Office of Inspector General

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

Semiannual Report to Congress

April 1, 2022–September 30, 2022

OIG

Semiannual Report to Congress

April 1, 2022–September 30, 2022

Office of Inspector General

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

Message From the Inspector General

Although it appears that the COVID-19 virus will be with us for some time, many of us have begun to take steps in both our personal and our professional lives to reconnect with others, rebuild our routines, and regain a sense of normalcy. As part of this transition, our office and both of the agencies we oversee are shifting to hybrid work.

The Board of Governors of the Federal Reserve System completed its return-to-office plan on June 3 and transitioned to a hybrid work schedule. The Consumer Financial Protection Bureau ended maximum telework by June and implemented optional full-time telework that will run through October 31. In separate evaluations, we assessed whether the Board and the CFPB implemented select workplace safety measures in response to the pandemic. We found that each agency's enhanced cleaning, air filtration practices, social distancing measures, building access controls, and other actions were executed in accordance with their respective plans.

Our oversight of pandemic response efforts remains critically important. I continue to serve on the Pandemic Response Accountability Committee (PRAC) and am vice chair of the PRAC Investigations Subcommittee as well as a member of the PRAC Financial Sector Oversight Subcommittee. In addition, our Office of Audits and Evaluations and Office of Information Technology continue to assess the Board's lending programs. Currently, we are evaluating the loan purchase and administration processes for the Main Street Lending Program (MSLP), vendor selection and management processes related to the Federal Reserve Bank of New York's lending programs, and cybersecurity risk management for vendors supporting the MSLP and the Secondary Market Corporate Credit Facility.

Our Office of Investigations maintains a heavy caseload examining fraud related to the emergency lending programs established in response to the pandemic. In one recent case, for example, a Missouri business owner was charged in a 52-count indictment for a $27.1 million bank fraud scheme that included $12.4 million in forgivable Paycheck Protection Program (PPP) loans meant to help businesses weather the pandemic. In another, the owner of a Massachusetts information technology services company was sentenced to 39 months in prison and 3 years of supervised release for repeatedly filing loan applications using false tax documents and payroll processing records in an attempted $13 million PPP fraud; he received $2 million, nearly all of which the government has since recovered. In total, over the past 6 months, our investigative work related to pandemic fraud has resulted in 38 full investigations; 23 arrests; 18 convictions; and over $16.2 million in criminal fines, restitution, and special assessments.

Overall, our Office of Investigations closed 28 investigations and resolved 70 hotline complaints. Our work resulted in 17 referrals for criminal prosecution; 24 arrests; 14 indictments; 19 criminal informations; 28 convictions; and over $26 million in criminal fines, restitution, and special assessments.

During this reporting period, we examined whether the 2020 trading activities of certain senior Board and Federal Reserve Bank officials violated the law or Federal Reserve policies and whether the trading activities warranted further investigation by other authorities. With a cross-disciplinary OIG team, we conducted a comprehensive review of relevant records and found that the trading activities of the senior Board officials did not violate the laws, rules, regulations, or policies as investigated by our office; the investigation of senior Reserve Bank officials is ongoing.

In other work this reporting period, we completed annual audits of each agency, pursuant to the Federal Information Security Modernization Act of 2014, to determine the effectiveness of the agencies' information security policies, procedures, and processes; we found that both agencies' information security programs continue to operate effectively. We reviewed select information security controls for the Board's Secure Document System, which provides for the secure distribution of Federal Open Market Committee documentation to authorized staff at the Board and the Reserve Banks, and found that overall, the security controls we tested were operating effectively. We also reviewed the software and license asset management processes of the Board's Division of Research and Statistics and determined that the division has not established a software and license inventory and associated review procedures in accordance with agency policy. We conducted a risk assessment of the CFPB's purchase card program and found that the risk of illegal, improper, or erroneous purchase card use is *low*. We assessed the CFPB's preparedness to implement certain components of the Open, Public, Electronic, and Necessary Government Data Act of 2018, which requires federal agencies to create publicly available data inventories and outlines specific duties for federal chief data officers, and found that the agency is generally prepared to implement the act. Finally, we contracted with an independent public accounting firm to audit the CFPB's compliance with the Payment Integrity Information Act of 2019 as it relates to the Civil Penalty Fund for fiscal year 2021; the contractor determined that the CFPB complied with the applicable requirements.

There have been several recent leadership changes at the Board. Lisa Cook, Philip Jefferson, and Michael Barr took office as members of the Board of Governors; the Board now has a full complement and is the most diverse it has been in its 108-year history. We have met with the new governors, and we look forward to continuing to work with leadership at the Board and the CFPB as we provide robust independent oversight to improve their programs and operations and to prevent and detect fraud, waste, and abuse.

It's exciting to look to the future as workplaces evolve and we begin a new era of hybrid work, which aims to facilitate connection and collaboration while also providing staff with autonomy and flexibility. I want to recognize that we could not have reached this moment without the incredible commitment, determination, and resilience of the OIG staff. I cannot overstate my gratitude and admiration for how skillfully and gracefully they handled the many unforeseen challenges of recent years. I am profoundly thankful for every one of them.

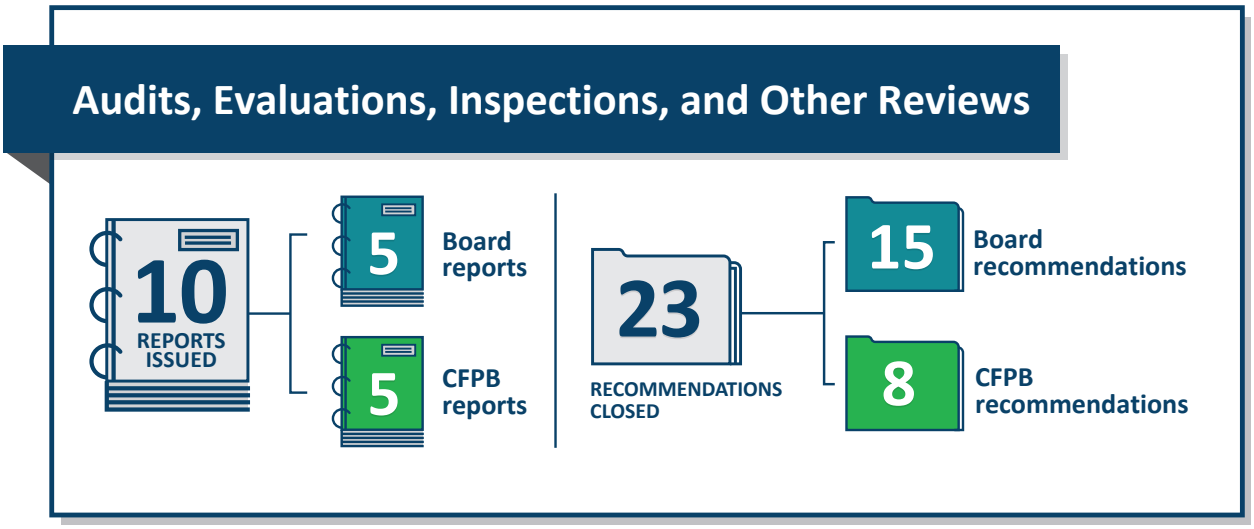
Sincerely,

Mark Bialek
Inspector General
October 31, 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 Consumer Financial Protection Bureau. The following are highlights, in chronological order, of our work during this semiannual reporting period.



Board Trading Activity

Former Vice Chair Richard Clarida's and Chair Jerome Powell's trading activities did not violate the laws, rules, regulations, or policies as investigated by our office.

The Board's Return-to-Office Plan

The Board implemented vaccination, building access, and other return-to-office (RTO) workplace safety measures in a manner consistent with the agency's RTO plan.

The CFPB's Reentry Plan

The CFPB implemented building access and other RTO workplace safety protocols at its headquarters building in a manner consistent with the agency's reentry plan and applicable federal guidance.

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 can strengthen its cybersecurity risk management processes.

The CFPB's Information Security Program

The CFPB's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. The CFPB can strengthen policies, procedures, and processes in the areas of data loss prevention, software asset management, and continuity planning.

