JULY 2023

Annual Report of the Council of Inspectors General on Financial Oversight

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

THIS PAGE INTENTIONALLY LEFT BLANK

Message from the Acting Chair

On July 10, 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) was signed into law, creating both the Financial Stability Oversight Council (FSOC) and the Council of Inspectors General on Financial Oversight (CIGFO). Chaired by the Treasury Secretary, FSOC is charged with identifying threats to the financial stability of the country, promoting market discipline, and responding to emerging risks to the stability of the nation's financial system. CIGFO, which includes the Inspectors General (IG) of nine major government financial entities, was established to facilitate information sharing among the IG members, provide a forum for discussion of IG member work as it relates to the broader financial sector, and evaluate the effectiveness and internal operations of FSOC.

This past year, as the Nation emerges from the Coronavirus Disease 2019 (COVID-19) pandemic, CIGFO continued to monitor the ongoing response of FSOC and its member agencies related to the public health and financial crisis. CIGFO also continued to monitor developments in challenges to the stability of the U.S. financial system such as climate-related financial risks and digital assets.

We are mindful of new risks and emerging challenges as well. As pointed out in FSOC's 2022 Annual Report, U.S. economic growth slowed in 2022, which may be the result of a convergence of factors: the war in Ukraine, the tightening of monetary policy, and lingering supply chain disruptions. Meanwhile, the country continues to experience annual inflation at its highest levels in 40 years. And in March 2023, the failure of three financial institutions triggered extraordinary actions on the part of the Federal Government. Taken together, these factors have caused a sense of economic uncertainty and a period of financial and economic stress unseen since perhaps the Great Recession of 2008 which precipitated the passage of Dodd-Frank and the creation of FSOC. It is imperative that now, more than ever, FSOC and CIGFO remain diligent in fulfilling their responsibilities and duties.

Dodd-Frank grants CIGFO the authority to convene working groups, by a majority vote, for the purpose of evaluating the effectiveness and internal operations of FSOC. CIGFO has, since 2011, established working groups that are comprised of staff from the CIGFO member Inspector General offices to conduct these reviews of FSOC operations and we have continued this important work this past year. In June 2022, CIGFO issued forward-looking crisis guidance compiled by a working group based on lessons learned from the experiences of federal agencies during prior crises and any learned during the pandemic. This guidance can be found in the Appendix to this report. In 2021, CIGFO convened another working group to review FSOC's response to Executive Order 14030, *Climate-related Financial Risk*, which is expected to be completed in the summer of 2023.

CIGFO's monitoring activities also include sharing financial regulatory information that enhances the knowledge and insight of its members about specific issues related to members' current and future work. For example, during its quarterly meetings, CIGFO members discussed FSOC's efforts to assess climate-related financial risk, reports and developments in the digital asset space and the recent financial institution failures; as well as legislative activities that could impact the financial regulatory system.

In the coming year, CIGFO members will continue, through their individual and joint work, to help strengthen the financial system by oversight of FSOC and its Federal member agencies.

/s/

Rich Delmar
Acting Chair, Council of Inspectors General on Financial Oversight
Acting Inspector General, Department of the Treasury

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

Council of Inspectors General on Financial Oversight

The Council of Inspectors General on Financial Oversight (CIGFO) was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), and meets on a quarterly basis to facilitate the sharing of information among Inspectors General. The CIGFO members discuss the ongoing work of each Inspector General who is a member of the Council, with a focus on concerns that may apply to the broader financial sector, and exchange ideas about ways to improve financial oversight. The CIGFO publishes an annual report that includes separate sections within the exclusive editorial control of each Inspector General. Those sections describe the concerns and recommendations of each Inspector General and a discussion of ongoing and completed work.

During the course of the year, the CIGFO continued to monitor coordination efforts among and between Financial Stability Oversight Council (FSOC) members. Specifically, CIGFO members were briefed on and/or discussed the following:

- U.S. Department of Housing and Urban Development Office of Inspector General work relating to Ginnie Mae's preparedness in responding to potential future crises
- Department of the Treasury report: *Crypto-Assets, Implications for Consumers, Investors, and Businesses*
- Executive Order 14067 – *Ensuring Responsible Development of Digital Assets*
- FSOC's *Report on Digital Asset Financial Stability Risks and Regulation*
- Legislative matters of interest, including proposed legislation on various digital asset topics and banking regulation
- FSOC's responses to the financial sector disturbances generated by failures in financial institutions with services concentrated in the technology industry

The Council of Inspectors General on Financial Oversight Reports

The Dodd-Frank Act authorizes CIGFO to convene a working group, by a majority vote, for the purpose of evaluating the effectiveness and internal operations of the FSOC.

To date, CIGFO has issued the following reports—

- 2012 - *Audit of the Financial Stability Oversight Council's Controls over Non-public Information*
- 2013 - *Audit of the Financial Stability Oversight Council's Designation of Financial Market Utilities*
- 2014 - *Audit of the Financial Stability Oversight Council's Compliance with Its Transparency Policy*
- 2015 - *Audit of the Financial Stability Oversight Council's Monitoring of Interest Rate Risk to the Financial System*
- 2017 - *Audit of the Financial Stability Oversight Council's Efforts to Promote Market Discipline*
- 2017 - *Corrective Action Verification of FSOC's Implementation of CIGFO's Audit Recommendations in the 2013 Audit of FSOC's Financial Market Utility Designation Process*
- 2018 - *Top Management and Performance Challenges Facing Financial Regulatory Organizations*
- 2019 - *Audit of the Financial Stability Oversight Council's Monitoring of International Financial Regulatory Proposals and Developments*
- 2019 - *Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations*
- 2020 - *Survey of FSOC and its Federal Member Agencies' Efforts to Implement the Cybersecurity Act of 2015*
- 2020 - *Council of Inspectors General on Financial Oversight Presidential Transition Handbook*
- 2022 - *CIGFO Guidance in Preparing for and Managing Crises*

The corrective actions described by FSOC, with respect to the audits listed above, met the intent of our recommendations and may be subject to verification in future CIGFO working group reviews.

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

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

We provide independent oversight by conducting audits, evaluations, investigations, and other reviews of the programs and operations of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB) and demonstrate leadership by making recommendations to improve economy, efficiency, and effectiveness, and by preventing and detecting fraud, waste, and abuse.

Background

Congress established our office as an independent oversight authority for the Board, the government agency component of the broader Federal Reserve System, and the CFPB.

Under the authority of the Inspector General Act of 1978, as amended (IG Act), we conduct independent and objective audits, evaluations, investigations, and other reviews related to the programs and operations of the Board and the CFPB.

- We make recommendations to improve economy, efficiency, and effectiveness, and we prevent and detect fraud, waste, and abuse.
- We share our findings and make corrective action recommendations to the Board and the CFPB; we do not manage agency programs or implement changes.
- We keep the Board chair, the CFPB director, and Congress fully informed of our findings and corrective action recommendations, as well as the agencies' progress in implementing corrective action.

In addition to the duties set forth in the IG Act, Congress has mandated additional responsibilities for our office. Section 38(k) of the Federal Deposit Insurance Act (FDI Act) requires us to review failed financial institutions supervised by the Board that result in a material loss to the Deposit Insurance Fund (DIF) and produce a report within 6 months. The Dodd-Frank Wall Street Reform and Consumer Protection Act amended section 38(k) of the FDI Act by raising the materiality threshold and requiring us to report on the results of any nonmaterial losses to the DIF that exhibit unusual circumstances warranting an in-depth review.

Section 211(f) of the Dodd-Frank Act also requires us to review the Board's supervision of any covered financial company that is placed into receivership under title II of the act and produce a report that evaluates the effectiveness of the Board's supervision, identifies any acts or omissions by the Board that contributed to or could have prevented the company's receivership status, and recommends appropriate administrative or legislative action.

The Federal Information Security Modernization Act of 2014 (FISMA) established a legislative mandate for ensuring the effectiveness of information security controls over resources that support federal operations and assets. In a manner consistent 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 techniques for selected information systems.

Section 15010 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act established the Pandemic Response Accountability Committee (PRAC) within the Council of the Inspectors General on Integrity and Efficiency (CIGIE). PRAC is required to conduct and coordinate oversight of covered funds and the coronavirus response to detect and prevent fraud, waste, abuse, and mismanagement and 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 as a member of PRAC, and as such, we participate in PRAC meetings, conduct PRAC oversight activities, and contribute to PRAC reporting responsibilities.

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

OIG Reports and Other Products Related to the Broader Financial Sector

In accordance with section 989E(a)(2)(B) of the Dodd-Frank Act, the following highlights the completed and ongoing work of our office, with a focus on issues that may apply to the broader financial sector.

COMPLETED WORK

Major Management Challenges for the Board and the CFPB

Although not required by statute, we annually report on the major management challenges facing the Board and the CFPB. These challenges identify the areas that, if not addressed, are most likely to hamper the Board's and the CFPB's accomplishment of their strategic objectives.

The major management challenges for the Board that apply to the financial sector will be issued in the second quarter of 2023.[1]

Among other items, we identified four major management challenges for the CFPB:

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

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. 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.

2022 Audit of the Board's Information Security Program, OIG Report 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.

[1] The major management challenges for the Board were subsequently issued in May 2023 and are available here.

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.

Observations on Cybersecurity Risk Management Processes for Vendors Supporting the Main Street Lending Program and the Secondary Market Corporate Credit Facility, OIG Report 2022-IT-B-015, November 9, 2022

The Board established the MSLP and the Secondary Market Corporate Credit Facility to help certain businesses, nonprofits, and employers through the COVID-19 pandemic. We assessed processes for managing cybersecurity risks for third-party vendors supporting the MSLP and the Secondary Market Corporate Credit Facility.

Overall, we found that System officials quickly established vendor contracts that generally met cybersecurity best practices. However, we identified ways to strengthen third-party cybersecurity risk management processes for future scenarios and found that Board and Reserve Bank information security program policy requirements for vendor risk management do not fully align.

Our report does not contain recommendations.

The Board Can Enhance the Effectiveness of Certain Aspects of Its Model Risk Management Processes for the SR/HC-SABR and BETR Models, OIG Report 2022-SR-B-016, December 7, 2022

The Board uses supervisory models to advance the risk-focused supervision of financial institutions. Because they inform the Board's supervision activities, these models must be sound and produce reasonable and reliable outputs. We assessed the effectiveness of the Board's model risk management processes for the Supervision and Regulation Statistical Assessment of Bank Risk (SR-SABR), Holding Company Statistical Assessment of Bank Risk (HC-SABR) (together, SR/HC-SABR), and Bank Exams Tailored to Risk (BETR) models, which the Board uses to monitor risks at community and regional banking organizations.

We found that the Board can enhance model risk management by ensuring timely review and validation of the SR/HC-SABR and BETR models, developing a comprehensive model inventory of top-tier supervisory models, and developing a formal mechanism for tracking the findings and recommendations of internal groups that review and validate models. Our report contains recommendations designed to enhance the effectiveness of the Board's model risk management processes for the SR/HC-SABR and BETR models. The Board concurred with our recommendations.

The Board Can Enhance Certain Governance Processes Related to Reviewing and Approving Supervisory Proposals, OIG Report 2022-SR-B-017, December 7, 2022

As part of its oversight of financial institutions, the Board develops supervisory proposals, which include guidance addressing significant supervision matters as well as stress tests to evaluate the resilience of large banks. We assessed the effectiveness of the Board's processes and practices for reviewing and approving supervisory proposals.

We found several ways for the Board to enhance its review and approval of supervisory proposals. For example, it can improve how it informs and consults Board members and can clarify when and how it solicits public feedback on these proposals. It can also clarify how some of the Board's operations should be executed in the absence of a vice chair for supervision, including delegated actions related to stress testing proposals.

Our report contains recommendations designed to enhance the effectiveness of the Board's processes and practices for reviewing and approving supervisory proposals. The Board concurred with our recommendations.

The Board Can Enhance Enterprise Practices for Data Management Roles and Responsibilities, OIG Report 2023-MO-B-001, January 18, 2023

The Board relies extensively on data to conduct research, analysis, and policymaking; supervise and regulate certain financial institutions and activities; oversee important aspects of the nation's payments system; and promote consumer protection, fair lending, and community development. We evaluated the agency's practices related to roles and responsibilities for managing data.

The Board uses a decentralized data management model, resulting in varying definitions, training methods, and approaches to data inventory across agency divisions. Further, the chief data officer has not been formally granted authority over data management and governance, which may lead to challenges implementing action plans outlined in the Board's data strategy.

Our report contains recommendations designed to enhance enterprise practices related to data management roles and responsibilities, training, and data inventory management. Our

report also recommends that authority for data management and governance be delegated to the chief data officer. The Board concurred with our recommendations.

2022 Audit of the CFPB's Information Security Program, OIG Report 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.

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

ONGOING WORK

Evaluation of the Board's and the Federal Reserve Banks' Access Controls and Practices for Disposing of Confidential Information in Select Applications Used for Supervising Community and Regional Banking Organizations

During the supervisory process, Board and Reserve Bank employees review, create, and store information, such as records collected from supervised institutions, that is exempt from public disclosure and that may include personally identifiable information. To protect this information from accidental disclosure or access by unauthorized parties, the Board and the Reserve Banks must have adequate controls. Inadequate safeguards for confidential information could have adverse implications for supervised institutions, their customers, and the Federal Reserve System. We are assessing the Board's and the Reserve Banks' access controls and practices for disposing of confidential supervisory information and sensitive personally identifiable information in select applications used for supervising community banking organizations and regional banking organizations.

Review of the Board's Approach to Climate Risk Supervision at Financial Institutions

As noted in the Board's November 2020 *Supervision and Regulation Report*, Federal Reserve System supervisors are responsible for ensuring that supervised institutions operate in a safe and sound manner and can continue to provide financial services to their customers in the face of all types of risk, including those related to climate change. The report noted, however, that assessing and managing climate related risks presents several challenges and that

supervisors are seeking to better understand, measure, and mitigate climate-related financial risks. Further, the report stated that supervisors will continue to work with other agencies and authorities on this endeavor. The Board established the Supervision Climate Committee to promote the resilience of supervised institutions to climate-related financial risks and is in the process of developing its supervisory approach on this topic. We will be issuing an Insights Paper identifying key areas of consideration as the Board develops and implements a supervisory approach for climate risks at financial institutions.

Evaluation of the Board's and the Federal Reserve Banks' Ethics Programs Pertaining to Personal Investment and Trading Activities[2]

As the central bank of the United States, the Board must maintain impartiality and avoid even the appearance of conflicts of interest to inspire public trust in the nation's financial system. The Board recently announced a broad set of new *investment and trading rules* that, among other things, will prohibit the purchase of individual securities, restrict active trading, and increase the timeliness of reporting and public disclosure. We are assessing the design and effectiveness of these new rules as well as the Board's and the Reserve Banks' approach to monitoring personal investment and trading activities for possible conflicts of interest

Evaluation of the Federal Reserve System's Loan Purchase Processes for Its Main Street Lending Program (MSLP)

In response to the COVID-19 pandemic, the Board established the MSLP—composed of five different lending facilities—to facilitate lending to small and medium-sized for-profit and nonprofit organizations. Through the MSLP, the Federal Reserve Bank of Boston purchased 1,830 loans amounting to approximately $17.5 billion from lenders; the majority of these loans were purchased during the last 2 months of the program. We are assessing the design and operating effectiveness of the System's processes for loan purchases.

