)	03/18	7	7	0	02/21	4	3
Security Control Review of the Board Division of Research and Statistics' General Support System (nonpublic)	09/18	9	9	0	10/21	7	2
2018 Audit of the Board's Information Security Program	10/18	6	6	0	10/21	5	1

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Board Can 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	01/22	6	0
The Board's Law Enforcement Operations Bureau Can Improve Internal Processes	09/19	6	6	0	03/22	4	2
2019 Audit of the Board's Information Security Program	10/19	6	6	0	10/21	4	2
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	03/22	1	5
The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced	09/20	10	10	0	02/22	8	2
2020 Audit of the Board's Information Security Program	11/20	4	4	0	10/21	2	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 Economics Divisions Can Enhance Some of Their Planning Processes for Economic Analysis	02/21	6	6	0	03/22	5	1
The Board Can Improve the Management of Its Renovation Projects	03/21	2	2	0	12/21	2	0
The Board's Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced	09/21	3	3	0	n.a.	0	3
The Board Can Improve the Efficiency and Effectiveness of Certain Aspects of Its Consumer Compliance Examination and Enforcement Action Issuance Processes	10/21	10	10	0	03/22	2	8
2021 Audit of the Board's Information Security Program	10/21	2	2	0	n.a.	0	2
The Board Can Enhance Its Personnel Security Program	01/22	6	6	0	03/22	0	6
The Board Has Effective Processes to Collect, Aggregate, Validate, and Report CARES Act Lending Program Data	02/22	2	2	0	n.a.	1	1

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems	03/22	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 Auditors' Report on the Bureau's Fiscal Year 2021 Compliance With the Digital Accountability and Transparency Act of 2014	Audit
2021 Audit of the Bureau's Information Security Program	Audit
The Bureau Can Improve Aspects of Its Quality Management Program for Supervision Activities	Evaluation
The Bureau Can Further Enhance Certain Aspects of Its Approach to Supervising Nondepository Institutions	Evaluation
Total number of audit reports: 2 Total number of evaluation reports: 2	

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	10/21	2	1
2017 Audit of the CFPB's Information Security Program	10/17	7	7	0	10/21	5	2
The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data	01/18	11	11	0	01/22	9	2
Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program	02/18	2	2	0	02/22	2	0
2018 Audit of the Bureau's Information Security Program	10/18	4	4	0	10/21	2	2
Technical Testing Results for the Bureau's SQL Server Environment (nonpublic)	05/19	5	5	0	02/22	5	0
The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP	07/19	3	3	0	02/22	1	2
2019 Audit of the Bureau's Information Security Program	10/19	7	7	0	10/21	4	3

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
Testing Results for the Bureau's Plan of Action and Milestones Process	04/20	2	2	0	02/22	1	1
Technical Testing Results for the Bureau's Legal Enclave (nonpublic)	07/20	4	4	0	02/22	0	4
Results of Scoping and Suspension of the Evaluation of the Bureau's Personnel Security Program	08/20	3	3	0	02/22	3	0
2020 Audit of the Bureau's Information Security Program	11/20	1	1	0	10/21	0	1
The Bureau Can Strengthen Its Hiring Practices and Can Continue Its Efforts to Cultivate a Diverse Workforce	03/21	10	10	0	03/22	0	10
The Bureau Can Improve Its Controls for Issuing and Managing Interagency Agreements	07/21	6	6	0	03/22	0	6
Evaluation of the Bureau's Implementation of Splunk (nonpublic)	09/21	4	4	0	n.a.	0	4
2021 Audit of the Bureau's Information Security Program	10/21	3	3	0	n.a.	0	3
The Bureau Can Improve Aspects of Its Quality Management Program for Supervision Activities	11/21	9	9	0	03/22	2	7

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Bureau Can Further Enhance Certain Aspects of Its Approach to Supervising Nondepository Institutions	12/21	5	5	0	n.a.	0	5

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

n.a. not applicable.

Table A-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	146
Investigations opened during the reporting period	27
Investigations closed during the reporting period	28
Investigations open at end of the reporting period	145
Investigative results for the reporting period	
Persons referred to DOJ prosecutors	23
Persons referred to state/local prosecutors	0
Declinations received	7
Joint investigations	131
Reports of investigation issued	0
Oral and/or written reprimands	0
Terminations of employment	0
Arrests	24
Suspensions	1
Debarments	0
Prohibitions from banking industry	0
Indictments	20
Criminal informations	16
Criminal complaints	5
Convictions	20
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	$22,539,526
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	20
Complaints received during reporting period	72
Total complaints for reporting period	92
Complaints resolved during reporting period	84
Complaints pending	8

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 initiated an investigation concerning the potential loss of data and disclosure of confidential supervisory information by Venkatesh Rao, a former employee of the Board. The investigation found that Rao removed restricted documents, which contained proprietary information used by the Board to conduct bank stress tests, from a Board building and stored the material at his home. On January 28, 2020, the matter was referred to the DOJ through the U.S. Attorney's Office for the District of Maryland, which agreed that day to prosecute the matter. On March 18, 2021, Rao pleaded guilty to the theft of government property from the Board. On May 28, 2021, he was sentenced to 1 year of supervised probation, a criminal fine of $2,500, and a special assessment of $25. This investigation is closed.