Many of our investigations during this semiannual reporting period concern fraud related to the Federal Reserve's pandemic response efforts, including 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, and the Main Street Lending Program (MSLP), which supported lending to small and medium-sized for-profit and nonprofit organizations in sound financial condition before the COVID-19 pandemic. In addition, our office also conducted investigations in support of our membership on the Pandemic Response Accountability Committee (PRAC).

Missouri Business Owner Indicted for $27.1 Million Bank and PPP Fraud

Tod Ray Keilholz, of Missouri, was charged in a 52-count indictment for a $27.1 million bank fraud scheme that included over $12.4 million in PPP loans. The charges include multiple counts of bank fraud, making false statements to a financial institution, making false statements to the SBA, money laundering, and aggravated identity theft.

California Company Chief Executive Officer Pleaded Guilty to $21 Million Cryptocurrency Fraud

Michael Alan Stollery, of California, chief executive officer (CEO) of Titanium Blockchain Infrastructure Services Inc. (TBIS), pleaded guilty for his role in a cryptocurrency fraud scheme involving TBIS's initial coin offering (ICO), which raised about $21 million from investors in the United States and overseas.

Owner of Massachusetts Tech Services Company Sentenced to Prison for $13 Million PPP Fraud

Elijah Majak Buoi, owner of information technology (IT) services company Sosuda Tech, was sentenced in connection with filing fraudulent PPP loan applications seeking more than $13 million. Buoi was sentenced to 39 months in prison and 3 years of supervised release, and he was ordered to pay restitution of $2 million and forfeiture of $2 million.

Former Executive Vice President Pleaded Guilty to Conspiracy to Defraud First NBC Bank in Louisiana

Robert B. Calloway pleaded guilty to conspiracy to defraud New Orleans–based First NBC Bank, where he worked as executive vice president. The bank, which failed in April 2017, was a subsidiary of First NBC Bank Holding Company. According to court documents, Calloway and other bank officers conspired to conceal the financial condition of a borrower from the bank's board of directors, auditors, and examiners; falsely stated in loan documents that the borrower was able to pay his loans with cash generated by his businesses; and concealed the fact that they made loans to the borrower to keep him and his companies off month-end reports that went to the bank's board, auditors, and examiners.

Introduction

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

In accordance with the Inspector General Act of 1978, 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 CFPB programs and operations
- help prevent and detect fraud, waste, abuse, and mismanagement in Board and CFPB programs and operations
- review existing and proposed legislation and regulations to make recommendations about possible improvements to Board and CFPB programs and operations
- keep the Board of Governors, the CFPB director, and Congress fully and currently informed

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

- Section 15010 of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act; 15 U.S.C. § 9001 note) established 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 CFPB's information security programs and practices, including testing the effectiveness of security controls and practices for selected information systems.

- Section 11B of the Federal Reserve Act (12 U.S.C. § 248(b)) mandates annual independent audits of the financial statements of each Federal Reserve Bank and of the Board. The Board performs the accounting function for the Federal Financial Institutions Examination Council (FFIEC), and we oversee the annual financial statement audits of the Board and of the FFIEC.[1] Under the Dodd-Frank Wall Street Reform and Consumer Protection Act, the U.S. Government Accountability Office performs the financial statement audit of the CFPB.
- The Payment Integrity Information Act of 2019 (PIIA; 31 U.S.C. §§ 3351–58) requires agency heads to periodically review and identify programs and activities that may be susceptible to significant improper payments. The CFPB has determined that its Consumer Financial Civil Penalty Fund is subject to the PIIA. The PIIA requires us to determine each fiscal year whether the agency complies with the act.
- The Government Charge Card Abuse Prevention Act of 2012 (5 U.S.C. § 5701 note and 41 U.S.C. § 1909(d)) requires us to conduct periodic risk assessments and audits of the Board's and the CFPB's purchase card, convenience check, and travel card programs to identify and analyze risks of illegal, improper, or erroneous purchases and payments.
- Section 211(f) of the Dodd-Frank 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 apply to the broader financial sector and ways to improve financial oversight.[2] Additionally, CIGFO must report annually about the IGs' concerns and recommendations, as well as issues that may apply to the broader financial sector. CIGFO can also convene a working group of its members to evaluate the effectiveness and internal operations of the Financial Stability Oversight Council, which was created by the Dodd-Frank Act and is charged with identifying threats to the nation's financial stability, promoting market discipline, and responding to emerging risks to the stability of the nation's financial system.

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

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

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

Pandemic Response Oversight

The economic disruptions caused by the COVID-19 pandemic resulted in an abrupt shock to financial markets and affected many credit channels relied on by households, businesses, and state and local governments. In response, the Board took steps to support the flow of credit to U.S. households and businesses. Notably, the Board used its emergency lending authority under section 13(3) of the Federal Reserve Act to create lending programs to ensure liquidity in financial markets and to provide lending support to various sectors of the economy. In addition, the CFPB has continued to play a vital role throughout the pandemic by enforcing federal consumer protection laws and protecting consumers from abuse.

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

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

Status Updates for Completed, Initiated, and Planned Work

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

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

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

The audits and evaluations we have initiated based on these planning activities and their status are outlined 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 evaluation 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 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 reporting phase.

Evaluations 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 (FRB Boston) purchased 1,830 loans worth $17.5 billion from banks and lenders, the majority of which were purchased in the last 2 months of the program. To handle the increase in volume, FRB Boston implemented an expedited loan purchase process

for certain lenders. FRB Boston is now in the process of administering the loans, including assessing overall credit risk and identifying substandard loans. To assist with managing the program, FRB Boston contracted with vendors for a variety of these purchase and administration functions, including purchase intake, credit administration, loan workout, and other services. We are conducting a two-phase assessment of the MSLP loan purchase and administration processes, including the design and operating effectiveness of internal controls. Our loan purchase evaluation is currently in fieldwork, and we plan to begin fieldwork on the loan administration evaluation in the fourth quarter of 2022.

Evaluation of the Board's and the CFPB's RTO Plans

We issued these reports in September 2022; see the summaries of the Board report and the CFPB report below.

Audit of the CFPB's Consumer Response Operations

The CFPB 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, Consumer Response faces an operational risk with respect to the timeliness with which it can respond to consumer complaints. We plan to assess the CFPB'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.

As part of its 2021 audit of the Board's information security program, as required by FISMA, our Office of Information Technology contracted with an independent third-party contractor to evaluate select security controls for a System-managed IT system that processes lending facility data. In addition, as part of its 2022 FISMA audit, the Office of Information Technology reviewed the Board's vendor risk management processes. This audit report was issued in September 2022; see the summary of the report below.

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 133 full investigations; 71 arrests; 48 convictions; and over $40.4 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 CFPB programs and operations. For example, we oversee audits of the Board's financial statements and conduct audits of (1) the efficiency and effectiveness of the Board's and the CFPB's processes and internal controls over their programs and operations; (2) the adequacy of controls and security measures governing these agencies' financial and management information systems and their safeguarding of assets and sensitive information; and (3) compliance with applicable laws and regulations related to the agencies' financial, administrative, and program operations. Our audits are performed in accordance with *Government Auditing Standards*, which is issued by the comptroller general of the United States.

Evaluations and inspections also assess aspects of the economy, efficiency, and effectiveness of Board and CFPB programs and operations. Evaluations are generally focused on the effectiveness of specific programs or functions; we also conduct our legislatively mandated reviews of failed financial institutions supervised by the Board as evaluations. 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

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

2022-IT-B-008R **June 15, 2022**

FISMA requires each agency IG to conduct an annual independent evaluation of the effectiveness of their agency's information security program and practices. This memorandum report provides additional details on our testing of the Board's software and license asset management processes, which we performed as part of our 2021 FISMA audit.

As noted in our FISMA report, we found that a Board division has not established a software and license inventory and associated review procedures in accordance with the agency's *Software Management Policy*. We believe that a software and license catalog, along with software review procedures, will help reduce the risks associated with the introduction and use of software and associated licenses within this division's environment, as well as enhance visibility into the software in use across the Board's network. As such, we made a recommendation to strengthen processes in this area.