Audit of the Board's Hiring Practices and Their Effect on Workforce Diversity

The Board's activities affect the lives of every American, and its continued success depends on its ability to attract a talented and diverse workforce that is representative of our nation's diversity. We are assessing the Board's hiring processes and procedures, determining the extent to which the Board's workforce diversity has changed since our 2015 diversity and inclusion report, and examining the effect that the Board's hiring practices may have on workforce diversity.

[2] The evaluation was subsequently completed in April 2023 and the report is available here.

Evaluation of the Federal Reserve System's Loan Administration Processes for Its Main Street Lending Program (MSLP)

In response to the COVID-19 pandemic, the Board established the MSLP—composed of five different lending facilities—to facilitate lending to small and medium-sized for-profit and nonprofit organizations. Through the MSLP, the Federal Reserve Bank of Boston is responsible for administering the loans, including assessing overall credit risk and identifying substandard loans. We are assessing the MSLP's processes for loan administration, including the design and operating effectiveness of internal controls.

Monitoring of the Federal Reserve's Lending Programs

In response to the economic effects of the COVID-19 pandemic, the Federal Reserve created new lending programs to provide loans to employers, certain businesses, and communities across the country to support the U.S. economy. Specifically, the following programs were created: the Main Street Lending Program, the Paycheck Protection Program Liquidity Facility, the Municipal Liquidity Facility, the Primary Market Corporate Credit Facility, and the Secondary Market Corporate Credit Facility. We initiated an active monitoring effort of these programs to gain an understanding of the operational, governance, reputational, and financial matters associated with them. Through this monitoring effort, we refine our focus on the programs and identify areas for future audits or evaluations.

2023 Audit of the Board's Information Security Program

The Federal Information Security Modernization Act of 2014 (FISMA) requires that each agency inspector general conduct an annual independent evaluation of its respective agency's information security program and practices. To meet FISMA requirements for 2023, we are conducting an audit of the Board's information security program. Our objectives are to evaluate the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, standards, and guidelines. We will use the results from our audit to respond to the Office of Management and Budget's fiscal year 2023 FISMA reporting metrics for inspectors general.

Evaluation of the Board's and the Federal Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions

As cybersecurity threats have become more frequent and more sophisticated over the last several years, cybersecurity has become a significant area of focus for financial institutions, the Board, and other federal financial regulators. Supervised institutions must report significant cybersecurity incidents to their primary federal regulator. After a supervised institution reports a cybersecurity incident to the Board, the Federal Reserve System assesses the severity of the incident on the institution and the financial sector, assigns a severity rating, and develops communications for internal and external stakeholders. We are assessing the Board's and the Reserve Banks' cybersecurity incident response process for supervised institutions.

Review of the Supervision of Silvergate Bank

In March 2023, the California Department of Financial Protection and Innovation announced that Silvergate Bank, a state member bank located in La Jolla, California, and supervised by the Federal Reserve Bank of San Francisco, had voluntarily begun the process of liquidation. On March 14, 2023, we initiated an independent review assessing the Board's and the Federal Reserve Bank of San Francisco's supervision of the institution, and we will make recommendations as appropriate.

Material Loss Review of Silicon Valley Bank

In March 2023, the California Department of Financial Protection and Innovation (DFPI) closed Silicon Valley Bank, a state member bank located in Santa Clara, California, and supervised by the Federal Reserve Bank of San Francisco. The DFPI appointed the Federal Deposit Insurance Corporation (FDIC) as receiver. As of December 31, 2022, Silicon Valley Bank had total assets of approximately $209 billion. On March 14, 2023, we initiated an engagement addressing the supervision of Silicon Valley Bank. In a March 26, 2023, press release, the FDIC estimated the cost of the failure to the Deposit Insurance Fund to be approximately $20 billion, which exceeds the statutory threshold requiring us to conduct a material loss review. Accordingly, our engagement will become a material loss review.

Evaluation of the Federal Reserve System's Vendor Selection and Management Processes Related to the Federal Reserve Bank of New York's (FRB New York) Emergency Lending Programs[3]

As part of its emergency lending program, FRB New York operated six emergency lending facilities, five of which were supported by multiple vendor contracts. FRB New York awarded some of its emergency lending program–related contracts noncompetitively because of the exigent circumstances, and other contracts pose potential conflict-of-interest risks to the System. FRB New York's reliance on vendors highlights the importance of its monitoring of vendor performance. We are assessing the Board's and FRB New York's processes related to vendor selection and management for FRB New York's emergency lending programs.

Evaluation of the CFPB's Process for Conducting Enforcement Investigations

The Dodd-Frank Act authorizes the CFPB to take appropriate enforcement actions to address violations of federal consumer financial laws. The CFPB's Division of Supervision, Enforcement and Fair Lending is responsible for this function and conducts investigations to assess whether financial institutions are complying with applicable federal consumer financial laws. According to the CFPB's 2022 performance plan and report, filing enforcement actions timely is an important measure of the CFPB's effectiveness because timely filing is a deterrent

[3] The evaluation was subsequently completed in April 2023 and the report is available here.

and provides consumers with greater protections. The report also details a performance goal for the expected time frame for filing or settling an enforcement action following the initiation of an investigation. We are assessing the Division of Supervision, Enforcement and Fair Lending's process for conducting enforcement investigations.

2023 Audit of the CFPB's Information Security Program

The Federal Information Security Modernization Act of 2014 (FISMA) requires that each agency inspector general conduct an annual independent evaluation of its respective agency's information security program and practices. To meet FISMA requirements for 2023, we are conducting an audit of the CFPB's information security program. Our objectives are to evaluate the effectiveness of the CFPB's (1) security controls and techniques for select information systems and (2) information security policies, procedures, standards, and guidelines. We will use the results from our audit to respond to the Office of Management and Budget's fiscal year 2023 FISMA reporting metrics for inspectors general.

Evaluation of the CFPB's Examiner Commissioning Program

The CFPB's Division of Supervision, Enforcement and Fair Lending is staffed with examiners who conduct supervisory reviews and examinations of institutions under the CFPB's jurisdiction. Given these responsibilities, examiners play a key role in executing the CFPB's mission. In October 2014, the CFPB transitioned from its Interim Examiner Commissioning Program to its formal Examiner Commissioning Program (ECP). Successful completion of the ECP is a significant milestone in an examiner's career, signifying an examiner's attainment of the broad-based technical expertise, knowledge, skills, and tools necessary to perform the duties of a commissioned examiner. We completed an evaluation of the program in September 2017 that resulted in recommendations designed to enhance the effectiveness of the ECP, which have since been implemented. For this evaluation, we plan to assess how the program has been operating over the last few years. Specifically, we will assess the CFPB's approach to examiner commissioning, including the case study component of the program. Further, we plan to benchmark the CFPB's ECP against other financial regulators' examiner commissioning programs.

Office of Inspector General Commodity Futures Trading Commission

The CFTC OIG acts as an independent Office within the CFTC that conducts audits, investigations, reviews, inspections, and other activities designed to identify fraud, waste and abuse in connection with CFTC programs and operations and makes recommendations and referrals as appropriate.

Background

The CFTC OIG was created in 1989 in accordance with the 1988 amendments to the Inspector General Act of 1978 (P.L. 95-452). OIG was established as an independent unit to:

- Promote economy, efficiency and effectiveness in the administration of CFTC programs and operations and detect and prevent fraud, waste and abuse in such programs and operations;
- Conduct and supervise audits and, where necessary, investigations relating to the administration of CFTC programs and operations;
- Review existing and proposed legislation, regulations and exchange rules and make recommendations concerning their impact on the economy and efficiency of CFTC programs and operations or the prevention and detection of fraud and abuse;
- Recommend policies for, and conduct, supervise, or coordinate other activities carried out or financed by such establishment for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in, its programs and operations; and
- Keep the Commission and Congress fully informed about any problems or deficiencies in the administration of CFTC programs and operations and provide recommendations for correction of these problems or deficiencies.

CFTC OIG operates independently of the Agency, and has not experienced interference from the CFTC Chairman or Commissioners in connection with the conduct of any investigation, inspection, evaluation, review, or audit, and our investigations have been pursued regardless of the rank or party affiliation of the target. The CFTC OIG consists of the Inspector General, the

Deputy Inspector General/Chief Counsel, the Assistant Inspector General for Auditing, the Assistant Inspector General for Investigations (vacant), one Attorney-Advisor, two Auditors, and one Senior Program Analyst. The CFTC OIG obtains additional audit, investigative, and administrative assistance through consultancies, contracts and agreements.

Role in Financial Oversight

The CFTC OIG has no direct statutory duties related to oversight of the futures, swaps and derivatives markets; rather, the CFTC OIG acts as an independent Office within the CFTC that conducts audits, investigations, reviews, inspections, and other activities designed to identify fraud, waste, and abuse in connection with CFTC programs and operations, and makes recommendations and referrals as appropriate. The CFTC's yearly financial statement and Customer Protection Fund audits are conducted by an independent public accounting firm, with OIG oversight.

Recent, Current or Ongoing Work in Financial Oversight

In addition to our work on CIGFO projects described elsewhere in this report, CFTC OIG continued the following projects during the past year:

2021-I-4 Pay Protection Program Proactive Investigation

In May 2021, OIG began a proactive investigation (2021-I-4) in coordination with CIGIE's Pandemic Response Accountability Committee (PRAC), CIGIE's Pandemic Analytics Center for Excellence, and the Small Business Administration, involving multiple phases. The first Phase identified CFTC employees who had obtained PPP loans and whether proper authorization for outside business activities had been obtained. CFTC OIG made recommendations to the Agency to improve the business processes and disclosures concerning outside business activities. Phase II and Phase III involve potential oversight issues. The Phase II and Phase III objectives are to:

- Identify CFTC registrants who have received PPP loans, with the potential goal of recommending that CFTC increase oversight efforts to assure CFTC's no-action relief is followed properly, if warranted, as well as other potential recommendations with regard to the oversight of registrants who have received PPP loans (including issues, if any, indicating potential systemic impact), and indicia of fraud in connection with the PPP loans identified.

- Identify CFTC contractors who obtained PPP loans to identify any indicia of fraud or potential reputational risks to the Agency.

OIG contracted with a third-party vendor to provide analytic support to examine the millions of records received in this investigation. OIG has shared its findings and has collaborated with other CIGFO OIGs on investigative methods to maximize the value of this investigation to the

oversight community. We reported our ongoing work on this project last year. During this year we suspended this project due to staff departures. At the close of the year, we were in the process of hiring attorneys with backgrounds in financial market regulation and/or microeconomics, as well as expert consultants.

White Paper Evaluating CFTC Experience with Digital Assets

Digital assets—including, among other things, cryptocurrency—have been widely adopted and used by both market participants and ordinary consumers. The CFTC has played an active role in the digital asset space, offering information to the public in the form of education and guidance as well as prosecuting digital asset-related conduct that violates the Commodity Exchange Act. We reported our ongoing work on this project last year. During this year we suspended this project due to staff departures. At the close of the year, we were in the process of hiring attorneys with backgrounds in financial market regulation and/or microeconomics, as well as expert consultants.

Office of Inspector General
Federal Deposit Insurance Corporation

The FDIC OIG mission is to prevent, deter, and detect fraud, waste, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the Agency.

Background

The Federal Deposit Insurance Corporation (FDIC) was created by the Congress in 1933 as an independent agency to maintain stability in the Nation's banking system by insuring deposits and independently regulating state-chartered, non-member banks. The FDIC insures $10.07 trillion in deposits at about 4,706 institutions, and promotes the safety and soundness of these institutions by identifying, monitoring, and addressing risks to which they are exposed. The Deposit Insurance Fund balance totaled $128.2 billion as of December 31, 2022.

The FDIC is the primary Federal regulator for approximately 3,032 of the insured institutions. An equally important role for the FDIC is as Receiver for failed institutions; the FDIC is responsible for resolving the failed institution and managing and disposing of its remaining assets.

The Office of Inspector General (OIG) at the FDIC is an independent and objective oversight unit established under the Inspector General (IG) Act of 1978, as amended. Our mission is to prevent, deter, and detect fraud, waste, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the Agency. We pursued audits, evaluations, and other reviews throughout the year in carrying out this mission. Of particular interest for this CIGFO report and implications for the broader financial sector, our audit and evaluation work covered topics such as information security program controls and practices pursuant to the Federal information Security Modernization Act of 2014, background investigations for privileged account holders**,** security controls over the FDIC's wireless network, implementation of the FDIC's information technology (IT) examination program, and security controls over the FDIC's Windows Active Directory.

Importantly, and in connection with matters affecting the financial sector, in February 2023, our Office also published its assessment of the Top Management and Performance Challenges Facing the FDIC. Our Top Management and Performance Challenges document summarizes the most serious challenges facing the FDIC and briefly assesses the Agency's progress to address them, in accordance with the Reports Consolidation Act of 2000 and Office of Management and Budget Circular A-136 (revised August 10, 2021).

In addition to the above areas related to the broader financial sector, our Office conducted significant investigations into criminal and administrative matters often involving sophisticated, complex multi-million-dollar frauds. These schemes involve bank fraud, embezzlement, money laundering, currency exchange manipulation, and other crimes involving banks, executives, directors, officials, insiders, and financial professionals. We are also working to detect and investigate cyber-criminal cases that threaten the banks and banking sector. Our cases reflect the cooperative efforts of other OIGs, U.S. Attorneys' Offices (USAO), FDIC Divisions and Offices, and others in the law enforcement community throughout the country. These working partnerships contribute to ensuring the continued safety and soundness of the Nation's banks and help ensure integrity in the FDIC's programs and activities.

Our Office also continues to play a key role in the investigation of individuals and organized groups perpetrating fraud through the Paycheck Protection Program (PPP) under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) and American Rescue Plan (ARP). To date, we have opened 190 cases associated with fraud in the CARES Act and ARP programs. We strongly support the Pandemic Response Accountability Committee's Fraud Task Force and the Department of Justice's COVID-19 Fraud Enforcement Task Force. We will continue to work in close collaboration with our law enforcement partners.

The FDIC OIG is also participating in the CIGFO Working Group that is examining FSOC's response to the Executive Order on climate-related financial risk.

FDIC OIG Audits and Evaluations Made Significant Recommendations for Improvements to the FDIC

During the 12-month period ending March 31, 2023, the FDIC OIG issued six audit and evaluation products and made 57 recommendations to strengthen controls in FDIC programs and operations. In the write-ups below, we discuss certain of our issued products, as they cover issues relevant to the broader financial sector.

The FDIC's Information Security Program – 2022

We issued our report on *The FDIC's Information Security Program–2022*. The audit evaluated the effectiveness of the FDIC's information security program and practices, as required by the Federal Information Security Modernization Act of 2014 (FISMA). The OIG engaged the professional services firm of Cotton & Company Assurance and Advisory, LLC to conduct this audit.

Department of Homeland Security (DHS) FISMA Reporting Metrics require OIGs to assess the effectiveness of their agencies' information security programs and practices using a maturity model. In Fiscal Year 2022, OIGs were required to evaluate a subset of 20 metrics. The FDIC's information security program was operating at a Maturity Level 4 (managed and measurable). The overall maturity level for FY 2022 was determined by a simple majority where the most frequent level (mode) across the 20 metric questions served as the overall rating. This mode-based scoring methodology does not fully capture the nature, scope, and magnitude of the risk posture of the agency's IT security. As a result, an agency may still face significant risks even if its rating score is considered to be managed and measurable. We cautioned the FDIC against complacency since deficiencies remain in the information security program at the FDIC.