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 initiated an investigation concerning allegations of the potential unauthorized disclosure of confidential supervisory information by a senior government employee related to certain bank holding companies' and nonbank financial companies' resolution plans. We were unable to substantiate allegations that the disclosure originated from a Board, Reserve Bank, or Bureau employee. After evidence emerged that the disclosure originated from a senior government employee of the FDIC, the matter was referred to the FDIC.
- We initiated an investigation concerning allegations of the potential unauthorized disclosure of confidential supervisory information. These allegations were unsubstantiated, and the investigation was closed.

- We initiated an investigation concerning allegations regarding the hiring process of senior officials at the Bureau, including potential prohibited personnel practices. These allegations were unsubstantiated, and the investigation was closed.
- We initiated an investigation concerning allegations that a private citizen was selling Board law enforcement uniforms on Facebook Marketplace. The investigation found that the uniforms were purchased by the private citizen at an auction of the contents of a storage unit rented by a senior employee in the Board's Law Enforcement Unit (LEU). The U.S. Attorney's Office for the District of Maryland declined to prosecute the matter. The Board suspended the employee for 2 days. This investigation was closed.

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	2	2
2018	4	9
2019	2	4
2020	3	9
2021	4	14
2022[a]	3	10

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 March 31, 2022.

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: 1

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 (*consistently implemented*) maturity, 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 a level-4 (*managed and measurable*) maturity. 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.

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'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 LEU's 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: 2

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: 2

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: 2

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: 1

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'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

We assessed the effectiveness of the Board's ongoing efforts to plan, develop, and integrate enterprise risk management (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.

The Board Can Improve the Efficiency and Effectiveness of Certain Aspects of Its Consumer Compliance Examination and Enforcement Action Issuance Processes

2021-SR-B-012 **October 6, 2021**

Total number of recommendations: 10
Recommendations open: 8

See the summary in the body of this report.

2021 Audit of the Board's Information Security Program

2021-IT-B-014 **October 29, 2021**

Total number of recommendations: 2
Recommendations open: 2

See the summary in the body of this report.

The Board Can Enhance Its Personnel Security Program

2022-MO-B-001 **January 31, 2022**

Total number of recommendations: 6
Recommendations open: 6

See the summary in the body of this report.

The Board Has Effective Processes to Collect, Aggregate, Validate, and Report CARES Act Lending Program Data

2022-FMIC-B-004 **February 28, 2022**

Total number of recommendations: 2
Recommendations open: 1

See the summary in the body of this report.

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

2022-IT-B-006 **March 23, 2022**

Total number of recommendations: 3
Recommendations open: 3

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	2	4
2019	2	5
2020	3	6
2021	6	35
2022[a]	0	0

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 March 31, 2022.

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 (*consistently implemented*) maturity, 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 a level-4 (*managed and measurable*) maturity. 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.

2018 Audit of the Bureau's Information Security Program

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

Total number of recommendations: 4
Recommendations open: 2

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.

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: 2

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: 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 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: 1

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 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.

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

We assessed the design and operating effectiveness of the Bureau's controls for issuing and managing interagency agreements (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.

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

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

Total number of recommendations: 4
Recommendations open: 4

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.

2021 Audit of the Bureau's Information Security Program

2021-IT-C-015 **October 29, 2021**

Total number of recommendations: 3
Recommendations open: 3

See the summary in the body of this report.

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

2021-SR-C-016 **November 1, 2021**

Total number of recommendations: 9
Recommendations open: 7

See the summary in the body of this report.

The Bureau Can Further Enhance Certain Aspects of Its Approach to Supervising Nondepository Institutions

2021-SR-C-017 **December 8, 2021**

Total number of recommendations: 5
Recommendations open: 5

See the summary in the body of this report.

Abbreviations

CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CEO	chief executive officer
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
DCCA	Division of Consumer and Community Affairs
DFMU	designated financial market utility
DOJ	U.S. Department of Justice
EIDL	Economic Injury Disaster Loan
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
FHFA	Federal Housing Finance Agency
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
IT	information technology
LEU	Law Enforcement Unit
LISCC	Large Institution Supervision Coordinating Committee
MDPS	multiregional data processing servicer
MSLP	Main Street Lending Program
OSE	Office of Supervision Examinations
PIIA	Payment Integrity Information Act of 2019

POA&M	plan of action and milestones
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
PSS	Personnel Security Services
QMP	Quality Management Program
SBA	U.S. Small Business Administration
SEFL	Division of Supervision, Enforcement and Fair Lending
SMCCF	Secondary Market Corporate Credit Facility
SSA	U.S. Social Security Administration
UDAP	unfair or deceptive acts or practices

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

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

OIG Hotline

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

800-827-3340