Given the sensitivity of the information in our review, our full memorandum report is restricted.

Security Control Review of the Board's Secure Document System

2022-IT-B-009R **June 15, 2022**

FISMA requires each agency IG to conduct an annual independent evaluation of the effectiveness of their agency's information security program and practices. To meet FISMA requirements, we reviewed select information security controls for the Board's Secure Document System (SDS). The SDS provides for the secure distribution of Federal Open Market Committee documentation to authorized staff at the Board and the Reserve Banks.

Overall, we found that the security controls we tested for the SDS were operating effectively. For example, we found that processes for contingency plan testing and alternate storage and processing were operating effectively. Further, we found that access to SDS information was appropriately provisioned. We made a recommendation related to improving the configuration management processes for the SDS application, and we identified a matter for management consideration related to strengthening access controls. The Board concurred with our recommendation.

Given the sensitivity of the information in our review, our full memorandum report is restricted.

OIG Closing of 22-0028-I Board Trading Activity

July 11, 2022

In response to a request from the Board, we initiated separate investigations of Board and Reserve Bank officials' trading activities.

With regard to Board officials, we found that former Vice Chair Richard Clarida's and Chair Jerome Powell's trading activities did not violate the laws, rules, regulations, or policies as investigated by our office. We found, however, that (1) former Vice Chair Clarida failed to report several trades on his 2019 and 2020 Office of Government Ethics Forms 278 as required by Office of Government Ethics regulation 5 C.F.R. part 2634 and (2) on behalf of a Powell family trust, in December 2019, a trust financial advisor

executed five trades during a Federal Open Market Committee trading blackout period. The investigation of senior Reserve Bank officials is ongoing.

The Board Implemented Safety Measures in a Manner Consistent With Its Return-to-Office Plan

2022-MO-B-010 **September 7, 2022**

In response to the COVID-19 pandemic, the Board established a core group of senior leaders to monitor COVID-19 pandemic developments and hired a public health expert. The core group of senior leaders, along with the public health expert and in consultation with the Executive Committee, the Senior Officer Committee, the Board chair, and the administrative governor, developed the Board's RTO plan. We assessed select vaccination, building access, and other RTO workplace safety measures put in place by the Board to ensure that the measures were implemented in a manner consistent with the agency's RTO plan.

For the select workforce safety measures we assessed, we found that the Board's actions aligned with its RTO plan and the external guidance referenced in the RTO plan. The Board implemented enhanced cleaning and air filtration practices and social distancing measures in its owned facilities and oversaw the implementation of these measures in its leased facilities. The Board also implemented building access controls, including a process to prevent unvaccinated individuals from accessing its facilities without preapproval and a process to monitor the number of employees in its facilities. Although our report does not contain any recommendations, it includes a matter for management consideration related to memorializing the key stakeholders that contributed to the Board's decisionmaking processes during its COVID-19 response and the implementation of its RTO plan.

2022 Audit of the Board's Information Security Program

2022-IT-B-013 **September 30, 2022**

The Office of Management and Budget's (OMB) fiscal year 2022 guidance for FISMA reporting directs IGs to evaluate the maturity level (from a low of 1 to a high of 5) of their agency's information security program across several core areas. These core areas align with the requirements in Executive Order 14028, *Improving the Nation's Cybersecurity*, as well as recent OMB guidance on modernizing federal cybersecurity. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security. We assessed 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, we found that the Board has developed a strategy for implementing a zero trust architecture in accordance with Executive Order 14028 and has continued

implementing the U.S. Department of Homeland Security's Continuous Diagnostics and Mitigation program, which provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their respective security posture. However, the Board can strengthen its cybersecurity risk management processes.

The Board has taken sufficient actions to close three of the nine recommendations from our prior FISMA audit reports that were open at the start of this audit. This report contains one new recommendation and one matter for management consideration designed to strengthen the Board's information security program in the area of cybersecurity risk management. The Board concurred with our recommendation.

Consumer Financial Protection Bureau

Independent Accountants' Report on the Bureau's Fiscal Year 2021 Compliance With the Payment Integrity Information Act of 2019

2022-FMIC-C-007 **April 27, 2022**

The PIIA requires agency heads to periodically review and identify all programs and activities that may be susceptible to significant improper payments. In addition, each fiscal year the IG of each agency must determine and report on whether the agency complies with the act. We contracted with an independent public accounting firm to audit the CFPB's compliance with the PIIA for the Civil Penalty Fund for fiscal year 2021. The audit was performed in accordance with *Government Auditing Standards* issued by the comptroller general of the United States. We reviewed and monitored the work of the firm to ensure compliance with the contract and *Government Auditing Standards*.

The firm determined that the CFPB complied with the two applicable requirements of the PIIA for fiscal year 2021 for the Civil Penalty Fund. Specifically, the CFPB published and posted on its website an annual financial statement for the most recent fiscal year, and it conducted a program-specific risk assessment. The other four PIIA requirements are not applicable to the Civil Penalty Fund because the CFPB has determined that the fund is not susceptible to significant improper payments. The firm made no recommendations in its report.

Fiscal Years 2020 and 2021 Risk Assessment of the Bureau's Purchase Card Program

August 31, 2022

CFPB purchase cards were used for about $3.5 million in total program spending in fiscal years 2020 and 2021. We analyzed the risks of illegal, improper, or erroneous purchases and payments.

The results of our assessment show that the risk of illegal, improper, or erroneous use in the CFPB's purchase card program is *low*. A risk level of *low* means that illegal, improper, or erroneous use is unlikely to occur and that such an occurrence would be expected to have a minimal effect on current operations and long-term objectives. As a result of the low risk level, we will not recommend that an audit of the program for fiscal year 2022 be included in our 2023 annual audit plan.

The CFPB Implemented Safety Measures in Accordance With Its Reentry Plan

2022-MO-C-011 **September 21, 2022**

In March 2020, the CFPB director communicated to staff that the agency was monitoring COVID-19 developments and taking measures to increase employee safety. The CFPB's initial measures in response to COVID-19 included developing a pandemic plan and a reentry plan. We assessed building access and other RTO workplace safety protocols implemented by the CFPB at its headquarters building to ensure that those measures were implemented in a manner consistent with the agency's reentry plan.

We found that the CFPB's safety measures aligned with applicable federal guidance and the agency's reentry plan. The CFPB implemented enhanced cleaning and air filtration practices in its headquarters building; social distancing measures to increase employee safety at headquarters during periods of mandatory and maximum telework; and building access controls, including monitoring the number of individuals in the headquarters building. Our report does not contain recommendations.

The CFPB Is Generally Prepared to Implement the OPEN Government Data Act and Can Take Additional Steps to Further Align With Related Requirements

2022-MO-C-012 **September 28, 2022**

The Open, Public, Electronic, and Necessary Government Data Act of 2018 (OPEN Government Data Act) is focused on improving the availability, transparency, and quality of federal data; it also adds new requirements relating to data governance, data management, and transparency processes. The CFPB's Office of the Chief Data Officer has primary responsibility for ensuring that the agency complies with the OPEN Government Data Act and other related requirements. We assessed the CFPB's compliance with finalized OMB guidance on OPEN Government Data Act requirements, examined the agency's readiness to implement the act's draft guidance, and identified lessons learned from other federal organizations that may enhance the CFPB's readiness to implement the act.

The CFPB generally complies with finalized OMB phase I guidance related to the OPEN Government Data Act. In addition, we found that the CFPB continues to make progress and is generally prepared to

implement draft OMB phase II guidance related to the act, once finalized. However, the CFPB can take additional steps to further align with requirements of the OPEN Government Data Act and related phase I and phase II guidance. Specifically, we found that the CFPB can enhance its data governance by making some technical updates to its *Policy on Information Governance* to reflect the agency's current operating structure. Additionally, the CFPB will obtain additional organizational benefits by preparing a draft strategic information resources management plan to more readily comply with phase II guidance, once finalized.

We made two recommendations to enhance the CFPB's preparedness to implement the requirements of the OPEN Government Data Act and related guidance. The CFPB concurred with our recommendations.