The FDIC had established certain information security program controls and practices that were consistent with policy, standards, and guidelines. However, the audit report describes significant control weaknesses that reduced the effectiveness of the FDIC's information security program and practices, including the following:

- **The FDIC's Supply Chain Risk Management (SCRM) Program Lacked Maturity:** The FDIC was still developing its policies and procedures to address the SCRM finding from the FISMA report for 2021. Additionally, we found, in our OIG evaluation report of the FDIC's SCRM program (issued March 2022) that the FDIC had not implemented several objectives outlined in its SCRM Implementation Project Charter; did not conduct supply chain risk assessments in accordance with best practices; had not ensured that its Enterprise Risk Management processes fully capture supply chain risks; and FDIC Contracting Officers did not maintain contract documents in the proper system. We issued nine recommendations, five of which remained unimplemented.

- **The FDIC Did Not Adequately Oversee and Monitor Information Systems:** The FDIC Chief Information Officer Organization had not completed the authorization in accordance with the National Institute of Standards and Technology Risk Management Framework for approximately 52 percent of its legacy systems and subsystems (as of May 19, 2022).

- **The FDIC Did Not Address Flaw Remediation Plans of Action and Milestones (POA&M) in a Timely Manner:** The FDIC had 31 POA&Ms related to flaw remediation open past their estimated completion dates (as of June 21, 2022). These POA&Ms covered, for example, patch management, security updates for software products, and outdated versions or unapplied security updates for certain applications.

- **The FDIC Did Not Configure Privileged Accounts in Accordance with the Principle of "Least Privilege":** We were conducting another audit of the FDIC's security controls over its Windows Active Directory at the time of the FISMA audit.

During the course of our work, we identified instances where accounts were configured with elevated account settings; however, there was no justification provided for such settings, and the elevated settings were no longer needed for administrators to perform their business roles. Additionally, we identified concerns relating to the Background Investigations for Privileged Account Holders at the FDIC and issued a Management Advisory Memorandum in June 2022.

- **The FDIC Did Not Fully Implement Its Document Labeling Guide:** In our FISMA report dated October 2021, we recommended that the FDIC implement document labeling guide requirements across the organization. However, the FDIC had not yet fully implemented this recommendation and did not anticipate implementation until later in 2022.

The report contained a recommendation for the FDIC to address the 31 flaw remediation POA&Ms. It also contained a listing of three unimplemented recommendations from prior FISMA reports.

Background Investigations for Privileged Account Holders

While conducting an ongoing audit of security controls over the FDIC's Windows Active Directory, which we describe in more detail below, we identified concerns related to the FDIC's policies and procedures for ensuring that certain contractors and employees who require privileged access to FDIC information systems and data have background investigations commensurate with appropriate determinations of risk. A privileged account holder may have access and authority to control and monitor systems, and perform administrative functions that ordinary users are not authorized to perform. We issued a Memorandum to convey the need for controls to address associated risks.

The Office of Management and Budget Circular A-130 requires that agencies implement access control policies for information resources that ensure individuals have the appropriate background investigation conducted prior to granting access. We reviewed 144 privileged account holders to determine whether the FDIC conducted background investigations commensurate with position risk designation levels recorded in the FDIC's personnel system. We identified one exception and another case where a contractor had privileged access until the contractor's background investigation was unfavorably adjudicated. We also determined that the FDIC did not have policies or procedures in place to re-evaluate risk designations and background investigation levels for FDIC employees or contractors who transition from being non-privileged account holders to privileged account holders or whose privileged access is increased after they have already started work at the FDIC. Such controls can help ensure that the FDIC considers the risks resulting from a contractor or employee's change in privileged access and that the appropriate background investigation level is in place before granting the privileged access.

The FDIC agreed that procedures could be improved in this area and planned to perform follow-up work to further assess the extent of risk associated with our observations and make improvements to procedures and processes as warranted by the end of calendar year 2022.

Security Controls Over the FDIC's Wireless Networks

The term, "Wi-Fi," refers to wireless technology that allows internet enabled devices (laptops, tablets, and smartphones) to connect to wireless access points and communicate through a wireless network. Wi-Fi technology offers benefits to organizations; however, it also introduces security risks to the confidentiality, availability, and integrity of FDIC data and systems because it is not bound by wires or walls. If not properly configured, Wi-Fi technology is susceptible to signal interception and attack.

We conducted a review to determine whether the FDIC has implemented effective security controls to protect its wireless networks.

We found that the FDIC did not comply or partially complied with five practices recommended by the National Institute of Standards and Technology and guidance from the FDIC and other Federal agencies in the following areas:

- **Configuration of Wireless Networks:** The FDIC did not properly configure its Policy Manager, which enforces security policies for wireless network connectivity. Also, the FDIC's CIOO Wi-Fi Operations Group did not have control or awareness of the set-up and configuration of numerous wireless devices operating in FDIC buildings and facilities.

- **Wireless Signal Strength:** The FDIC did not have processes to examine and modify the signal strength of wireless devices/networks broadcasting throughout its buildings and leaking outside of FDIC facilities.

- **Security Assessments and Authorizations:** The FDIC did not maintain a current Authorization to Operate for its wireless network and did not conduct sufficient continuous monitoring testing activities to support the Agency's ongoing authorization of its wireless network.

- **Vulnerability Scanning:** The FDIC did not include certain wireless infrastructure devices in its vulnerability scans. In addition, the FDIC did not use credentialed scans on wireless infrastructure devices.

- **Wireless Policies, Procedures, and Guidance:** The FDIC did not maintain policies and procedures addressing key elements of the FDIC's wireless networks, including roles and responsibilities for the CIOO's Wi-Fi Operations Group; procedures for remediating wireless equipment alerts; standards for configuration settings; updates of wireless inventory records; and detection of rogue access points.

As a result, the FDIC faced potential security risks based upon its wireless practices and controls, including unauthorized access to the FDIC networks and insecure wireless devices broadcasting Wi-Fi signals. The FDIC had effective controls related to physical access controls of wireless devices, access control and encryption, monitoring of user internet destinations on its wireless networks, and disabling legacy wireless networks.

We made eight recommendations intended to strengthen the security controls over the FDIC's wireless networks and protect the confidentiality, availability, and integrity of FDIC systems and data. Management concurred with our recommendations. We engaged the professional services firm of TWM Associates, Inc. to conduct the technical aspects of this review.

Implementation of the Information Technology Risk Examination (InTREx) Program

Cyber risks present some of the greatest systemic threats facing the financial services sector – both domestically in the United States, and globally. The FDIC – along with the Federal Reserve Board (FRB) and Office of the Comptroller of the Currency – have all recognized that cybersecurity is a critical challenge facing the banking industry. These threats include ransomware attacks, denial of service, data breaches, phishing, and supply chain vulnerabilities. And they are increasing in both sophistication and frequency. Banks also may suffer cybersecurity incidents through their interconnections with third-party providers that deliver administrative or management services to financial institutions, such as accounting, human resources, and transaction processing.

The FDIC supervises banks to ensure that their operations function in a safe and sound manner, and comply with all laws and regulations. The FDIC examines institutions to assess their financial condition, management practices – as well as the banks' capabilities to identify and address Information Technology (IT) and cyber risks, and to maintain appropriate internal controls.

In June 2016, the FDIC implemented the InTREx program. We conducted an audit to determine whether the InTREx program effectively assesses and addresses IT and cyber risks at financial institutions.

We found that the FDIC needs to improve its InTREx program to effectively assess and address IT and cyber risks at financial institutions. Specifically, we found the following weaknesses in the program that limited the ability of examiners to assess and address IT and cyber risks at financial institutions:

- The InTREx program was outdated and did not reflect current Federal guidance and frameworks for three of four InTREx Core Modules;
- The FDIC did not communicate or provide guidance to its examiners after updates were made to the program;
- FDIC examiners did not complete InTREx examination procedures and decision factors required to support examination findings and examination ratings;
- The FDIC had not employed a supervisory process to review IT workpapers prior to the completion of the examination, in order to ensure that findings were sufficiently supported and accurate;
- The FDIC did not offer training to reinforce InTREx program procedures to promote consistent completion of IT examination procedures and decision factors;
- The FDIC's examination policy and InTREx procedures were unclear, which led examiners to file IT examinations workpapers in an inconsistent and untimely manner;
- The FDIC did not provide guidance to examination staff on reviewing threat information to remain apprised of emerging IT threats and those specific to financial institutions;
- The FDIC was not fully utilizing available data and analytic tools to improve the InTREx program and identify emerging IT risks; and
- The FDIC had not established goals and performance metrics to measure its progress in implementing the InTREx program.

The weaknesses detailed above collectively demonstrated the need for the FDIC to take actions to ensure that its examiners effectively assess and address IT and cyber risks during IT examinations. We made 19 recommendations to address these weaknesses.

Security Controls Over the Windows Active Directory

It is important for the FDIC to ensure that only individuals with a business need are allowed access to its many systems that contain sensitive information. The FDIC uses Active Directory (AD) to centrally manage user identification, authentication, and authorization. AD infrastructure is an attractive target for attackers because the same functionality that grants legitimate users access to systems and data can be hijacked by malicious actors for nefarious purposes.

We performed an audit to assess the effectiveness of controls for securing and managing the Windows AD to protect the FDIC's network, systems, and data. We engaged the professional services firm of Cotton & Company Assurance and Advisory, LLC (Cotton) to conduct this audit.

The FDIC had not fully established and implemented effective controls for securing and managing the Windows AD to protect the FDIC's network, systems, and data in 7 of the 12 areas we assessed. The FDIC needed to improve controls in the following areas:

- **Password Management:** We identified weaknesses in how the FDIC managed passwords and password changes. In addition, multiple privileged users (a) reused their passwords; (b) shared their passwords across multiple accounts; and (c) did not change their passwords for over a year.

- **Account Configuration:** Privileged accounts were configured with excessive privileges. Such privileges were not justified as necessary and could allow attackers to inflict significant damage if these accounts were compromised.

- **Access Management:** The FDIC account deletion setting did not remove over 900 users after they exceeded the required thresholds related to account inactivity. In addition, the FDIC suspended its automated account inactivity setting for a month in late 2021 without compensating controls.

- **Privileged Account Management:** Three FDIC users held privileged access for almost a year after the access was no longer required for their positions.

- **Windows Operating System Maintenance:** Several servers and a workstation were running unsupported versions of the Windows or Windows Server Operating System.

- **AD Policies and Procedures:** The AD Operations Manual included inaccurate information about the FDIC's implementation of AD.

- **Audit Logging and Monitoring:** The FDIC did not enable performance monitoring on two domain controllers supporting its AD infrastructure.

The FDIC's ineffective AD security controls could pose significant risks to FDIC data and systems. In addition, the cumulative impact of these weaknesses could result in an attacker covertly obtaining administrative privileges to the FDIC's AD, potentially allowing the attacker to obtain, manipulate, or delete data across the network, causing serious damage to the FDIC and its mission and reputation. Moreover, account misconfigurations by the FDIC may provide FDIC employees and contractors unnecessary elevated privileges on the FDIC's network.

We found that the FDIC had effective controls in the remaining five control areas we assessed related to configuration management, contingency planning, patch management, vulnerability remediation, and defining key AD points of contact.

We made 15 recommendations to address the AD security control weaknesses in the 7 areas listed above. The FDIC concurred with all recommendations.

The FDIC OIG Assessed the Top Management and Performance Challenges Facing the FDIC

The FDIC plays a unique role in support of the U.S. financial system. At the time we issued our Top Management and Performance Challenges report in February 2023, the FDIC insured nearly $10 trillion in deposits at more than 4,700 banks, supervised over 3,200 banks, and oversaw the $125 billion DIF that protects bank depositor accounts and resolves failing banks. The readiness of the FDIC to execute all facets of its mission promotes confidence and stability in the Nation's financial system.

Our report noted that banks are facing a rising interest rate environment while the U.S. economy faces inflationary pressure and continued uncertainties remain resulting from Russia's invasion of Ukraine. Banks have also adopted new technologies and third-party partnerships to engage customers at a time of increasing cyber security breaches. Banks are also entering into markets for digital assets, which may increase money laundering and terrorist financing risks. The FDIC's operating environment is also changing. The FDIC moved to a hybrid working environment and faces increased retirements and resignations among FDIC personnel.

In light of these circumstances, our report summarized the most serious challenges facing the FDIC and briefly assessed the Agency's progress to address them, pursuant to the Reports Consolidation Act of 2000 and Office of Management and Budget Circular A-136 (revised August 27, 2020). Our report is based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities. To compile this report, we received input and considered comments from the FDIC, and while exercising our independent judgment, we incorporated suggestions where appropriate and fair.

We identified nine Top Challenges facing the FDIC that could impact its capabilities to promote public confidence and financial stability:

Preparing for Crises in the Banking Sector. The FDIC has a unique mission to administer the DIF and insure Americans' bank deposits against losses during crises. The FDIC's effective maintenance of the DIF, supervision of banks, and resolution of failed banks provides financial stability to the United States. The FDIC faces crisis readiness challenges to fully develop its plans to respond to an unfolding crisis, including exercising the orderly

liquidation of systemically important entities. Further, FDIC readiness and supervisory activities should take into account climate-related risks. FDIC supervisory processes should also be agile to respond to evolving risks such as fraud in crises-related Government-guaranteed loan programs and the evasion of US-imposed economic and trade sanctions.

Mitigating Cybersecurity Risks at Banks and Third Parties. Cybersecurity has been identified as the most significant threat to the banking sector and the critical infrastructure of the United States. The FDIC faces challenges to ensure that examiners have the skillsets and knowledge to conduct information technology examinations that adequately identify and mitigate cybersecurity risks at banks and their third-party service providers. Further, the FDIC should ensure that it has effective processes for the intake of banks' cybersecurity incident reports and uses these reports to mitigate identified risks, identify trends and patterns of nefarious activity, and adjust supervisory processes. Mitigating cybersecurity risk is critical, as a cyber incident at one bank or third-party service provider has the potential to cause contagion within the financial sector.

Supervising Risks Posed by Digital Assets. About 52 million Americans have invested in digital assets and 136 FDIC-insured banks have ongoing or planned digital asset activities. The FDIC should work with other regulators to provided clarity regarding the regulation of digital assets. The FDIC should also have examiners with appropriate skillsets and examination processes to assess the safety and soundness of banks' digital asset activities and identify consumer risks. Further, the FDIC should ensure that its examinations, policies, and procedures address consumer risks regarding digital assets, including the relationship of deposit insurance and digital assets.

Fostering Financial Inclusion for Underserved Communities. Federal statute mandates that the FDIC study the unbanked market in the United States and identify the primary issues that prevent unbanked individuals from establishing conventional accounts in financial institutions. Converting the information gleaned from the study of unbanked individuals into effective actions that banks can take to increase access to the financial system for unbanked individuals is a challenging endeavor for the FDIC. Further, the FDIC should also ensure that its examiners have the skills, capabilities, and procedures to assess the effect of banks' use of artificial intelligence in decision making. Artificial Intelligence can be beneficial by increasing the speed and reducing the cost of bank operations, but it can also result in biases against individuals when the algorithms or data used for these decisions are flawed.