2022 Audit of the CFPB's Information Security Program

2022-IT-C-014 September 30, 2022

OMB's fiscal year 2022 guidance for FISMA reporting directs IGs to evaluate the maturity level (from a low of 1 to a high of 5) of their agency's information security program across several core areas. These core areas align with the requirements in Executive Order 14028, *Improving the Nation's Cybersecurity*, as well as recent OMB guidance on modernizing federal cybersecurity. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security. We assessed the effectiveness of the CFPB's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The CFPB's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. Since our review last year, we found that the CFPB has developed its zero trust strategy implementation plan, which outlines the various initiatives and budgetary requirements for the implementation of the agency's zero trust architecture by fiscal year 2024. In addition, we found that the CFPB has improved its maturity in the areas of information security continuous monitoring and supply chain risk management. However, the CFPB can strengthen policies, procedures, and processes in the areas of data loss prevention, software asset management, and continuity planning to ensure that its program remains effective.

The CFPB has taken sufficient actions to close recommendations related to system authorization and change control processes from our prior FISMA audit reports that were open at the start of this audit. This report includes six new recommendations designed to strengthen the CFPB's information security program in the areas of data protection and privacy, software asset management, and continuity planning. Our report also includes a matter for management consideration related to the development of procedures for using a third-party service to monitor vendors' compliance with the CFPB's cybersecurity requirements. The CFPB 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 CFPB employees as well as alleged misconduct or criminal activity that affects the Board's or the CFPB's ability to effectively supervise and regulate the financial community. We operate under statutory law enforcement authority granted by the U.S. attorney general, which vests our special agents with the authority to carry firearms, to seek and execute search and arrest warrants, and to make arrests without a warrant in certain circumstances. Our investigations are conducted in compliance with *Quality Standards for Investigations*, issued by CIGIE, and *Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority*.

During this period, the Office of Investigations met with officials at both the Board and the CFPB 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, known as *state member banks*. Under delegated authority from the Board, the Reserve Banks supervise bank holding companies and state member banks, and the Board's Division of Supervision and Regulation oversees the Reserve Banks' supervisory activities.

Our investigations concerning bank holding companies and state member banks typically involve allegations that senior officials falsified financial records, lied to or misled examiners, or obstructed examinations 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 before 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. Our office is also part of the DOJ's COVID-19 Fraud Enforcement Task Force.

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

Missouri Business Owner Indicted for $27.1 Million Bank and PPP Fraud

Tod Ray Keilholz, of Missouri, was charged in a 52-count indictment for a $27.1 million bank fraud scheme that included over $12.4 million in PPP loans. The charges include multiple counts of bank fraud, making false statements to a financial institution, making false statements to the SBA, money laundering, and 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 indictment, Keilholz was the sole owner of TRK Construction, TRK Valpo, TL Builders, and Project Design. In multiple PPP loan applications, he allegedly made false claims and used bogus documents to inflate the incomes of his businesses and to claim payrolls for employees who did not exist or no longer worked for him. He received over $12.4 million in PPP loans as a result of his scheme. His subsequent PPP loan applications, for potentially more than $13 million, were denied. Rather than use the proceeds for payroll and other business expenses as required, Keilholz paid down debts—including an unrelated bank loan and line of credit totaling $3.5 million that he also allegedly obtained through fraud—and funneled $325,000 to his wife, a Missouri state government employee.

This case is being investigated by our office, the Federal Bureau of Investigation (FBI), Internal Revenue Service (IRS) Criminal Investigation (CI), the SBA OIG, and the U.S. Treasury Inspector General for Tax Administration (TIGTA). It is being prosecuted by the U.S. Attorney's Office for the Western District of Missouri.

CEO of California Company Pleaded Guilty to $21 Million Cryptocurrency Fraud

Michael Alan Stollery, of California, CEO of TBIS, pleaded guilty for his role in a cryptocurrency fraud scheme involving TBIS's ICO, which raised about $21 million from investors in the United States and overseas.

Stollery was the CEO and founder of TBIS, a purported cryptocurrency investment platform. He touted TBIS as a cryptocurrency investment opportunity, luring investors to purchase BARs, the cryptocurrency token or coin offered by TBIS's ICO, through a series of false and misleading statements. Although he was required to do so, Stollery did not register the ICO with the U.S. Securities and Exchange Commission,

nor did he have a valid exemption from the commission's registration requirements. To entice investors, Stollery falsified aspects of TBIS's white papers, which purportedly offered investors and prospective investors an explanation of the cryptocurrency investment offering, including the purpose and technology behind the offering, how the offering was different from other cryptocurrency opportunities, and the prospects for the offering's profitability. Stollery also planted fake client testimonials on TBIS's website and falsely claimed that he had business relationships with the Federal Reserve and dozens of prominent companies to create the false appearance of legitimacy. Stollery further admitted that he did not use the invested money as promised but instead commingled the ICO investors' funds with his personal funds, using at least a portion of the offering proceeds for expenses unrelated to TBIS, such as credit card debt and bills for his Hawaii condominium.

This case was investigated by our office and the FBI. It is being prosecuted by the DOJ Criminal Division.

Owner of Massachusetts Tech Services Company Sentenced to Prison for $13 Million PPP Fraud

Elijah Majak Buoi, owner of IT services company Sosuda Tech, was sentenced in connection with filing fraudulent PPP loan applications seeking more than $13 million. Buoi was sentenced to 39 months in prison and 3 years of supervised release, and he was ordered to pay restitution of $2 million and forfeiture of $2 million.

Buoi devised a scheme to obtain PPP funds by repeatedly filing false and fraudulent loan applications in which he systematically used false tax documents and payroll processing records until he was ultimately awarded a loan. As a result of his scheme, Buoi obtained a $2 million PPP loan. The government recovered about $1.97 million of the loan funds.

This case was investigated by our office, the FBI, the Federal Deposit Insurance Corporation (FDIC) OIG, and the IRS CI. It was prosecuted by the U.S. Attorney's Office for the District of Massachusetts and the DOJ Criminal Division.

New York–Florida Resident Sentenced to Prison for $6.8 Million PPP Fraud

Gregory J. Blotnick, a dual New York and Florida resident, was sentenced to 51 months in prison for his role in a scheme to fraudulently obtain over $6.8 million in PPP loans. He was also sentenced to 2 years of supervised release and ordered to pay restitution of $4,577,631.

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. He falsified various pieces of information to the lenders, including the number of employees, federal tax returns, and payroll

documentation. Based on these misrepresentations, the lenders provided his purported business with about $4.6 million in PPP loans. Blotnick then transferred most of the funds to brokerage accounts and lost more than $3 million in stock trades.

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

California Resident Pleaded Guilty to $6.6 Million PPP Fraud

Muhammad Noor Ul Ain Atta, of California, pleaded guilty to a two-count criminal information charging him with wire fraud and laundering of monetary instruments in connection with a scheme to submit false loan applications that brought him more than $6.6 million in Economic Injury Disaster Loan (EIDL) and PPP funds.

Atta submitted 11 fraudulent PPP loan applications for 7 of his shell companies. The fraudulent PPP loan applications misrepresented the number of employees and the average monthly payroll expenses of his companies and falsely certified that he would use the loan proceeds for permissible business purposes. Atta also submitted false tax and payroll documentation in support of his applications. In total, Atta received $6,643,540 in loan proceeds. Atta then laundered loan proceeds and deposited them in bank accounts in the United States and Pakistan.

This case was investigated by our office, the IRS CI, the SBA OIG, and TIGTA. It is being prosecuted by the U.S. Attorney's Office for the Central District of California and by the DOJ Fraud Section.

Florida Resident Charged in $6 Million PPP Fraud

Ego Ferguson, of Florida, was charged by indictment with wire fraud and engaging in financial transactions in criminally derived property in connection with a $6 million PPP fraud scheme. 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 in the indictment, Ferguson caused the preparation and submission of fraudulent PPP loan applications on behalf of various companies. The applications contained falsely certified numbers of employees and employee payrolls. Ferguson also provided fraudulent IRS forms indicating that the companies paid employee wages and taxes, when in fact the companies had not. Ferguson charged a fee of 20 percent for these loans and maintained a spreadsheet showing the submission of apparent PPP loans totaling over $6 million.

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

Oklahoma Resident Sentenced to Prison for $5.4 Million PPP Fraud

Olusola Ojo, of Oklahoma, was sentenced to 48 months in prison, followed by 5 years of supervised release, and ordered to pay $150,000 in restitution and a $400 special assessment. Ojo was previously found guilty of one count of bank fraud conspiracy, two counts of bank fraud, and one count of aggravated identity theft. 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 was prosecuted by the U.S. Attorney's Office for the Northern District of Oklahoma.

California Business Owner Sentenced to Prison for Embezzling $4.8 Million and for PPP Fraud

Kevin Lee Co, of California, was sentenced to 10 years in prison after pleading guilty to wire fraud, money laundering, and submitting false statements to a financial institution.

Co embezzled about $4.8 million from his former employer and used the money to purchase, among other things, luxury cars, home furniture, and season tickets to professional football and basketball games, and spent $1 million on the online video game *Game of War*. While out of custody and awaiting sentencing on those charges, Co defrauded federally insured financial institutions by submitting false statements to qualify for PPP loans for his company, Apollo HP. Co failed to disclose his pending criminal charges and guilty pleas as required, and two banks approved loans for his company. As a result, the financial institutions suffered a total loss of $530,552.

This case was investigated by our office, the FBI, and the IRS CI. It was prosecuted by the U.S. Attorney's Office for the Eastern District of California.

Oklahoma Couple Pleaded Guilty to $2.7 Million PPP Fraud

Spouses William Mark Sullivan and Michelle Cadman-Sullivan, of Oklahoma, each pleaded guilty to conspiracy to commit bank fraud after attempting to obtain a $2.7 million PPP loan. Their plea

agreements call for the defendants to pay restitution of $114,282 to Arvest Bank in Tulsa, Oklahoma, and $628,645 to The Exchange Bank in Skiatook, Oklahoma, for a total of $742,927 in proceeds illegally obtained by the defendants. The couple was previously indicted and charged with bank fraud conspiracy. In addition, Cadman-Sullivan was charged with four counts of aggravated identity theft.

According to the allegations, the couple fraudulently applied for six PPP loans totaling more than $2.7 million at Arvest Bank and The Exchange Bank. They created bogus businesses—Oklahoma Paving, U.S. Central Construction, USA-1 Construction, and Oklahoma Energy—and falsified employee counts and payroll expenses on their loan applications. They also failed to disclose to the banks that they were submitting duplicative and overlapping applications. The couple admitted to transferring the $742,927 in funds they received to various bank accounts and using the funds for personal expenses.

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.

Owner of Massachusetts Company Agreed to Plead Guilty to $2.5 Million PPP Fraud

Vinicius Santana, a Florida resident and owner of Massachusetts-based painting company Complete Home Care, has been charged with and has agreed to plead guilty to filing fraudulent applications to obtain $2.5 million in PPP loan funds.

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

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

New Jersey Business Owner Admits to $1.8 Million PPP Fraud

Rocco A. Malanga, a businessman formerly of New Jersey, pleaded guilty to one count of bank fraud and one count of money laundering and admitted to fraudulently obtaining nearly $1.8 million in federal PPP loans.

Malanga fraudulently submitted at least three PPP loan applications to three lenders on behalf of three business entities. In the applications, he fabricated the number of individuals employed by each business

entity as well as average monthly payrolls. Malanga then diverted some of the proceeds from the loans to fund a business that did not receive PPP loan funds.

This case was investigated by our office, the FDIC OIG, the IRS CI, and the SSA OIG. It is being prosecuted by the U.S. Attorney's Office for the District of New Jersey and the DOJ Criminal Division.

Pennsylvania Resident Charged in $1.7 Million PPP Fraud

Darryl Duanne Young, of Pennsylvania, was charged for his role in a scheme to fraudulently obtain over $1.7 million in federal PPP loans for himself and others. Specifically, he was charged with one count of conspiracy to commit bank fraud, four counts of bank fraud, and two counts of money laundering. 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 court documents, Young submitted and directed others to submit fraudulent PPP loan applications, supported by falsified tax documents and bank statements, to a victim lender. He received over $230,000 in PPP loans for businesses he controlled and received a percentage of loan proceeds for his help in submitting fraudulent applications on behalf of others.

This case is being investigated by our office, the FDIC OIG, the FHFA OIG, Homeland Security Investigations, the IRS CI, the SSA OIG, and the USPIS. It is being prosecuted by the U.S. Attorney's Office for the District of New Jersey.

Florida Man Charged in $1.6 Million EIDL and PPP Fraud

Mohamed A. Awad, of Florida, was charged with two counts of wire fraud for his role in a scheme to fraudulently obtain over $1.6 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 court documents, Awad engaged in a scheme to illegally obtain the loans through numerous misrepresentations to lenders. He submitted fraudulent loan applications with fabricated employee numbers, bogus tax documents, and other misrepresented company information. Awad transferred the loan proceeds to various bank accounts he controlled, withdrawing significant amounts in cash and transferring at least $760,000 to banks based in Egypt.

This case is being investigated by our office, the FBI, the FDIC OIG, the IRS CI, the USPIS, and the SSA OIG. It is being prosecuted by the U.S. Attorney's Office for the District of New Jersey.

Massachusetts Resident Charged in $1.5 Million EIDL and PPP Fraud

Joao Mendes, of Massachusetts, pleaded guilty to one count of wire fraud in connection with a scheme to submit false applications to obtain over $1.5 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 charging documents, Mendes submitted or caused to be submitted multiple fraudulent EIDL and PPP loan applications on behalf of various entities. The fraudulent PPP loan applications misrepresented the number of employees and the average monthly payroll expenses of Mendes's various businesses. He also allegedly submitted false tax records in support of his loan applications. As a result of the fraudulent applications, Mendes and others received over $1.5 million in EIDL and PPP funds. Once Mendes received the funds, he spent them for his personal benefit, including purchasing cryptocurrency; transferred funds to other accounts he controlled; and transferred funds to other individuals.

The case is being investigated by our office, the FBI, the FDIC OIG, the FHFA OIG, the IRS CI, the SBA OIG, TIGTA, and the USPIS. It is being prosecuted by the U.S. Attorney's Office for the District of Massachusetts and the DOJ Criminal Division.

California Couple Charged in $1.4 Million PPP Fraud

Spouses Christopher A. Mazzei and Erin V. Mazzei, of California, were charged by a federal grand jury with a four-count indictment that included wire fraud, money laundering, and conspiracy in connection with a $1.4 million PPP fraud scheme. The fact that a defendant has been charged with a crime is merely an accusation, and a defendant is presumed innocent until and unless proven guilty.

The indictment alleges that the Mazzeis submitted applications for PPP funds to a Hawaii financial institution and two other financial institutions on behalf of three purported businesses, each time using interstate wires. For each application, the Mazzeis allegedly created false IRS tax returns and payroll records, which they presented as authentic and submitted to the banks to support their loan applications. As a result of the false and fraudulent applications, the Mazzeis received $1,365,000 in PPP loan funds, which they then used for personal purposes, including purchasing multiple sport utility vehicles and a home in Hawaii, among other things.

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

Kentucky Businessowner Sentenced to Prison for $1.3 Million PPP Fraud

Randall "Rocky" Blankenship Jr., owner of several Kentucky business entities, was sentenced to 42 months in federal prison after pleading guilty to conspiracy to commit wire fraud to obtain PPP loans under false pretenses. Upon his release from prison, he will be under the supervision of the U.S. Probation Office for 3 years. He also agreed to pay restitution of $1,323,829 and a $30,000 fine.

Blankenship, with the help of a certified public accountant, created fake tax documents and payroll records indicating that his businesses—Blankenship RV Finance Solutions, RSGG Properties, RSGG Holdings, and RSGG Investments—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 over $1.3 million in loans. Blankenship used some of the funds for his recreational vehicle business (which had already received a PPP loan and was ineligible for additional loans at the time) and for his personal use, including paying off casino debt and purchasing real estate.