Fortifying IT Security at the FDIC. The FDIC is custodian of about 1.8 petabytes of sensitive and Personally Identifiable Information relating to failed banks and more than 4,700 insured banks. The FDIC continues to face challenges to ensure that it has strong information security processes to guard against persistent and increasing cyber threats against Federal agencies. Security control weaknesses of FDIC systems limit the effectiveness of FDIC controls, which places the confidentiality, integrity, and availability of FDIC systems and data at risk. The FDIC should have robust personnel security and suitability program and privacy controls to safeguard IT access to sensitive information and guard against insider threats.

Managing Changes in the FDIC Workforce. A total of 21 percent of the FDIC workforce was eligible to retire in 2022, and that figure would climb to 38 percent within 5 years (2027). These retirements may have a significant impact on key Divisions involved in Crises Readiness efforts and for subject matter experts in areas such as consumer compliance and information technology. At the same time, the FDIC is experiencing increased resignations of its examiners-in-training. Absent effective human capital management, the FDIC may lose valuable knowledge and leadership skill sets upon the departure of experienced examiners, managers, and executives. Meeting these challenges is especially important as the FDIC shifts its operations to a hybrid environment.

Improving the FDIC's Collection, Analysis, and Use of Data. Data and information can enhance the FDIC's and its supervised banks' capabilities to mitigate threats to the U.S. financial system. The FDIC faces challenges in receiving and using reliable information. Specifically, the FDIC should establish processes to acquire, analyze, and disseminate threat information from Government partners, databases, and repositories. Such information informs senior FDIC officials and decision-makers, FDIC examiners and Regional personnel, its supervisory program officials, and banks. Further, the FDIC should improve the reliability of its internal data to ensure that the FDIC Board and senior management can confidently use the data to assess program effectiveness.

Strengthening FDIC Contracting and Supply Chain Management. The FDIC awards nearly $600 million in contracts every year. Over a 5-year period, the FDIC awarded more than 2,600 contracts valued at $2.85 billion. The FDIC faces challenges to establish an effective contract management program that ensures the FDIC receives goods and services according to contract terms, price, and timeframes. An effective FDIC procurement program is important because the FDIC relies on contractor services for day-to-day activities and especially during crises. The FDIC should also have programs in place to mitigate security risks associated with the supply chains for contracted goods and services. Weaknesses in contractor-provided software to Government agencies have exposed examples of these supply chain risks. Further, the FDIC should have whistleblower processes and provisions within FDIC contracts to protect contractor personnel who report allegations of contractor violations and gross mismanagement.

Implementing Effective Governance at the FDIC. Effective governance allows FDIC Board members and senior FDIC officials to proactively manage risk, formulate regulatory policy, and provide clear guidance to banks and FDIC Regional Offices. Through these processes, the FDIC can allocate resources, prioritize and improve the flow of risk information to decision makers, and work toward achieving the FDIC's mission. The FDIC should ensure that risks to the FDIC are identified and monitored through an effective

Enterprise Risk Management Program. The FDIC should also ensure that OIG-identified program weaknesses are promptly resolved and remediated. FDIC program performance should be measured using outcome measures to assess whether the FDIC is meeting a program's strategic objectives. The FDIC should also clarify its implementation of Executive Branch best practices, ensure the validity of its rulemaking process, and promulgate rules based on rigorous cost benefit analyses.

The FDIC has taken certain concrete and measurable steps to address some of these Challenges, as noted in our Challenges report. We also recognized that there may have been other ongoing plans, inputs, intentions, or future activities that were still under development at the time of our issuance of the report.

FDIC OIG Investigations Helped Ensure Integrity in the Banking Sector and Addressed Fraud in the Federal Pandemic Response

Our Office is committed to partnerships with other OIGs, the Department of Justice (DOJ), and other state and local law enforcement agencies in pursuing criminal acts affecting banks and in helping to deter fraud, waste, abuse, and misconduct. We play a key role in investigating sophisticated schemes of bank fraud, embezzlement, money laundering, cyber-crime, and currency exchange rate manipulation—fraudulent activities affecting FDIC-supervised or insured institutions. Whether it is bank executives who have caused the failures of banks, or criminal organizations stealing from Government-guaranteed loan programs -- these cases often involve bank directors and officers, Chief Executive Officers, attorneys, real-estate insiders, financial professionals, crypto-firms and exchanges, Financial Technology (FinTech) companies, and international financiers.

The OIG also actively participates in many financial fraud and cyber working groups nationwide to keep current with new threats and fraudulent schemes that can undermine the integrity of the FDIC's operations and the financial services industry as a whole.

Our investigative results over the 12 months ending March 31, 2023, included the following: 106 indictments; 115 convictions; 83 arrests; and potential monetary recoveries (fines, restitution, asset forfeitures, settlements, and special assessments) of more than $378.1 million.

As illustrated in the case examples that follow, we continue to identify financial fraud schemes that affect FDIC-supervised and insured institutions. We also partner with other agencies, including the Small Business Administration (SBA), to identify fraud in the guaranteed loan portfolios of FDIC-supervised institutions. These investigations are important, as large-scale fraud schemes can significantly affect the financial industry and the financial condition of FDIC-insured institutions. In this regard, and as illustrated below, we continue to investigate Paycheck Protection Program (PPP) cases of individuals defrauding the Government-guaranteed loan program intended to help those most in need during the pandemic crisis. In fact, since inception of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act),

we have been involved in 190 such cases. Notably, during the period April 1, 2022 through March 31, 2023, the FDIC OIG's efforts related to the Federal Government's COVID-19 pandemic response resulted in 73 indictments and informations; 50 arrests or self-surrenders; and 69 convictions involving fraud in the CARES Act Programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases totaled in excess of $52 million.

Examples to illustrate the varied nature of our impactful investigative cases follow.

Rancher Sentenced for Running $244 Million "Ghost Cattle" Scam

Cody Allen Easterday (Easterday) was sentenced to 132 months imprisonment, 3 years of supervised release, and ordered to pay $244,031,132 in restitution in the Eastern District of Washington. Easterday previously pleaded guilty to one count of wire fraud after having orchestrated and carried out a massive, brazen, and long-term "ghost cattle" scheme where he fraudulently billed Tyson Foods and another company more than $244 million dollars for the purchase and feeding of cattle that never existed. Easterday ultimately carried out the fraud in order to cover significant losses sustained in commodity trades through CME Group, Inc. and further used fraud proceeds for his personal use and benefit. The scheme was the largest-ever criminal fraud scheme prosecuted in the Eastern District of Washington.

Easterday is the owner of Easterday Ranches, Easterday Farms, and Easterday Farms Dairy. He used loan advances and accounts held at Rabobank, N.A. (now Mechanics Bank) and Rabo AgriFinance to facilitate and fund market manipulation in Live Cattle and Feeder Cattle commodity futures contracts. CME Group, Inc., the world's largest financial derivatives exchange, was defrauded when Easterday submitted falsified paperwork that resulted in CME exempting Easterday Ranches from otherwise-applicable position limits in live cattle futures contracts. In order to cover approximately $200 million in commodity futures contracts trading losses, Easterday created and submitted false and fraudulent invoices totaling more than $244 million to Tyson Foods and another company between approximately 2016 and November 2020. These false and fraudulent invoices sought and obtained reimbursement from Tyson Foods and the other victim company for the purported costs of purchasing and raising hundreds of thousands of cattle that neither Easterday nor Easterday Ranches ever purchased, and that did not actually exist. The remainder of the $244 million Easterday stole from Tyson and the other victim company was converted to Easterday's personal use and for the benefit of the Easterday farming empire – an empire that, by 2020, included more than 22,000 acres of farmland, 150 employees, revenues of over $250,000,000, and even a private plane and hangar. Easterday's conduct also led Easterday Ranches and Easterday Farms to default on a $45 million loan issued by Washington Trust Bank. It is also alleged that Easterday may have misrepresented his assets to lenders in connection with the purchase of a dairy farm in 2019.

Source: *Fraud Section of the Criminal Division of DOJ.*
Responsible Agencies: *FDIC OIG and United States Postal Inspection Service (USPIS).*
Prosecuted by *the Fraud Section of the Criminal Division of DOJ and the USAO, Eastern District of Washington.*

Former Bank President and CEO Found Guilty of Fraud Resulting in the Failure of First NBC Bank

Former First NBC Bank President and Chief Executive Officer (CEO) Ashton J. Ryan, Jr. was convicted at trial by a Federal jury on 46 counts of bank fraud, conspiracy, and false bank entries. From 2006 through April 2017, Ryan and others conspired to defraud First NBC Bank through a variety of schemes. Ryan was the President and CEO of the Bank for most of its existence. Ryan and others conspired to defraud First NBC Bank by disguising the true financial status of certain borrowers and their troubled loans, concealing the true financial condition of the Bank from the Board of Directors, auditors, and examiners.

When members of the Board or the Bank's outside auditors or examiners asked about loans to these borrowers, Ryan and others made false statements about the borrowers and their loans, omitting the truth about the borrowers' inability to pay their debts without getting new loans. As a result, the balance on these borrowers' loans continued to grow resulting, ultimately, in the failure of First NBC. The Bank's failure cost the FDIC's Deposit Insurance Fund slightly under $1 billion.

Source: *This investigation was initiated from a complaint received by the FDIC.*
Responsible Agencies: *FDIC OIG, Federal Bureau of Investigation, and FRB OIG.*
Prosecuted by *the USAO, Eastern District of Louisiana.*

Hilo Man Receives 42 Months in Prison for Defrauding Covid-19 Relief Programs

Carey Mills, of Hilo, Hawaii, was sentenced to 42 months in Federal prison for wire fraud in connection with a scheme to defraud the Federal government of program funds intended for COVID-19-related relief. Mills pleaded guilty to a single-count information on May 17, 2022. In addition to a term of imprisonment, the Court also imposed a 5-year term of supervised release and ordered Mills to pay restitution to the SBA in the amount of $937,575.

From May to August 2020, Mills submitted multiple applications for PPP and Economic Injury Disaster Loan (EIDL) funds on behalf of three businesses under his control, Kanaka Maoli Hookupu Center, New Way Horizon Travel, and Uilani Kawailehua Foundation, each time utilizing interstate wires. To support the applications, Mills submitted fraudulent payroll documents and IRS forms, which included false employee and wage payment records. As a result of these applications, Mills received $937,575 in the form of three forgivable PPP loans and one EIDL grant to which he was not entitled.

Mills used the Federal relief money to fund personal expenses, including the purchase of eight vehicles and two residential properties. The Mills case was the first COVID-19 program fraud sentencing in the District of Hawaii.

Source: *This investigation was initiated from a referral from the USAO-Hawaii and U.S. Treasury Inspector General for Tax Administration (TIGTA).*
Responsible Agencies: *FDIC OIG, TIGTA, SBA OIG, and Homeland Security-Investigation.*
Prosecuted by *the USAO, Hawaii.*

Former Wells Fargo Executive Agrees to Plead Guilty to Obstructing a Bank Examination Involving the Opening of Millions of Accounts Without Customer Authorization

Carrie L. Tolstedt, the former head of Wells Fargo Bank's retail banking division, agreed to plead guilty to obstructing a government examination into the bank's widespread sales practices misconduct, which included opening millions of unauthorized accounts and other products. The Office of the Comptroller of the Currency (OCC), which investigated misconduct at Wells Fargo, also reached a resolution with Tolstedt in a regulatory proceeding. As part of the consent order resolving that matter, Tolstedt agreed to a ban from working in the banking industry and to pay a $17 million civil penalty.

From approximately 2007 to September 2016, Tolstedt was Wells Fargo's senior executive vice president of community banking and was head of the Community Bank, which operated Well Fargo's consumer and small business retail banking business. The Community Bank managed many of the products that Wells Fargo sold to individual customers and small businesses, including checking and savings accounts, CDs, debit cards, bill pay, and other products.

Wells Fargo previously admitted that, from 2002 to 2016, excessive sales goals led Community Bank employees to open millions of accounts and other financial products that were unauthorized or fraudulent. In the process, Wells Fargo collected millions of dollars in fees and interest to which it was not entitled, harmed customers' credit ratings, and unlawfully misused customers' sensitive personal information.

Many of these practices were referred to within Wells Fargo as "gaming." Gaming strategies included using existing customers' identities – without their consent – to open accounts. Gaming practices included forging customer signatures to open accounts without authorization, creating PINs to activate unauthorized debit cards, and moving money from millions of customer accounts to unauthorized accounts in a practice known internally as "simulated funding."

Gaming also included opening credit cards and bill pay products without authorization, altering customers' contact information to prevent customers from learning of unauthorized accounts and to prevent Wells Fargo employees from reaching customers to conduct customer satisfaction surveys, and encouraging customers to open accounts they neither wanted nor needed.

According to the plea agreement, Tolstedt was aware of sales practices misconduct within the Community Bank and the fact that employees were terminated each year for gaming. By no later than 2006, Tolstedt was learning about the gaming practices from corporate investigations and, over time, learned that terminations for gaming in the Community Bank were steadily increasing, that the misconduct was linked in part to sales goals within the Community Bank, and that termination numbers likely underestimated the scope of the problem.

Although the Community Bank eventually took steps purportedly designed to proactively identify sales misconduct, the measures used by the bank flagged only a small portion of the potentially problematic activity for investigation. As of July 2014, only the most egregious .01 to .05 percent of employees engaging in activity considered a "red flag" for sales practices misconduct were investigated – with the remaining 99.95 to 99.99 percent left unexamined under this process.

In May 2015, Tolstedt participated in the preparation of a memorandum, which she knew would be provided to the OCC in connection with its examination of sales practice issues at Wells Fargo. To minimize the scope of the sales practices misconduct within the Community Bank, Tolstedt corruptly obstructed the OCC's examination by failing to disclose statistics on the number of employees who were terminated or resigned pending investigation for sales practices misconduct. She also failed to disclose that the Community Bank proactively investigated only a very small percentage of employees who engaged in activity flagged as potential sales practices misconduct.

Wells Fargo in 2020 acknowledged the widespread sales practices misconduct within the Community Bank and paid a $3 billion penalty in connection with agreements reached with the United States Attorneys' Offices for the Central District of California and the Western District of North Carolina, the Justice Department's Civil Division, and the Securities and Exchange Commission.

Responsible Agencies: *FDIC OIG, FBI, Federal Housing Finance Agency OIG, FRB OIG, and the USPIS. The Office of the Comptroller of the Currency and the Securities and Exchange Commission provided additional investigative assistance.*
Prosecuted by *the USAO, Central District of California; USAO, Western District of North Carolina; and Major Frauds Section, DOJ.*

Business Email Compromise Subject Sentenced

On September 2, 2022, Muhammed Naveed was sentenced to serve 46 months in prison for his role in a business email compromise (BEC) scheme. Naveed was also ordered to pay restitution of $446,000 for his role in the operation of an unlicensed money transmitting business.

The investigation into suspected computer intrusion and BEC scheme identified fraudulent emails from spoofed domains that were used to trick numerous companies to unwittingly transmit funds from FDIC-insured institutions to the subject controlled accounts rather than to accounts intended by the companies. During the course of the investigation, Naveed was identified as a money mule—that is, an individual who transfers money acquired illegally on behalf of others, and his business, Blacksmith Corporation, was identified as having received money as a result of this fraudulent scheme.

Source: *FBI.*
Responsible Agencies: *FDIC OIG and FBI.*
Prosecuted by *the USAO, Eastern District of Virginia.*

***

Learn more about the FDIC OIG at www.fdicoig.gov or follow us on Twitter at FDIC_OIG.