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

Former Executive Vice President Pleaded Guilty to Conspiracy to Defraud First NBC Bank in Louisiana

Robert B. Calloway pleaded guilty to conspiracy to defraud New Orleans–based First NBC Bank, where he worked as executive vice president. The bank, which failed in April 2017, was a subsidiary of First NBC Bank Holding Company, a Board-supervised bank holding company.

According to court documents, Calloway and other bank officers conspired to conceal the financial condition of a borrower from the bank's board of directors, auditors, and examiners. The coconspirators falsely stated in loan documents that the borrower was able to pay his loans with cash generated by his businesses, hiding the fact that the borrower was only making his existing loan payments by getting new loans from the bank. Calloway and others also concealed the fact that they made loans to the borrower to keep him and his companies off month-end reports that went to the bank's board, auditors, and examiners. These month-end reports listed borrowers who were not paying their loans or whose accounts were overdrawn. By keeping the borrower and his entities off those reports, Calloway and others were able to hide their scheme and keep lending to the borrower despite the borrower's inability to pay his loans. Calloway also completed loan review forms that went to external auditors in which he omitted material information about the borrower and his inability to pay his loans.

This case was 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.

Former Chief Credit Officer Pleaded Guilty to Conspiracy to Defraud First NBC Bank in Louisiana

William J. Burnell pleaded guilty to conspiracy to defraud New Orleans–based First NBC Bank, where he worked as chief credit officer. The bank, which failed in April 2017, was a subsidiary of First NBC Bank Holding Company, a Board-supervised bank holding company.

According to court documents, Burnell was responsible for compiling month-end reports listing overdrawn borrowers and past-due loans. Burnell was also responsible for approving credit risk ratings before the bank decided to lend to its customers. As chief credit officer, Burnell was relied on by the bank's board of directors, external auditors, and federal and state regulators to inform them about problems with the bank's asset quality, including its loans. Nevertheless, Burnell conspired with other First NBC Bank officers to defraud the bank by concealing material information about borrowers.

This case was 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 Residents Sentenced for PPP Fraud

Aleta Necole Thomas was sentenced to 30 months in federal prison, followed by 5 years of supervised release, for her role in leading two others in a scheme to apply for almost $800,000 in PPP loans. Katrina West and Pepper Jones were each sentenced to 2 years' probation. The three will pay restitution of $774,753.50. The government previously seized about $210,991 from bank accounts held by Thomas pursuant to federal seizure warrants, which will go toward restitution. Thomas previously pleaded guilty to two counts of making false statements to a financial institution; West and Jones each pleaded guilty to one count of making false statement.

Thomas submitted false statements and reports to Cross River Bank when she applied for a PPP loan. She submitted a borrower application form falsely stating that Coming Correct Community Ministry had an average monthly payroll of $35,000. She further claimed she had 26 employees, for whom she paid payroll taxes, or independent contractors and submitted additional false documentation, including IRS forms. In addition, Thomas submitted false statements and reports to First Electronic Bank in applying for a PPP loan in which she made similar claims.

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

Nevada Resident Sentenced to Prison for PPP Fraud While on Pretrial Release for Attempted Robbery Charge

Keyawn Lloyd Cook Jr., of Nevada, was sentenced to 1 year and 9 months in prison after pleading 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.

Cook, while on pretrial release for an attempted robbery charge, submitted at least five fraudulent loan applications over a 15-month period for EIDL and PPP loans. Cook submitted applications in the names of multiple nonexistent businesses he claimed to operate in various industries. Cook falsely claimed to have 9 to 12 employees in the EIDL loan applications and he falsely claimed gross revenues of $50,000 for a bogus barber shop in the PPP loan application. 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, the IRS CI, and the SBA OIG. It was prosecuted by the U.S. Attorney's Office for the District of Nevada.

Nevada Felon Sentenced to Prison for Unlawful Possession of a Stolen Firearm and for EIDL and PPP Fraud

Darnele Javoris Nelson, also known as Ricky Ellis and Gamarmaurice Newson, of Nevada, was sentenced to 4 years in prison followed by 3 years of supervised release after pleading guilty to one count of felon in possession of a firearm and one count of wire fraud for submitting fraudulent EIDL and PPP loan applications.

Nelson has prior felony convictions for robbery and vehicular manslaughter in California, felony assault with a deadly weapon in California, and possession of 15 or more unauthorized access devices in New York. He is prohibited by law from possessing a firearm. In 2019, he was a passenger in a car in which police found a stolen, loaded semiautomatic handgun with an extended magazine. While on both supervised release and pretrial release, Nelson submitted at least three EIDL applications to the SBA for about $30,000 and at least one PPP loan application for $20,833. In all four applications, Nelson falsely stated that he was the proprietor of several fictitious companies; he reported false revenues and numbers of employees and stated that he was not facing felony charges or serving parole or probation for a felony conviction.

This case was investigated by our office; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the FBI; the IRS CI; the Las Vegas Metropolitan Police Department; and the SBA OIG. It was prosecuted by the U.S. Attorney's Office for the District of Nevada.

Oklahoma Resident Pleaded Guilty to PPP Fraud

Ladawn Pinkney, of Oklahoma, pleaded guilty to one count of wire fraud for her role in a PPP fraud scheme. Pinkney was previously indicted by a grand jury in the Northern District of Oklahoma and charged with four counts of wire fraud.

Pinkney admitted to submitting two fraudulent PPP loan applications to Fountainhead SBF containing false representations that she owned an established business. She then received about $41,666, which she deposited into her own bank account; she did not use the funds for the purposes represented in the PPP loan applications. Pinkney later submitted false and fraudulent loan forgiveness applications to the SBA, and the loans were forgiven.

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

Nevada Felon Pleaded Guilty to Unlawful Possession of Ammunition and PPP Fraud

Jonathan Millard Robinson, of Nevada, pleaded guilty to unlawful possession of ammunition and fraudulently submitting a PPP loan application.

Robinson, who was already on supervised release, admitted that he was previously convicted in North Carolina of conspiracy to distribute cocaine base and distributing cocaine. Both convictions are felonies that prohibit him by law from possessing ammunition. Robinson fraudulently submitted a PPP loan application to a lender to obtain about $20,833. In the application, Robinson falsely stated that he was the proprietor of a company, which did not in fact exist; reported false revenue derived from the fake company; and falsely denied that he was serving parole or probation for a prior felony conviction.

This case was investigated our office; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the FBI; the IRS CI; the Las Vegas Metropolitan Police Department; and the SBA OIG. It is being prosecuted by the U.S. Attorney's Office for the District of Nevada.

Former Bank Employee Pleaded Guilty to Embezzlement in Oklahoma

Mary Jayne Masters, a former employee of an Arvest Bank branch in Oklahoma, pleaded guilty to one count of bank theft for her role in embezzling $13,450 from the state member bank.

Masters admitted that on more than 20 occasions, she manipulated cash currency straps and removed $20 bills from them or replaced the $20 bills with $1 bills with the intent to steal money that was in the

care, custody, and control of Arvest Bank. The thefts were discovered after Arvest Bank deposited the cash straps in question with a Reserve Bank.

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

Consumer Financial Protection Bureau

Title X of the Dodd-Frank Act created the CFPB to implement and enforce federal consumer financial law. The CFPB 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 CFPB'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 CFPB's responsibilities typically involve allegations that company directors or officers provided falsified business data and financial records to the CFPB, lied to or misled examiners, or obstructed examinations in a manner that may have affected the CFPB's ability to carry out its supervisory responsibilities. Such activity may result in criminal violations, such as false statements or obstruction of examinations.

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

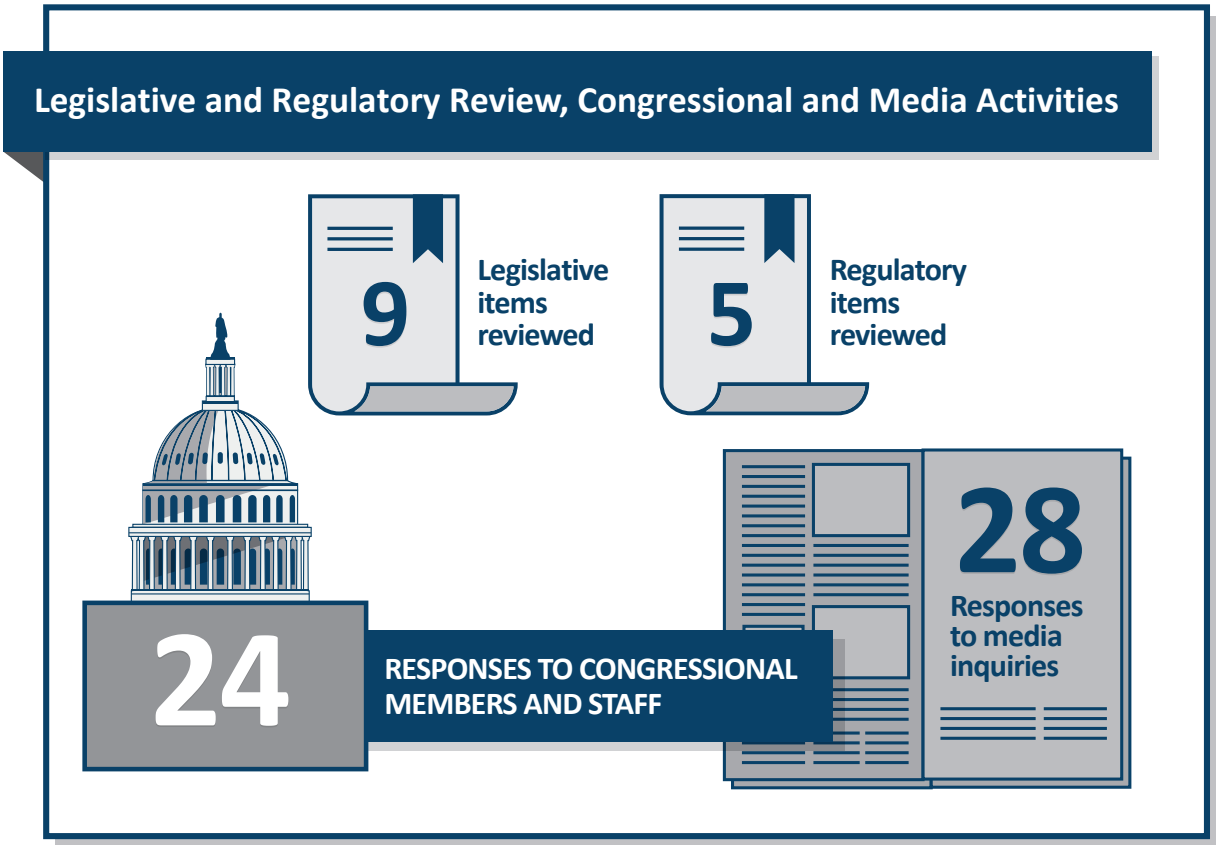
Hotline

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

During this reporting period, the OIG Hotline received 76 complaints. Complaints within our purview are evaluated and, when appropriate, referred to the relevant component within the OIG for audit, evaluation, investigation, or other review. Some complaints convey concerns about matters within the responsibility of other federal agencies or matters that should be addressed by a program or operation of the Board or the CFPB. We refer such complaints to the appropriate federal agency for evaluation and resolution.

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

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



Legislative and Regulatory Review

Our Office of Legal Services 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 CFPB.

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 CFPB's programs and operations. During this reporting period, Legal Services reviewed 9 legislative items and 5 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 24 responses to congressional members and staff concerning the Board and the CFPB. Additionally, we responded to 28 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 almost 24,000 reports, detailing for fiscal year 2022 alone almost $55 billion in potential savings and over 5,000 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, Inclusion, and Accessibility Work Group. The Diversity, Equity, Inclusion, and Accessibility Work Group works to affirm, advance, and augment CIGIE's commitment to promote a diverse, equitable, inclusive, and accessible workforce and workplace environment throughout the OIG community.

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

Our Office of Information Technology plays a key role on the Information Technology Committee of the Federal Audit Executive Council and works with IT audit staff throughout the OIG community 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.
- In June 2022, we completed a peer review of the Pension Benefit Guaranty Corporation (PBGC) OIG audit organization. The PBGC OIG received a peer review rating of *pass*. There were no report recommendations, nor were any recommendations pending from any previous peer reviews of the PBGC OIG audit 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
Testing Results for the Board's Software and License Asset Management Processes	Testing
Security Control Review of the Board's Secure Document System	Audit
OIG Closing of 22-0028-I Board Trading Activity	Review
The Board Implemented Safety Measures in a Manner Consistent With Its Return-to-Office Plan	Evaluation
2022 Audit of the Board's Information Security Program	Audit
Total number of audit reports: 2 Total number of evaluation reports: 1 Total number of other reports: 2	

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

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
2016 Audit of the Board's Information Security Program	11/16	9	9	0	09/22	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	05/22	7	1
2017 Audit of the Board's Information Security Program	10/17	9	9	0	09/22	8	1
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	09/22	5	1
The Board Can Strengthen Information Technology Governance	11/18	6	6	0	06/20	3	3
The Board's Law Enforcement Operations Bureau Can Improve Internal Processes	09/19	6	6	0	06/22	6	0

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
2019 Audit of the Board's Information Security Program	10/19	6	6	0	09/22	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	09/22	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	09/22	10	0
2020 Audit of the Board's Information Security Program	11/20	4	4	0	09/22	3	1
The Board Economics Divisions Can Enhance Some of Their Planning Processes for Economic Analysis	02/21	6	6	0	09/22	6	0
The Board's Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced	09/21	3	3	0	06/22	1	2
The Board Can Improve the Efficiency and Effectiveness of Certain Aspects of Its Consumer Compliance Examination and Enforcement Action Issuance Processes	10/21	10	10	0	08/22	8	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
2021 Audit of the Board's Information Security Program	10/21	2	2	0	09/22	2	0
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
The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems	03/22	3	3	0	n.a.	0	3
Testing Results for the Board's Software and License Asset Management Processes (nonpublic)	06/22	1	1	0	n.a.	0	1
Security Control Review of the Board's Secure Document System (nonpublic)	06/22	1	1	0	n.a.	0	1
2022 Audit of the Board's Information Security Program	09/22	1	1	0	n.a.	0	1

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

n.a. not applicable.

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

Report title	Type of report
Independent Accountants' Report on the Bureau's Fiscal Year 2021 Compliance With the Payment Integrity Information Act of 2019	Audit
Fiscal Years 2020 and 2021 Risk Assessment of the Bureau's Purchase Card Program	Risk assessment
The CFPB Implemented Safety Measures in Accordance With Its Reentry Plan	Evaluation
The CFPB Is Generally Prepared to Implement the OPEN Government Data Act and Can Take Additional Steps to Further Align With Related Requirements	Evaluation
2022 Audit of the CFPB's Information Security Program	Audit
Total number of audit reports: 2 Total number of evaluation reports: 2 Total number of other reports: 1	

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

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
2014 Audit of the CFPB's Information Security Program	11/14	3	3	0	09/22	2	1
2017 Audit of the CFPB's Information Security Program	10/17	7	7	0	09/22	5	2
The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data	01/18	11	11	0	08/22	10	1
2018 Audit of the Bureau's Information Security Program	10/18	4	4	0	09/22	2	2
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	6	1
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
2020 Audit of the Bureau's Information Security Program	11/20	1	1	0	09/22	1	0
The Bureau Can Strengthen Its Hiring Practices and Can Continue Its Efforts to Cultivate a Diverse Workforce	03/21	10	10	0	09/22	1	9

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Bureau Can Improve Its Controls for Issuing and Managing Interagency Agreements	07/21	6	6	0	09/22	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	09/22	0	3
The Bureau Can Improve Aspects of Its Quality Management Program for Supervision Activities	11/21	9	9	0	08/22	5	4
The Bureau Can Further Enhance Certain Aspects of Its Approach to Supervising Nondepository Institutions	12/21	5	5	0	09/22	1	4
The CFPB Is Generally Prepared to Implement the OPEN Government Data Act and Can Take Additional Steps to Further Align With Related Requirements	09/22	2	2	0	n.a.	0	2
2022 Audit of the CFPB's Information Security Program	09/22	6	6	0	n.a.	0	6

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

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

Note: Because the Board and the CFPB are primarily regulatory and policymaking agencies, our recommendations typically focus on program effectiveness and efficiency, as well as strengthening internal controls. As such, the monetary benefit associated with their implementation typically is not readily quantifiable. In the event that an audit, 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	145
Investigations opened during the reporting period	52
Investigations closed during the reporting period	28
Investigations open at end of the reporting period	169
Investigative results for the reporting period	
Persons referred to DOJ prosecutors	17
Persons referred to state/local prosecutors	0
Declinations received	12
Joint investigations	138
Reports of investigation issued	2
Oral and/or written reprimands	0
Terminations of employment	0
Arrests	24
Suspensions	0
Debarments	1
Prohibitions from banking industry	3
Indictments	14
Criminal informations	19
Criminal complaints	6
Convictions	28
Civil actions	$0

See notes at end of table.