Office of Inspector General
Federal Housing Finance Agency

The Federal Housing Finance Agency (FHFA) Office of Inspector General (OIG) promotes the economy, efficiency, and integrity of FHFA programs and operations, and deters and detects fraud, waste, and abuse, thereby supporting FHFA's mission. We accomplish our mission by conducting audits, evaluations, compliance reviews, investigations, and other independent oversight of the Agency's programs and operations, engaging in robust enforcement efforts to protect the interests of the American taxpayers, and keeping our stakeholders fully and currently informed of our work.

Background

The Housing and Economic Recovery Act of 2008 established the Federal Housing Finance Agency (FHFA or Agency) in July 2008. FHFA serves as regulator and supervisor of several entities: Fannie Mae and Freddie Mac (the Enterprises); Common Securitization Solutions, LLC, an affiliate of each Enterprise (CSS); the Federal Home Loan Banks (FHLBanks) (collectively, the Enterprises, CSS, and the FHLBanks are the regulated entities); and the FHLBanks' fiscal agent, the Office of Finance. FHFA is responsible for ensuring the regulated entities' safety and soundness so that they serve as a reliable source of liquidity and funding for housing finance and community investment. As of December 31, 2022, the Enterprises collectively reported more than $7.5 trillion in assets and the FHLBanks reported more than $1.2 trillion.

Since September 2008, FHFA also has served as the Enterprises' conservator. Initially, the conservatorships were intended to be a temporary measure during a period of extreme stress to stabilize the mortgage markets and promote financial stability. They are now in their fifteenth year.

OIG's Risk-Based Oversight Strategy

FHFA's dual roles as the regulated entities' supervisor and the Enterprises' conservator present unique challenges for OIG. Consequently, OIG structures its oversight program to rigorously examine FHFA's exercise of its dual responsibilities, which differ significantly from those of the typical federal financial regulator. Given the regulated entities' size and complexity and FHFA's unique responsibilities, OIG must make informed and targeted choices about what we audit, evaluate, review for compliance, and investigate.

Management and Performance Challenges

Each year we assess and identify FHFA's top management and performance challenges and align our work with those challenges. Our memorandum to the FHFA Director identifying FHFA's management and performance challenges for Fiscal Year 2023 is available on our website. It reports on the most serious challenges which, if not addressed, could adversely affect FHFA's accomplishment of its mission. A summary of the oversight activities during FY 2023 is discussed in our Annual Plan.

The management and performance challenges for FY 2023 are:

- Effective supervision of the regulated entities
- Stewardship of the Enterprise conservatorships
- Oversight of information risk for the regulated entities
- Oversight of counterparty risk, third-party risk, and fourth-party risk for the regulated entities
- Oversight of model risk for the regulated entities
- Oversight of people risk for the regulated entities
- Oversight of resiliency risk for the regulated entities

The first four challenges reiterate themes we identified in prior years. For FY 2023, we also highlight FHFA's oversight of key operational risks at the regulated entities, including model risk, people risk, and resiliency risk. Importantly, these challenges interconnect.

Significant Reports

OIG focuses much of its oversight activities on identifying vulnerabilities in these areas and recommending positive, meaningful actions that the Agency could take to mitigate these risks and remediate identified deficiencies.

Taken together, this body of work provides important insights across FHFA's programs and operations, including the entities under the Agency's purview.

Enterprises

In addition to its statutory charge to serve as the Enterprises' regulator and supervisor, since 2008, FHFA has also served as their conservator. In AUD-2023-003, we reported that FHFA made conservatorship decisions in accordance with its conservatorship decision policy and procedures and performed conservatorship monitoring and surveillance. We found certain instances where FHFA's document management and retention practices adversely impacted FHFA's ability to demonstrate its rationale for certain decisions. We also found that FHFA's current policies and procedures increase the risk that conservatorship decision activity would not be conducted in accordance with FHFA management's intentions. We highlighted information related to another aspect of FHFA's Enterprise engagement in EVL-2023-001. Announced in December 2021, FHFA conducted an independent review of a sample of appraisal reports and concluded that valuation bias persists in housing finance in America. FHFA told us that the Agency made referrals to the Department of Housing and Urban Development and also made information available to the Department of Justice and Consumer Financial Protection Bureau. Although the Agency had not filed complaints with the state licensing authorities responsible for investigating complaints against appraisers, doing so would provide those authorities with the actionable information needed to initiate investigations of the appraisers FHFA identified. These two reports resulted in four recommendations, which the Agency accepted. In WPR-2022-001, we explained that Fannie Mae and Freddie Mac rely on numerous third parties to originate and service mortgages and to provide a wide array of services essential to their business operations. Third parties to the Enterprises rely on their own third parties, which are fourth parties to the Enterprises. Like third parties, fourth parties pose risk to the Enterprises that must be managed, and the Enterprises face challenges managing that risk, particularly related to their limited direct oversight of fourth parties.

CSS

FHFA is the regulator and supervisor for the Enterprises' affiliate, CSS, which provides vital services to them, including securities issuance and administration. These services are critical to the Enterprises' role in the secondary market. As we explained in WPR-2023-001, the magnitude and complexity of the data and technology involved in operating the underlying platform present a high level of inherent risk. Board and senior management shortcomings could also increase management risk. EVL-2023-002 reported that in early 2022, the Deputy Director of the Division of Enterprise Regulation (DER) appointed the CSS examiner-in-charge to be responsible for CSS-specific examinations. We confirmed that the scope of the 2022 annual examination included the CSS Board of Managers, and the CSS examiner-in-charge will consider the Board's activities when assigning the examination rating. However, we observed that DER has a key person dependency

because of its level of reliance on the CSS examiner-in-charge. We also noted DER's outdated examination guidance for CSS-related examinations. Our evaluation resulted in two recommendations to the Agency, both of which it accepted. A follow-up compliance review, COM-2023-001, found that CSS adhered to the timing and format requirements in a relevant FHFA advisory bulletin for its monthly reports to DER. Thus, the advisory bulletin has provided a framework under which DER can oversee CSS' cyberattack risks.

FHLBank System

FHFA also serves as supervisor and regulator of the FHLBank System. As we explained in WPR-2023-002, the FHLBank System plays an important role in providing liquidity to member institutions and supporting housing and community development. However, trends in advances reinforce that the FHLBank risk landscape is susceptible to sudden shifts in demand driven by economic events, underscoring the importance of managing and mitigating associated risks. Tied to the FHLBanks' housing and community development mission, in AUD-2023-001, we found that FHFA's Division of Federal Home Loan Bank Regulation performed annual examinations of the FHLBanks' affordable housing programs in accordance with its guidance. We also found that the division did not plan or perform an in-depth review of a significant area within one of the higher risk affordable housing programs for more than 10 years. The division officials told us that this in-depth review was delayed awaiting the amendment of an affordable housing program regulation, which took longer than expected, and was not fully applied until 2021. The audit resulted in three recommendations, which were accepted by FHFA. More broadly, COM-2023-004 found that the Division of Federal Home Loan Bank Regulation complied with its revised Minimum Frequency Guidelines for how often certain examination work programs must be performed.

Agency Operations

Our body of work encompasses not only FHFA's oversight of the regulated entities but also the Agency's internal operations. FHFA must manage information risk as a core component of Agency operations. In AUD-2023-002, we identified multiple exceptions to federal requirements and FHFA standards and guidelines regarding FHFA's oversight of its cloud system and implementation of select controls for which FHFA management is responsible. In our view, these exceptions occurred with sufficient frequency to warrant heightened management attention to the cybersecurity risk posed to its cloud system, and we offered six recommendations to the Agency, which it accepted. Regarding retired electronic media, in COM-2023-003, we found that FHFA secures retired electronic media behind two physical barriers and maintains documentation demonstrating accountability for devices as they are transferred between divisions and, ultimately, outside of the Agency. As we first identified in 2020, we found that FHFA still did not consistently perform inventories of its retired electronic media and did not reconcile discrepancies in its inventory records. Thus, we reopened our 2020 recommendation, which FHFA accepted. In follow-up work on FHFA's offboarding controls, COM-2022-008, we found

that the Agency largely adhered to the tested Offboarding Procedures, but it did not satisfy its own requirements to collect and destroy Personal Identity Verification cards from one out of four personnel possessing such cards who separated from FHFA during the review period. This high failure rate demonstrated that FHFA had not effectively implemented a recommendation from our related 2019 audit. We re-opened that recommendation as a result. In response, FHFA committed to abide by applicable federal standards regarding the collection and destruction of Personal Identity Verification cards.

Investigative Accomplishments

OIG's investigative mission is to prevent and detect fraud, waste, and abuse in the programs and operations of FHFA and its regulated entities. OIG's Office of Investigations executes its mission by investigating allegations of significant criminal and civil wrongdoing that affect the Agency and its regulated entities. The Office conducts investigations in strict accordance with professional guidelines established by the Attorney General of the United States and also with CIGIE's Quality Standards for Investigations.
The Office of Investigations is comprised of highly trained law enforcement officers, investigative counsels, analysts, and attorney advisors. We maximize the impact of our criminal and civil law enforcement efforts by working closely with federal, state, and local law enforcement agencies nationwide.

OIG's Office of Investigations serves as the primary federal law enforcement organization that specializes in deterring and detecting fraud perpetrated against the Enterprises, which collectively hold more than $7.5 trillion of mortgages on their balance sheets. Each year, the Enterprises acquire millions of mortgages worth hundreds of billions of dollars. The Office of Investigations also investigates cases involving the 11 regional FHLBanks, which have over $1.2 trillion in assets, and, in some instances, cases involving banks that are members of the FHLBanks.

Notable Criminal Cases

Former Attorney Found Guilty in Multimillion-Dollar Embezzlement Conspiracy Resulting in the Failure of a Bank, Illinois

On March 10, 2023, in the Northern District of Illinois, after a four-week long trial, former attorney and real estate developer Robert Kowalski was convicted by a federal jury of embezzlement, bankruptcy fraud, and tax fraud charges for his role in an embezzlement conspiracy that led to the 2017 failure of Washington Federal Bank for Savings, a member bank of the FHLBank of Chicago.

Washington Federal was shut down in December 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans.

Evidence at trial revealed Kowalski diverted more than $8 million from the bank, plus property that was rightly the collateral of the bank for other loans. His receipt of embezzled funds was concealed by entering them on the bank's records as loan disbursements.

Mortgage Broker and Document Preparer Sentenced in Origination Fraud Scheme, California

In December 2022, in Los Angeles County Superior Court, a mortgage broker and document preparer were sentenced for their roles in a loan origination scheme that led to over $25 million in exposure for the Enterprises and the approval of fraudulent mortgage loans worth over $8 million.

Alex Dadourian was sentenced to 64 months in prison, while Vartan Pirlant was sentenced to six months in jail, 180 days of home confinement, and two years of probation. Dadourian and Pirlant were also ordered to pay over $8.1 million and $20,000 (jointly and severally), respectively, in restitution.

Dadourian, a licensed mortgage broker for Success Funding, conspired with Pirlant, a document preparer, to defraud financial lenders by taking out 17 mortgage loans based on fraudulent applications and supporting documentation. Together they forged employment verifications and education records used to assess creditworthiness, as well as inflated earnings statements. Dadourian received more than $254,000 in fees and commissions.

$495 Million Settlement in Principle Reached with Credit Suisse to Resolve Allegations of Fraud and Deceit in Sale of Toxic Mortgage-Backed Securities, New Jersey

On October 24, 2022, a consent order and final judgment was entered in Mercer County New Jersey Superior Court against Credit Suisse Securities (USA) LLC, Credit Suisse First Boston Mortgage Securities Corp., and DLJ Mortgage Capital, Inc. (collectively Credit Suisse) for $495 million to resolve a state lawsuit arising from the offer and sale of residential mortgage-backed securities. Many of the loans securitized and sold to investors were guaranteed by the GSEs.

In December 2013, a civil complaint was filed against Credit Suisse by the New Jersey Attorney General's Office on behalf of the New Jersey Bureau of Securities.

According to the complaint, Credit Suisse made material misrepresentations in the offering documents about the risks of the residential mortgage-backed securities, including failing to disclose material defects of the underlying mortgages. Credit Suisse packaged billions of dollars' worth of defective residential loans into publicly traded residential mortgage-backed securities, which were sold to unsuspecting investors through registration statements, prospectuses, and other offering materials containing fraudulent representations about the quality of the underlying loans.

Additionally, the lawsuit alleged: that Credit Suisse failed to disclose to investors the wholesale abandonment of underwriting guidelines designed to ensure that the mortgage loans underlying its securities trusts were made in accordance with appropriate lending guidelines; that numerous loan originators had poor track records of defaults and delinquencies; and that some loan originators had even been suspended from doing business with Credit Suisse.

Conspirator Sentenced in Deed Fraud Scheme, Texas

On February 9, 2023, in the Southern District of Texas, Clarence Roland III was sentenced to 120 months in prison, three years supervised release, and ordered to pay over $3.2 million in restitution and over $1.9 million in a money judgment for his role in a deed fraud scheme where several of the properties were secured with mortgages acquired by the Enterprises. Roland was previously convicted by a federal jury of conspiracy to commit wire fraud affecting a financial institution, wire fraud, and money laundering. According to court documentation, Roland conspired with Arlando Jacobs in a scheme to cancel and challenge mortgage loans held in the name of Jacobs or others.

Jacobs was previously sentenced in the Eastern District of Texas to 51 months in prison, five years supervised release, and ordered to pay $7.6 million in restitution.

According to testimony, Roland and Jacobs solicited other conspirators to establish over 11 business entities or shell companies and office spaces with mailing addresses to carry out their scheme. Roland and others then fraudulently acquired real property by manipulating and filing false deeds and other documents. The conspirators fabricated a series of documents to falsely create the appearance of transferred ownership of real property to the shell companies. They signed documents claiming to represent one of the many entities in the transactions including Fannie Mae. Roland sold the properties and received profits from the sales. The original mortgage liens were not paid off and the mortgage holders were ultimately defrauded.

Business Owner Sentenced in Paycheck Protection Program Fraud Scheme, New Jersey

On June 7, 2022, in the District of New Jersey, Gregory Blotnick was sentenced to 51 months in prison, two years supervised release, and ordered to pay over $4.5 million in restitution and forfeiture for his role in a scheme that defrauded multiple FHLBank member banks to fraudulently obtain over $6.8 million in Paycheck Protection Program forgivable loans. He previously pleaded guilty to wire fraud and money laundering.

According to court documentation, Blotnick submitted 21 fraudulent Paycheck Protection Program loan applications to 13 lenders on behalf of nine purported businesses that he controlled. He falsified information to the lenders, including number of employees, federal

tax returns for his purported businesses, and payroll documentation. Of the approximately $6.8 million sought, Blotnick obtained over $4.5 million in Paycheck Protection Program funds and then misused the loan proceeds, including by transferring funds to brokerage accounts where he placed more than $3 million in losing stock trades.

OFFICE of INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

Office of Inspector General U.S. Department of Housing and Urban Development

The U.S. Department of Housing and Urban Development (HUD), Office of Inspector General (OIG), safeguards HUD's programs from fraud, waste, and abuse and identifies opportunities for HUD programs to progress and succeed.

Background

HUD's mission is to create strong, sustainable, inclusive communities and quality affordable homes for all. HUD is working to strengthen the housing market to bolster the economy and protect consumers; meet the need for quality affordable rental homes; use housing as a platform for improving quality of life; and build inclusive and sustainable communities free from discrimination. Its programs are funded through roughly $75 billion in annual congressional appropriations. While organizationally located within HUD, HUD OIG provides independent oversight of HUD programs and operations.

HUD has two component entities that have a major impact on the Nation's financial system: the Federal Housing Administration (FHA) and the Government National Mortgage Association (Ginnie Mae). As one of the largest providers of mortgage insurance in the world, FHA provides lenders with protection against losses when homeowners and owners of multifamily properties and healthcare facilities default on their loans. FHA has insured approximately 53.7 million single-family properties since its inception in 1934. FHA reported that in fiscal year 2022 it endorsed 982,202 home mortgages (valued at more than $255 billion) through its forward mortgage program, 70% of which were to purchase a home. FHA's portfolio also included 3,525 insured residential care facilities, and 61 hospitals. As of December 2021, FHA had a combined insurance portfolio valued at $1.4 trillion.[4] FHA receives limited congressional funding and is primarily self-funded through mortgage insurance premiums.

Ginnie Mae is a self-financing, U.S. Government corporation in HUD. It approves lenders (known to Ginnie Mae as issuers) to issue mortgage-backed securities (MBS) secured by pools of government-backed home loans. These loans are insured or guaranteed by FHA, HUD's Office of Public and Indian Housing, the U.S. Department of Veterans Affairs, and the U.S. Department of Agriculture. Ginnie Mae guarantees investors the timely payment of principal and interest on MBS backed by the full faith and credit of the United States government. If an

[4] https://www.hud.gov/sites/dfiles/Housing/documents/2022FHAAnnualRptMMIFund.pdf

issuer of an MBS fails to make the required pass-through payment of principal and interest to investors, Ginnie Mae is required to advance the payment as part of its guarantee and, in the instances of issuer default, will assume control of the issuer's MBS pools and the servicing of the loans in those pools. The purchasing, packaging, and reselling of mortgages in a security form frees up funds that lenders use to originate more loans. In fiscal year 2022, Ginnie Mae issued more than $653 billion MBSs, pushing the total MBS outstanding to nearly $2.3 trillion.[5]

HUD OIG Oversight Relating to Financial Matters

HUD OIG strives to influence positive outcomes for HUD programs and operations through timely and relevant oversight, while safeguarding HUD's programs from fraud, waste, and abuse. HUD OIG's oversight efforts focus on identifying and addressing HUD's most significant management challenges, as highlighted in our Top Management Challenges for Fiscal Year 2023 report.[6] Some of the top challenges that HUD faces are affected by the dynamic financial environment and HUD's pandemic relief programs and funds. Ultimately, HUD OIG uses the top challenges it identifies to drive oversight efforts, including in the following areas most related to the financial sector:

- **Mitigating Counterparty Risks in Mortgage Programs** – Through FHA and Ginnie Mae, HUD supports sustainable homeownership and encourages investment in affordable rental housing by insuring mortgage loans lenders provide to traditionally underserved home buyers and to owners of various affordable rental housing, and by guaranteeing payments to investors who purchase securities collateralized by government-insured loans, providing liquidity in this market. FHA and Ginnie Mae must work with outside entities, including property owners, banks, nonbank lenders, and issuers. Each of these outside entities has responsibilities and obligations they must meet in responsibly doing business with the government. FHA, Ginnie Mae, and HUD must identify, mitigate, and manage risks related to each entity (also referred to as "counterparty") to protect the Mortgage Insurance Fund and the Guaranty Fund.

- **Fraud Risk Management** - Fraud negatively impacts the administration, effectiveness, reputation, and success of HUD's programs in carrying out its mission. Beyond monetary losses to the Federal taxpayer, when HUD funds are diverted to fraud, its programs do not receive the financial support intended to meet its critical mission. This is especially egregious since HUD's programs are designed to assist some of America's most vulnerable populations and to provide emergency relief to

[5] https://www.ginniemae.gov/about_us/what_we_do/Annual_Reports/annual_report22.pdf
[6] Top Management Challenges Facing the U.S. Department of Housing and Urban Development for Fiscal Year 2023, issued Nov. 14, 2023, available at https://www.hudoig.gov/reports-publications/top-management-challenges/fy-2023-top-management-challenges

Americans in urgent need of housing assistance. Every dollar diverted to fraud is a dollar that does not go to helping these intended beneficiaries. Further, the reputational harm caused by fraud may result in a negative shift in perception that can lead key stakeholders to lose faith in HUD and its partners. Managing fraud risk is a pervasive challenge across the government. It is critical that HUD address this risk head on since fraud in HUD programs undercuts HUD's ability to meet all of its strategic goals.

- **Sustaining Progress in Financial Management** - Throughout fiscal year 2022, HUD continued to make progress in addressing previously identified financial management weaknesses; however, new instances were also identified. These weaknesses, coupled with continued weaknesses in HUD's internal control framework and financial management systems, demonstrate that HUD must continue to sustain progress it has made as well as implement additional improvements to its financial management environment to achieve a fully capable level of financial maturity. Further, HUD and its component entities must continue sustaining improvements made in financial management to consistently produce reliable and timely financial reports and ensure compliance with significant laws and regulations.

In addition, following the issuance of HUD OIG's Priority Open Recommendations, OIG has been helping HUD resolve the most significant open recommendations, which, if implemented, will have the greatest impact on helping HUD achieve its mission.

HUD OIG Oversight Related to the Financial Sector

During the 1-year period ending March 31, 2023, HUD OIG issued 50 audits, evaluations, and other reviews to strengthen the programs and operations of HUD. Key oversight reports and investigations related the broader financial sector are summarized below.

Ginnie Mae Did Not Ensure That All Pooled Loans Had Agency Insurance[7]

OIG performed a corrective action verification review of the actions taken by Ginnie Mae to implement the recommendations cited in Audit Report 2016-KC-0002, Ginnie Mae Improperly Allowed Uninsured Loans To Remain in Mortgage-Backed Securities Pools, September 21, 2016. OIG found that Ginnie Mae established both a maximum time in which single-family loans could remain pooled without insurance and a process for requiring the removal of pooled loans that remained uninsured after that time. However, the loan-matching process did not ensure that pooled loans would be insured by an agency of the Federal Government, as required by

[7] 2023-KC-0001, available at https://www.hudoig.gov/reports-publications/report/ginnie-mae-did-not-ensure-all-pooled-loans-had-agency-insurance

the MBS Guide. As a result, OIG estimated that at least 3,200 pooled loans with a principal balance of at least $903 million were not matched to agency insurance data files before the certification date. OIG made two additional recommendations, one of which was that Ginnie Mae update and synchronize its procedures to include notifications that provide issuers with unmatched loans adequate time to take corrective action to comply with the requirements of the MBS Guide.

Ginnie Mae Mostly Implemented a Crisis Readiness Program That Followed Federal Guidance[8]

OIG audited Ginnie Mae's crisis readiness and response actions before the onset of and during the coronavirus disease 2019 (COVID-19) pandemic to determine whether Ginnie Mae had implemented a crisis readiness program, including precrisis planning, a crisis readiness plan, and a crisis management strategy, that followed Federal guidance. OIG determined that Ginnie Mae generally followed Federal guidance in precrisis planning and executed its crisis management strategy with respect to the COVID-19 pandemic. However, it did not have an agency wide crisis readiness plan, addressing likely hazards arising from a crisis, or include all key elements in line with crisis guidance from CIGFO. OIG recommended that Ginnie Mae develop and implement an agency wide crisis readiness plan addressing likely hazards arising from a crisis, to include all key elements that align with CIGFO crisis guidance.

HUD Communicated Critical Information to Homeowners About COVID-19 Policies but Improvements Can Be Made[9]

OIG audited HUD's efforts to proactively communicate information to homeowners with FHA-insured mortgages through its website, its joint website, and other proactive methods about protections, repayment options, loss mitigation options, and responsibilities related to COVID-19. This audit determined that HUD proactively communicated critical information to homeowners; however, HUD's COVID-19 Resources for Homeowners webpage did not clearly present the deadline for requesting forbearance, detail available loss mitigation options after forbearance, and include detailed information for homeowners with reverse mortgages. Additionally, letters mailed to homeowners may not have been timely for some and did not discuss loss mitigation. As a result, homeowners may not have been aware of available protections and loss mitigation options. OIG made five recommendations to help HUD address these issues.

[8] 2023-KC-0004, available at https://www.hudoig.gov/reports-publications/report/ginnie-mae-mostly-implemented-crisis-readiness-program-followed-federal

[9] 2023-NY-0001, available at https://www.hudoig.gov/reports-publications/report/huds-communication-homeowners-about-covid-19-policies

Opportunities Exist for Ginnie Mae To Improve Its Guidance and Process for Troubled Issuers[10]

OIG audited Ginnie Mae's guidance and process for managing troubled issuers to assess Ginnie Mae's policy and procedures for rapid relocation extinguishments and assess Ginnie Mae's implementation of a previous OIG recommendation to develop and implement controls to identify the total impact of a large or multiple-user default (the maximum size default Ginnie Mae could adequately execute) and individual issuers' ability to adapt to changing market conditions. This audit determined that Ginnie Mae's guidance and process for troubled issuers contained gaps. OIG made six recommendations to help Ginnie Mae address the issues identified.

Improvements Are Needed in HUD's Fraud Risk Management Program[11]

OIG audited HUD's fraud risk management program at the enterprise and program-office levels and assessed its overall maturity. OIG's objective was to determine HUD's progress in implementing a fraud risk management framework at the enterprise and program-office levels that encompasses control activities to prevent, detect, and respond to fraud. OIG found that all four phases of HUD's fraud risk management program were in the early stages of development, or at an "ad hoc" maturity level. OIG recommended that HUD (1) perform a complete agency wide fraud risk assessment and develop a plan to improve the maturity of HUD's fraud risk program; (2) communicate to program staff the differences among HUD's processes for enterprise risk management, the Payment Integrity Information Act of 2019, and HUD's financial risk management risk assessment; and (3) develop policies, procedures, and strategies for collecting and analyzing data to identify fraud in HUD's programs, promote fraud awareness, and develop antifraud risk mitigation tools.

Investigative Activity and Outcomes

OIG also helps protect HUD from counterparty risk by conducting investigations of alleged fraud negatively affecting the FHA insurance funds and securing recoveries. OIG also investigates misconduct associated with the FHA and Ginnie Mae programs. For the one year period ending March 31, 2023, HUD OIG Office of Investigation completed 80 single-family investigations of fraud against the FHA insurance fund. Many of the investigations focused on loan origination fraud involving forward mortgages. Recoveries from these cases totaled more than $106 million (criminal, civil, and administrative recoveries).

Key examples of significant cases include:

[10] 2023-KC-0003, available at https://www.hudoig.gov/reports-publications/report/opportunities-exist-ginnie-mae-improve-its-guidance-and-process

[11] 2023-FO-0001, available at https://www.hudoig.gov/reports-publications/report/improvements-are-needed-huds-fraud-risk-management-program

Investigation of Alleged Misconduct by a Ginnie Mae Senior Vice President[12]

OIG initiated an investigation upon receipt of information alleging that a Ginnie Mae Senior Vice President may have provided nonpublic Ginnie Mae information to representatives of a private investment firm. The investigation found that the employee (1) provided nonpublic information about a Ginnie Mae issuer to the firm that the employee knew or should have known was not authorized for public release, (2) provided the firm with preferential treatment or created the appearance that he was doing so in certain of his interactions with it, and (3) did not take sufficient care to avoid creating the appearance that he may have been acting unlawfully in certain of his interactions with the firm. OIG found that this conduct violated 5 CFR (Code of Federal Regulations) 2635.703, 2635.101(b)(8), and 2635.101(b)(14). OIG referred this matter to the appropriate office within the U.S. Department of Justice for prosecutorial consideration, and no prosecution resulted. OIG also referred its findings in this matter to HUD and Ginnie Mae for any administrative action they may deem appropriate.

Brothers Ordered to Pay Over Half a Million Dollars in Familial Mortgage Fraud Scheme[13]

Calvin Abramowitz, a borrower, and Philip Abramowitz, a seller, were collectively sentenced in U.S. District Court for the District of Maryland to 12 months incarceration, 36 months supervised release, and ordered to pay $587,858 restitution to FHA, of which $378,684 is to be paid jointly and severally pursuant to their earlier guilty pleas to conspiracy to commit bank fraud. The defendants conspired to defraud financial institutions by failing to disclose their familial relationship and submitting falsified documents.

Trio Sentenced to More Than 5 Years Incarceration Related to Mortgage Fraud Conspiracy[14]

Joseph Bates III and George Kritopoulos, real estate developers, along with David Plunkett, accountant, were collectively sentenced in U.S. District Court for the District of Massachusetts to 66 months incarceration, 96 months supervised release, and ordered to pay $2,444,138 restitution to various Federal government and private entities, of which $286,155 was payable to HUD. Kritopoulos was convicted by jury trial to conspiracy, wire fraud, aiding in the preparation of a false tax return, obstruction of justice, and bank fraud. Bates pled guilty to conspiracy, wire fraud, and bank fraud. Plunkett pled guilty to bank fraud and aiding in the submission of a false tax return. From 2006 until 2015, the defendants engaged in a scheme to defraud financial institutions by submitting fraudulent documents to qualify borrowers they recruited for conventional and FHA-insured mortgages.

[12] https://www.hudoig.gov/reports-publications/investigation-summary/investigation-alleged-misconduct-ginnie-mae-senior-vice
[13] https://www.justice.gov/usao-md/pr/baltimore-business-owner-sentenced-federal-prison-fraudulently-obtaining-federally
[14] https://www.justice.gov/usao-ma/pr/salem-man-sentenced-four-years-prison-decade-long-mortgage-fraud-scheme

Real Estate Professionals Sentenced to More Than 14 Years Incarceration and More Than $10 Million in Restitution[15]

Three real estate professionals were collectively sentenced in U.S. District Court to more than 14 years' incarceration and 15 years supervised release and ordered to pay jointly and severally more than $10 million in restitution, of which more than $6 million is payable to the FHA. For more than 3 years, the conspirators recruited buyers to purchase multiunit residential properties owned by a business entity controlled by one of the subjects and used false information about the buyers' assets and income to support fraudulent mortgage loan applications to a mortgage company. They falsified the buyers' loan applications by falsely increasing assets. They then transferred cash from the business entity's and others' accounts to the buyers' bank accounts and falsified documents to hide the transfers. After the loans were approved, the conspirators returned the funds to the business entity. When the transactions were closed, the conspirators defrauded the mortgage company by hiding that the business entity and others, not the buyers, had provided the cash to close the transactions. Ultimately, the buyers were not able to repay the loans, which resulted in losses to several financial institutions and FHA.

Direct Endorsement Lender Agreed to Pay Over $1 Million to Resolve False Claims Act Violations[16]

American Financial Network, an FHA direct endorsement lender, entered into a settlement agreement with the United States to resolve allegations that the company approved mortgages that did not meet FHA requirements. American Financial Network agreed to pay more than $1 million, of which $518,572 is payable to FHA. For nearly 8 years, American Financial Network knowingly failed to perform required quality control reviews and approved loans that did not qualify for FHA insurance.