Investigative actions	Number or dollar value[a]
Administrative monetary recoveries and reimbursements	$0
Civil judgments	$225,000
Criminal fines, restitution, and special assessments	$26,643,237
Forfeiture	$2,961,294

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	8
Complaints received during reporting period	76
Total complaints for reporting period	84
Complaints resolved during reporting period	70
Complaints pending	14

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 CFPB 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 CFPB 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 allegations that senior CFPB employees provided false or misleading information to Congress and disclosed nonpublic information to a nongovernment entity. During the course of this investigation, while we did not substantiate the initial allegations, we did substantiate that one former CFPB employee violated the CFPB's *Process for Presentations and Speeches* when he failed to submit talking points for CFPB-wide clearance before speaking at an outside event. The employee left CFPB employment before the start of our investigation. The matter was not referred to the DOJ, and the case was 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 CFPB 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 that senior CFPB employees provided false or misleading information to Congress and disclosed nonpublic information to a nongovernment entity. The investigation was unable to substantiate the allegations, and the investigation was closed. During the course of this investigation, we substantiated that one former CFPB employee violated the CFPB's *Process for Presentations and Speeches* when he failed to submit talking points for CFPB-wide clearance before speaking at an outside event.
- We initiated an investigation relating to allegations that a senior CFPB employee intentionally withheld evidence or provided false information about supervision examination findings to CFPB management. The allegations were unsubstantiated, and the 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 CFPB 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	1	2
2020	2	6
2021	2	4
2022[a]	6	13

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

a. Through September 30, 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.

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

2020 Audit of the Board's Information Security Program

2020-IT-B-020 November 2, 2020

Total number of recommendations: 4
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 effectively at a level-4 (*managed and measurable*) maturity. 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 Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced

2021-IT-B-011 September 15, 2021

Total number of recommendations: 3
Recommendations open: 2

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: 2

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. 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 unfair or deceptive acts or practices (UDAP) and fair lending matters.

The Division of Consumer and Community Affairs (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. DCCA can also develop 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.

The Board Can Enhance Its Personnel Security Program

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

Total number of recommendations: 6
Recommendations open: 6

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 Personnel Security Services (PSS) section can enhance the Board's personnel security program by defining objectives or risk tolerances to measure program performance and consistently following its processes for documenting position risk designations for the background investigations. 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, 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.

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

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. We also 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.

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

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.

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.

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

2022-IT-B-008R **June 15, 2022**

Total number of recommendations: 1
Recommendations open: 1

See the summary in the body of this report.

Security Control Review of the Board's Secure Document System (nonpublic)

2022-IT-B-009R **June 15, 2022**

Total number of recommendations: 1
Recommendations open: 1

See the summary in the body of this report.

2022 Audit of the Board's Information Security Program

2022-IT-B-013 **September 30, 2022**

Total number of recommendations: 1
Recommendations open: 1

See the summary in the body of this report.

Consumer Financial Protection Bureau

Table C-2. Reports to the CFPB 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	3
2019	2	3
2020	2	5
2021	6	30
2022[a]	2	8

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

a. Through September 30, 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 CFPB 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 CFPB'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 CFPB'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 CFPB'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 CFPB'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 CFPB 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: 1

The CFPB'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 CFPB has offboarding controls related to conflicts of interest for executive employees' postemployment restrictions, the CFPB 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 CFPB. We evaluated the effectiveness of the CFPB's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The CFPB'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 CFPB 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 CFPB 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 CFPB has developed a life cycle process for deploying and managing security risks for CFPB 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 CFPB 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: 1

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

The CFPB's information security program is operating effectively at a level-4 (*managed and measurable*) maturity. We identified opportunities for the CFPB 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 CFPB's information security program, which we performed to meet FISMA requirements, we tested the CFPB's plan of action and milestones (POA&M) process, which the agency uses to document and remediate information security weaknesses.

We found that costs associated with remediating cybersecurity weaknesses listed in POA&Ms were not accurately accounted for. We also identified instances in which the status of cybersecurity weaknesses included in the CFPB'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 CFPB'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 CFPB 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 CFPB was aware of several of these issues, it had not taken timely action to mitigate the risks; the CFPB had accepted specific risks related to certain vulnerabilities in the Legal Enclave but had not formally documented its rationale for these decisions.

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: 9

The CFPB'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 CFPB'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 CFPB 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 CFPB'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 CFPB's controls for issuing and managing interagency agreements (IAAs), including compliance with relevant laws and regulations.

The CFPB'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 CFPB'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 CFPB policy, and the CFPB 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 CFPB's implementation of Splunk to assess the system's compliance with FISMA and the information security policies, procedures, standards, and guidelines of the CFPB.

The CFPB's implementation of Splunk generally adheres to security best practices, the agency's information security policies and procedures, and FISMA. However, the CFPB 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

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

The CFPB's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. Since our review last year, the CFPB has taken several steps to strengthen its information security program. Nonetheless, similar to our previous FISMA audits, we identified opportunities for the CFPB 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 Improve Aspects of Its Quality Management Program for Supervision Activities

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

Total number of recommendations: 9
Recommendations open: 4

We assessed the design and effectiveness of the Division of Supervision, Enforcement and Fair Lending's (SEFL) Quality Management Program (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, the Office of Supervision Examinations 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.

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: 4

The Dodd-Frank Act authorizes the CFPB 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 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 CFPB's jurisdiction. We also found that limited staffing levels in SEFL's Office of Supervision Examinations constrain the CFPB'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.

The CFPB Is Generally Prepared to Implement the OPEN Government Data Act and Can Take Additional Steps to Further Align With Related Requirements

2022-MO-C-012 **September 28, 2022**

Total number of recommendations: 2
Recommendations open: 2

See the summary in the body of this report.

2022 Audit of the CFPB's Information Security Program

2022-IT-C-014 **September 30, 2022**

Total number of recommendations: 6
Recommendations open: 6

See the summary in the body of this report.

Abbreviations

CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CEO	chief executive officer
CI	Criminal Investigation
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
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 Boston	Federal Reserve Bank of Boston
FRB New York	Federal Reserve Bank of New York
IAA	interagency agreement
ICO	initial coin offering
IG	inspector general
IRS	Internal Revenue Service
IT	information technology
MDPS	multiregional data processing servicer
MSLP	Main Street Lending Program
OMB	Office of Management and Budget
OPEN Government Data Act	Open, Public, Electronic, and Necessary Government Data Act of 2018

PBGC	Pension Benefit Guaranty Corporation
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
RTO	return-to-office
SBA	U.S. Small Business Administration
SDS	Secure Document System
SEFL	Division of Supervision, Enforcement and Fair Lending
SMCCF	Secondary Market Corporate Credit Facility
SSA	U.S. Social Security Administration
TBIS	Titanium Blockchain Infrastructure Services Inc.
TIGTA	U.S. Treasury Inspector General for Tax Administration
UDAP	unfair or deceptive acts or practices
USPIS	U.S. Postal Inspection Service

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

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

OIG Hotline

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

800-827-3340