Money Mules Ordered To Pay More Than $1.2 Million in Restitution[17]

Money mules John Fuss, Jeremy Christopher, Tracey Brookshier, Mary Booth, Ronnie Booth, and Perry Crenshaw were collectively sentenced in U.S. District Court to 64 months incarceration, 6 years supervised release, and 13 years probation and ordered to pay more than $1.2 million in restitution to various victims. Ronnie Booth, Mary Booth, and Brookshier were sentenced in connection with their earlier guilty pleas to aiding and abetting the operation of an unlicensed money-transmitting business. Fuss, Jones, and Crenshaw were sentenced in connection with their earlier guilty pleas to conspiracy to commit money laundering. For more than 7 years, the conspirators participated in a money-laundering operation involving multiple fraud schemes in which victims were instructed to send funds to the conspirators through

[15] https://www.justice.gov/usao-nj/pr/essex-county-man-sentenced-108-months-prison-mortgage-and-securities-fraud-schemes#:~:text=The%20108%2Dmonth%20sentence%20imposed,guilty%20to%20in%20this%20case.
[16] https://www.justice.gov/usao-edwa/pr/california-mortgage-lender-agrees-pay-more-1-million-resolve-fraud-allegations
[17] More information about the investigation is available at https://www.justice.gov/usao-edtx/pr/six-charged-transnational-money-laundering-operation-involving-elder-fraud.

intimidation or the promise of receiving a service or product in return. Victims of the mortgage modification scheme included FHA-insured borrowers, who were solicited by individuals purporting to be with the victims' mortgage companies and falsely promised lower interest rates and monthly mortgage payments. More than 1,000 victims were impacted by the various schemes.

Office of Inspector General
National Credit Union Administration

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) promotes the economy, efficiency, and effectiveness of NCUA programs and operations and detects and deters fraud, waste and abuse, thereby supporting the NCUA's mission of providing, through regulation and supervision, a safe and sound credit union system that promotes confidence in the national system of cooperative credit.

Background

The Under the IG Act, the OIG conducts independent audits, investigations, and other activities and keeps the NCUA Board and the Congress informed of its work. In addition to the duties set out in the IG Act, the Federal Credit Union Act requires the OIG to conduct a material loss review of an insured credit union if the loss to the NCUA's Share Insurance Fund exceeds $25 million and an amount equal to 10 percent of the total assets of the credit union at the time in which the NCUA Board initiated assistance or was appointed liquidating agent. In addition, for any loss to the Share Insurance Fund that does not meet the threshold, the Federal Credit Union Act requires the OIG to conduct a limited-scope review to determine whether unusual circumstances exist related to the loss that would warrant conducting a full-scope MLR.

OIG Reports Related to the Broader Financial Sector

We issued a report on the Top Management and Performance Challenges facing the NCUA, and related audit reports, which can also apply to the broader financial sector:

- Managing Interest Rate Risk and Liquidity Risk
- Cybersecurity and IT Governance – Protecting Systems and Data
- Risks Posed by Third-Party Service Providers
- Industry Consolidation and Challenges Facing Small Credit Unions
- Supporting Diversity in the Credit Union Industry

With regard to the first challenge we identified, high levels of interest rate risk can increase a credit union's liquidity risks, contribute to asset quality deterioration and capital erosion, and put pressure on earnings. Credit unions must be prudent and proactive in managing interest rate risk and the related risks to capital, asset quality, earnings, and liquidity. This is particularly the case for those credit unions whose assets are concentrated in fixed-rate long term mortgages that were originated when interest rates were at record lows.

With regard to cybersecurity challenges, this remains a significant, persistent, and ever-changing threat to the financial sector. Credit unions' growing reliance on increasingly complex technology-related operating environments exposes the credit union system to escalating cyberattacks. Cyberattacks can affect the safety and soundness of institutions and lead to their failure, thus causing losses to the NCUA's Share Insurance Fund. The prevalence of malware, ransomware, distributed denial of service attacks, and other forms of cyberattacks are causing challenges at credit unions of all sizes, which will require credit unions to continually evolve and adapt to the changing threat environment to ensure containment. To ensure the NCUA remains vigilant in protecting its own systems and data, we conducted an audit to assess how well the agency is preventing and detecting cyber threats. Specifically, our audit assessed the effectiveness of the NCUA's firewalls and Security Information and Event management (SIEM) solution to determine if they were designed and implemented to prevent and detect cybersecurity threats to the NCUA's network. We concluded that the NCUA adequately designed and implemented its firewall and SIEM security technologies to prevent and detect cybersecurity threats. However, we noted weaknesses related to account recertification processes for privileged users with access to cybersecurity tools and controls around the SIEM tool audit logging, visibility, and retention processes.

With regard to the challenge posed by the NCUA's lack of credit union vendor oversight authority, the NCUA cannot accurately assess the actual risk present in the credit union system or determine if the risk-mitigation strategies of credit union service organizations and third-party vendors, which provide much of the industry's information technology infrastructure, are adequate and can effectively protect the system from potential attacks. This regulatory blind spot leaves thousands of credit unions, millions of credit union members, and billions of dollars in assets potentially exposed to unnecessary risks. To address this, the NCUA continues to request comparable authority as its counterparts on the Federal Financial Institutions Examination Council to examine credit union service organizations and third-party vendors. We conducted an audit in 2020 that concluded that the NCUA should be provided this authority. Both GAO and the Financial Stability Oversight Council also support providing the NCUA vendor authority. In 2022, the House Financial Services Committee approved a bill to provide the NCUA with vendor authority and that measure was later added to the House-approved 2023 National Defense Authorization Act (NDAA). In the Senate, S. 4698, the Improving Cybersecurity of Credit Unions Act, was introduced to provide the NCUA this authority. However, the provision for vendor authority was not included in the final NDAA or any other statute.

With regard to the challenge of industry consolidation, we noted that small credit unions face challenges to their long-term viability for a variety of reasons, including lower returns on assets, declining membership, high loan delinquencies, increasing non-interest expenses, and a lack of succession planning for credit union boards and key personnel. If current consolidation trends persist, there will be fewer credit unions in operation and those that remain will be considerably larger and more complex. To ensure the NCUA continues to help the credit union system grow, we have started an audit that is reviewing the NCUA's chartering activities, including determining whether the NCUA's efforts to streamline its chartering process have made it more efficient and effective for potential organizers interested in applying for a new federal credit union charter, and whether the NCUA has adequately communicated its revised chartering process to potential organizers interested in applying for a charter and operating a federally insured credit union.

Regarding the challenge of lack of access to the financial system by minority communities, in September 2022, we issued a report titled Audit of the NCUA's Minority Depository Institutions Preservation Program (MDIPP) to determine whether the NCUA's MDIPP achieved its goals. Our report determined that the NCUA took actions to preserve the present number and minority character of MDIs, provided technical assistance to prevent insolvency of MDIs, promoted and encouraged the creation of MDIs, and provided MDIs with training, technical assistance, and educational programs. However, based on our survey of MDIs, we believe the NCUA should evaluate its communications with MDIs. In addition, we determined the NCUA lacked a process to conduct a required review to determine if MDIs continue to meet the MDI definition.

In addition to our Management Challenges report and audits related to the challenges identified in the report, in December 2022, we issued an audit report that assessed the NCUA's Continuity of Operations (COOP) program, which could be instructive for the broader financial sector. Our audit determined the COOP program operated in accordance with applicable laws, regulations, policies, and procedures and was ready and able to execute should the need arise. However, we also determined the NCUA should perform a full failover test of its IT network to ensure management is made aware of any potential weaknesses and correct them, as necessary, and that the Office of Continuity and Security Management (OCSM) and the Office of the Chief Information Officer (OCIO) needed to improve communication with each other regarding COOP and security matters.

We are also currently auditing the NCUA's quality assurance program, which assesses all activities relating to the oversight of Federally insured credit unions. The results of our audit may raise concerns that apply to the broader financial sector.

Finally, we participated in the two CIGFO working groups that worked on the report titled Guidance in Preparing for and Managing Crises, and the audit of FSOC's response to the May 20, 2021, Executive Order on Climate-Related Financial Risk. We also continued to participate in a CIGFO working group designed to coordinate investigative efforts combating fraud associated with CARES Act stimulus programs.

Office of Inspector General
U.S. Securities and Exchange Commission

The U.S. Securities and Exchange Commission (SEC, Commission, or agency) Office of Inspector General (OIG) promotes the integrity, efficiency, and effectiveness of the critical programs and operations of the SEC and operates independently of the agency to help prevent and detect fraud, waste, and abuse in those programs and operations, through audits, evaluations, investigations, and other reviews.

Background

The SEC's mission is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. The SEC strives to promote capital markets that inspire public confidence and provide a diverse array of financial opportunities to retail and institutional investors, entrepreneurs, public companies, and other market participants. Its core values consist of integrity, excellence, accountability, teamwork, fairness, and effectiveness. The SEC's goals are protecting the investing public against fraud, manipulation, and misconduct; developing and implementing a robust regulatory framework that keeps pace with evolving markets, business models, and technologies; and supporting a skilled workforce that is diverse, equitable, inclusive, and fully equipped to advance agency objectives.

The SEC is responsible for overseeing the nation's securities markets and certain primary participants, including broker-dealers, investment companies, investment advisers, clearing agencies, transfer agents, credit rating agencies, and securities exchanges, as well as organizations such as the Financial Industry Regulatory Authority, Municipal Securities Rulemaking Board, Public Company Accounting Oversight Board, Securities Investor Protection Corporation, and the Financial Accounting Standard Board. Under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), the agency's jurisdiction was expanded to include certain participants in the derivatives markets, private fund advisers, and municipal advisors.

The SEC's headquarters are in Washington, DC, and the agency has 11 regional offices located throughout the country. The agency's functional responsibilities are organized into 6 divisions and 25 offices, and the regional offices are primarily responsible for investigating and litigating potential violations of the securities laws. The regional offices also have examination staff to inspect regulated entities such as investment advisers, investment companies, and broker-dealers. As of March 2023, the SEC employed 4,630 full-time equivalents.

The SEC OIG was established as an independent office within the SEC in 1989 under the Inspector General Act of 1978, as amended (IG Act). The SEC OIG's mission is to promote the integrity, efficiency, and effectiveness of the SEC's critical programs and operations. The SEC OIG prevents and detects fraud, waste, and abuse through audits, evaluations, investigations, and other reviews related to SEC programs and operations.

The SEC OIG Office of Audits conducts, coordinates, and supervises independent audits and evaluations of the SEC's programs and operations at its headquarters and 11 regional offices. These audits and evaluations are based on risk and materiality, known or perceived vulnerabilities and inefficiencies, and information received from the Congress, SEC staff, the U.S. Government Accountability Office, and the public.

The SEC OIG Office of Investigations performs investigations into allegations of criminal, civil, and administrative violations involving SEC programs and operations by SEC employees, contractors, and outside entities. These investigations may result in criminal prosecutions, fines, civil penalties, administrative sanctions, and personnel actions. The Office of Investigations also identifies vulnerabilities, deficiencies, and wrongdoing that could negatively impact the SEC's programs and operations.

In addition to the responsibilities set forth in the IG Act, Section 966 of Dodd-Frank required the SEC OIG to establish a suggestion program for SEC employees. The SEC OIG established its SEC Employee Suggestion Program in September 2010. Under this program, the OIG receives, reviews, considers, and recommends appropriate action with respect to such suggestions or allegations from agency employees for improvements in the SEC's work efficiency, effectiveness, and productivity, and use of its resources, as well as allegations by employees of waste, abuse, misconduct, or mismanagement within the SEC.

SEC OIG Work Related to the Broader Financial Sector

In accordance with Section 989E(a)(2)(B)(i) of Dodd-Frank, below is a discussion of the SEC OIG's completed and ongoing work, focusing on issues that may apply to the broader financial sector.

Completed Work

Enforcement Investigations: Measures of Timeliness Showed Some Improvement But Enforcement Can Better Communicate Capabilities for Expediting Investigations and Improve Internal Processes: Report No. 576; February 15, 2023

The SEC Division of Enforcement (Enforcement) is responsible for civil enforcement of the federal securities laws. Each year, Enforcement advances the SEC's mission by investigating and bringing hundreds of actions against individuals and entities for fraud and other misconduct, and by securing remedies that protect investors and the markets. In conducting investigations, Enforcement strives to balance the need for complete, effective, and fair investigations with the need to file enforcement actions in as timely a manner as possible.

We conducted this evaluation to (1) assess Enforcement's efforts to expedite and accelerate the pace of investigations, where possible and appropriate, and (2) review Enforcement's performance goal-setting and monitoring processes related to the pace of investigations.

During the period we reviewed (fiscal year [FY] 2016 to FY 2021), Enforcement's efforts aligned with federal and agency requirements for performance goal-setting and monitoring as part of annual performance planning and reporting. Enforcement supported the SEC's efforts to develop performance plans and goals, and provided reliable data to support such goals and reporting requirements. We reviewed and tested data supporting two prior SEC performance goals, for which Enforcement was responsible, and noted no concerns with respect to completeness and accuracy. Metrics associated with these goals measured (1) the pace of investigations that lead to the filing of enforcement actions, and (2) the average number of months between the opening of an investigation and the filing of the first enforcement action arising from that investigation. As of October 2018, Enforcement no longer reports at the agency level on these performance goals. Nonetheless, Enforcement actively monitored the pace of investigations through regular reports, mandatory quarterly case review meetings, and other routine meetings.

Our analysis of case data from FY 2016 to FY 2021 found that two measures of timeliness showed some improvement. Specifically, the average time from opening an investigation to the first filed enforcement action decreased from 24.1 months to 22.8 months, and the percentage of first filed enforcement actions filed within 2 years improved from 53 percent to 54 percent. However, some respondents to a survey we conducted of Enforcement personnel disagreed that Enforcement management had sufficiently taken actions to expedite investigations. For example, out of about 320 staff-level respondents:

- 70 (or about 22 percent) disagreed or strongly disagreed that Enforcement management promoted best practices regarding efficiencies in various phases of Enforcement investigations;
- 63 (or about 20 percent) disagreed or strongly disagreed that Enforcement management effectively promoted opportunities to leverage data analytics capabilities; and

- 65 (or about 20 percent) disagreed or strongly disagreed that Enforcement management provided training on tools that help staff expedite investigations.

Management provided us examples of actions taken to expedite investigations but can better communicate across Enforcement its capabilities for expediting investigations.

Additionally, although about 87 percent of all respondents to our survey (managers and staff) agreed or strongly agreed that Enforcement management emphasizes the importance of expediting investigations, some respondents reported that improvements to internal processes (including the action memo process), systems, and Enforcement staffing and workload may help expedite investigations.

Lastly, we found significant differences in the processing times for matters under inquiry handled by different SEC regional offices and, overall, personnel expressed concerns about the timely closing of investigations as soon as it becomes apparent that no enforcement action will be recommended. Timely action in these respects can help Enforcement make more efficient use of its limited resources and focus on those matters that warrant further attention and investigation.

We issued our final report on February 15, 2023, and recommended that Enforcement: (1) review processes for communicating across the organization information on existing capabilities and resources that help expedite investigations, (2) develop a plan to address causes of investigative delays noted in our survey of Enforcement personnel, and (3) review Enforcement-wide procedures for timely processing matters under inquiry and controls that ensure investigations are timely closed to identify and disseminate best practices. The report is available on our website at https://www.sec.gov/files/enforcement-investigat-meas-timeliness-show-some-improvement-enforcement-can-better-comm.pdf.

SEC's Whistleblower Program: Additional Actions Are Needed To Better Prepare for Future Program Growth, Increase Efficiencies, and Enhance Program Management; Report No. 575; December 19, 2022

According to the SEC Office of the Whistleblower (OWB), assistance and information from a whistleblower who knows of possible securities law violations can be among the most powerful weapons in the law enforcement arsenal of the SEC. Since the inception of the SEC whistleblower program in 2011, the Commission has awarded more than $1.3 billion to over 300 individuals. In FY 2021, the SEC awarded more than it ever had (about $564 million) to the largest number of whistleblowers (108) in a single year.

We conducted this audit to assess the growth of the SEC's whistleblower program and the functioning of key program controls. The engagement scope period was from FYs 2017 to 2021 and included whistleblower hotline calls, award claims, and awards that took place before and after the SEC's September 2020 adoption of amended whistleblower program rules.

We reviewed whistleblower payments for a sample of Final Orders issued in FY 2021 and determined that, in those instances, whistleblowers were paid in accordance with applicable rules and Final Orders. In addition, payments were approved before issuance, in accordance with OWB's policies and procedures. Moreover, the SEC took steps to improve whistleblower claims processing and tracking procedures, including (1) implementing an initiative to more efficiently develop the initial drafts of attorney declarations, (2) adopting certain rule amendments, and (3) implementing a modernized claims tracking system. However, before these efforts, OWB was experiencing a significant backlog in processing whistleblower claims, which increased the amount of time whistleblowers waited before receiving the Commission's Final Order. In addition, aspects of some improvements were not consistently implemented or fully leveraged. As a result, opportunities remain for OWB to further improve as the whistleblower program continues to grow.

We also reviewed a sample of claims packages and supporting artifacts and determined that some Claims Review Staff (CRS) determinations were approved when more than half of the CRS members were absent or recused. This occurred because the CRS did not implement an operating agreement detailing certain processes or control activities, such as the number of CRS members required to approve a claims package. Because the Commission relies on the CRS with respect to whistleblower awards, including denials and approvals of multi-million dollar awards, we believe a lack of guidelines, rules, and standards governing CRS actions and decisions increases the risk to the Commission's Final Orders.

When reviewing OWB's internal data management, we identified some inaccurate or incomplete data. These deficiencies occurred, at least in part, because OWB did not establish effective controls over manually inputted data entries used to track whistleblower claims and manage the whistleblower program. Without such controls, OWB continues to risk inaccurate and incomplete reporting of claims tracking data and, in some cases, delays in key whistleblower program processes.

We also found that OWB took steps to effectively communicate with external parties and promote awareness of the program. However, OWB did not always (1) timely respond to whistleblower hotline voicemails or maintain information to assess the timeliness of responses; (2) notify helpful whistleblowers that a time-sensitive opportunity to file a whistleblower claim was available, as instructed by OWB policy; and (3) post to its webpage the Commission's Final Orders. These conditions occurred, in part, because OWB policies and procedures did not sufficiently address these issues, creating opportunities for OWB to improve aspects of whistleblower program communication.

Lastly, we identified two matters that did not warrant recommendations. We discussed these matters with agency management and encourage management to consider any actions needed in response.

We issued our final report on December 19, 2022, and made eight recommendations to help further increase efficiencies in the SEC's whistleblower program, better prepare for future whistleblower program growth, reduce risk, and improve controls over whistleblower program data and communication with external parties. The report is available on our website at https://www.sec.gov/files/secs-whistleblower-program-additional-actions-needed-report-no-575.pdf.

Final Management Letter: Changes to the Internal Review Process for Proposed Rules May Impact the Office of the Advocate for Small Business Capital Formation and the Office of the Investor Advocate; September 29, 2022

During a recent OIG evaluation, we identified a matter related to the agency's internal communication and coordination specific to the rulemaking process. We previously identified an opportunity to strengthen communication and coordination across the SEC's divisions and offices as an emerging theme in our October 2021 statement on SEC's management and performance challenges (U.S. Securities and Exchange Commission, Office of Inspector General, *The Inspector General's Statement on the SEC's Management and Performance Challenges October 2021* [October 8, 2021]). Our observations in the course of conducting the Office of the Advocate for Small Business Capital Formation (OASB) evaluation demonstrate that strengthening communication and coordination remains a growth area for the SEC.

OASB and the Office of the Investor Advocate (OIAD) were established pursuant to Congressional mandates involving a measure of independence. Among other things, these offices are statutorily required to help ensure that the concerns of specific SEC stakeholders (namely, small businesses and investors) are appropriately considered as decisions are being made and policies are being adopted at the Commission, at self-regulatory organizations, and in Congress. With respect to agency rulemaking, OASB and OIAD rely on the SEC's rulemaking divisions and offices to timely provide drafts of proposed rules for review and comment.

Around December 2021, the Office of the Chair modified the process for coordinating internal reviews of draft agency rules, resulting in OASB and OIAD receiving only fatal flaw drafts of proposed rules for a brief period. This change was neither formally documented nor communicated to those offices, and, according to the former directors of OASB and OIAD, they were not aware of the change until after it took effect. Although OASB and OIAD personnel stated that they generally were able to carry out their responsibilities during this period, changes to internal processes likely to impact their review and comment related to draft proposed agency rules may unintentionally limit OASB's and OIAD's ability to fulfill their advocacy roles and carry out office functions, and could hinder effective collaboration and information sharing across the agency.

On September 29, 2022, we issued our final management letter on this topic. Although we commended management's commitment to promoting effective and collaborative information sharing across the SEC's divisions and offices, we encouraged the Office of the Chair to consider, as a management practice, notifying OASB and OIAD before future changes to the rulemaking process, potentially impacting these offices, are implemented.

This management letter is available on our website at https://www.sec.gov/files/finl-mgmt-ltr-changes-internal-review-process-prop-rules-may-impact-oasb-capital-formation-and-oia.pdf.

OASB Complied With Statutory Requirements But Can Improve As It Matures; Report No. 573; August 30, 2022

OASB is an independent office of the SEC established pursuant to the SEC Small Business Advocate Act of 2016 (Advocate Act). OASB's mission is to advance the interests of small businesses and their investors at the SEC and in the capital markets.

We conducted this evaluation to assess OASB's design and implementation of operations, policies, and controls—including coordination and collaboration with other SEC divisions and offices and external stakeholders—to determine whether OASB has met applicable statutory requirements and strategic goals and objectives. Specifically, we sought to (1) evaluate OASB's processes for planning and conducting outreach and engagement activities and for assessing the performance of such activities; (2) assess the design and implementation of OASB's rulemaking feedback process; and (3) verify whether OASB was organizing and executing the SEC's annual Small Business Forum, preparing an independent annual report, serving as a member of the Small Business Advisory Committee, and consulting with the Investor Advocate as required.

We determined OASB effectively established a new independent organization and complied with the statutory requirements outlined in the Advocate Act. Specifically, since commencing operations in January 2019, OASB has done the following:

- conducted outreach events, including educational activities;
- assisted small businesses and their investors;
- analyzed the potential impact of proposed self-regulatory organizations' rules and SEC rulemaking on small businesses and their investors;
- consulted with the SEC Investor Advocate;
- issued annual independent reports on activities;
- participated on the Small Business Advisory Committee; and
- planned, organized, and executed the SEC's annual Small Business Forum.

Although the Advocate Act does not require OASB to coordinate with other SEC divisions and offices, many of the OASB's functions require OASB personnel to work closely with other divisions and offices. We met with personnel from SEC divisions and offices that OASB coordinated with, and none of them identified any challenges or gaps in coordination with OASB.

OASB created a Foundational Business Plan (April 2019) that identified its office's mission and provided a framework for reaching full-scale programming. OASB then published a strategic plan on July 9, 2021, that outlined 4 key goals and 11 strategies. Although OASB identified goals in its strategic plan, OASB did not develop performance measures (qualitative and/or quantitative) to assess the efficacy of key activities in its strategic goals. Without performance measures, OASB potentially limits (1) the effectiveness of key programmatic activities, and (2) its ability to make data-driven improvements, as needed, to ensure that OASB achieves its strategic goals.

Furthermore, although OASB issued policies and procedures, the documents in effect at the time of our review did not include detailed information about workflows, responsibilities, data collection and management, or the expected timing of certain actions, all of which OASB personnel described to us when we asked about OASB's standard practices. In addition, OASB's Outreach Management System (OMS) User Guide and OMS Admin User Guide did not offer detailed data entry information for the OMS system. Without detailed policies and procedures, as OASB matures and grows as an organization, there is an increased risk that its processes may not be followed correctly, reviews of SEC and self-regulatory organizations proposed rules may be performed inconsistently, and decision making may not be documented properly.

We issued our final report on August 30, 2022, and made two recommendations to strengthen OASB's programs and operations as it matures, including (1) identifying and establishing performance measures for activities, and (2) updating OASB's policies and procedures. The report is available on our website at https://www.sec.gov/files/oasb-complied-statutory-requirements-can-improve-it-matures-rpt-573.pdf.

Ongoing Work

Review of SEC Controls Over Public Comments Submitted Online and Actions Taken in Response to a Known Error

Rulemaking is the process by which federal agencies promulgate rules. In some instances, rulemaking implements legislation passed by Congress and signed into law by the President. Other rulemaking updates rules under existing laws or creates new rules within an agency's authority. Federal agencies, including the SEC, are generally required to give interested persons an opportunity to participate in the rulemaking process through submission of written data, views, or arguments (referred to as comments or public comments). The SEC invites interested persons to comment on SEC proposed rules and self-regulatory organization filings, among other matters, using several methods, including online through an internet comment form (also known as a webform). In 2022, the SEC disclosed a technological error that resulted in a number of public comments submitted through the Commission's internet comment form not being received by the Commission. Subsequently, we initiated a review of the SEC's (1) controls over public comment letters submitted online, and (2) actions and response efforts since notifying us of the webform error in August 2022.

The results of our completed review will be reported in the next annual reporting period.

Special Inspector General for the Troubled Asset Relief Program

The mission of the Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) is to prevent and detect fraud, waste, and abuse in the more than $442 billion appropriated by Congress through the Emergency Economic Stabilization Act (EESA) and $2 billion funded through the Consolidated Appropriations Act of 2016, and to promote economy, efficiency, effectiveness, and accountability in these economic stability programs. SIGTARP conducts investigations of suspected illegal activity in, and independent audits of, these EESA long-term economic stability programs.

Background

EESA has two parts:

> (1) Short-term Treasury purchases of "troubled assets," which led to investments in banks, insurance companies and automotive companies - these programs have been largely completed, as has SIGTARP's work in this area; and
>
> (2) Long-term programs intended to bring economic stability to the financial industry and communities by protecting home values and preserving homeownership - programs that spent over $1 billion during fiscal years 2020-2021, and will continue to operate until 2024.

Under these long-term economic stability programs, the Department of Treasury and Fannie Mae (with assistance from Freddie Mac) run a program that funds incentives to more than 150 financial institutions, including some of the largest in our nation, to lower mortgage payments to terms that are affordable and sustainable for homeowners at risk of foreclosure. Treasury also funded grant-like programs administered by housing finance agencies in 19 states. This included assistance for homeowners unemployed, underemployed, or suffering other hardships due to the COVID-19 pandemic.

SIGTARP is primarily a federal law enforcement office. SIGTARP investigations have resulted in criminal charges against 471 defendants with a 96% DOJ conviction rate. Courts have sentenced to prison 321 defendants, including 75 bankers. SIGTARP's investigations have also resulted in DOJ, the SEC, and others bringing enforcement actions against 25 banks or corporations, including some of the largest financial institutions.

More than $11 billion has been recovered from SIGTARP investigations – a cumulative 28 times return on investment. So far in FY 2023, the government has recovered $1,570,420.

SIGTARP's Select Audit Results (April 1, 2022 to March 31, 2023)

Four Released Evaluations Pertain to the Home Affordable Modification Program (HAMP)

In April and May 2022, SIGTARP released three evaluations examining different aspects of HAMP. In two of the evaluations, SIGTARP identified key characteristics of homeowners and mortgage servicers in HAMP using Treasury's data and other relevant data sources. For the third evaluation, SIGTARP reviewed Treasury's oversight of mortgage servicers participating in HAMP. SIGTARP examined Treasury's oversight of HAMP servicers, as well as oversight conducted on behalf of Treasury by Freddie Mac and Fannie Mae. The results of these evaluations provided valuable information and recommendations to Treasury, Congress, and the public on who is currently benefitting from HAMP and the servicers participating in the program, and how federal taxpayer dollars are being used.

SIGTARP issued its final evaluation in March 2023. The evaluation was an analysis of previously issued HAMP and HHF recommendations. Objectives were to summarize the findings and recommendations SIGTARP made in its reports and other products on HHF and HAMP, to assess the status of the recommendations, and to identify lessons learned for ongoing and future housing programs.

SIGTARP's products identified findings that led to 285 recommendations on the HHF (221) and HAMP (64) programs. SIGTARP organized its recommendations by three categories including (1) promote economy, efficiency, and effectiveness of the programs; (2) prevent and detect fraud, waste, and abuse; and (3) promote transparency and accountability. Nearly 50% of the recommendations aimed to promote economy, efficiency, and effectiveness of HHF and HAMP, while 40% of the recommendations sought to prevent and detect fraud, waste, and abuse.

Treasury fully implemented 98, or 34 percent, of SIGTARP's recommendations and partially implemented 105, or 37 percent. Treasury's implementation of these recommendations resulted in program changes that enabled more eligible struggling homeowners to receive much needed assistance, recoveries of wasted program funds, and greater protections from fraud, waste, and abuse. Almost 30 percent of SIGTARP's recommendations remain unimplemented, representing missed opportunities to further enhance the programs and lessons learned for future housing and federal programs.

SIGTARP's Select Investigative Results (April 1, 2022 to March 31, 2023)

Risk of Fraud, Waste, and Abuse by Financial Institutions in the HAMP Program

SIGTARP's top law enforcement priority is to investigate and bring to justice unlawful conduct by any of the banks and other financial institutions that received $22.3 billion in HAMP.[18] HAMP modifies mortgages (interest rates, terms, etc.) for homeowners at risk of foreclosure, to make mortgage payments more affordable and sustainable for homeowners. There are over 550,000 homeowners participating in all 50 states. SIGTARP has several open, confidential investigations.

Justice for Defendants Convicted of Scamming Homeowners Who Were Seeking Foreclosure Assistance Through HAMP

SIGTARP has caught 121 scammers who were convicted for defrauding nearly 31,000 homeowners nationwide seeking foreclosure relief through HAMP. The courts have sentenced 101 scammers to prison.

Georgia Woman Sentenced in Connection with Defrauding TARP Recipient Bank

On August 3, 2022, Ladonna Barton was sentenced to time served, three years of supervised release and ordered to pay restitution of $46,947 for her role in defrauding River City Bank (RCB) in Rome, Georgia, a TARP recipient bank. Barton received loan proceeds through materially false and fraudulent pretenses, representations and promises, as well as material omissions during her participation in the scheme. The U.S. Attorney's Office for the Northern District of Georgia prosecuted this matter.

CEO of Louisiana Federal Credit Union Sentenced for Filing a False Document in Connection with TARP

On April 6, 2022, Helen Godfrey-Smith, former Chief Executive Officer of the Shreveport Federal Credit Union, was sentenced to one year of probation and ordered to pay a fine of $5,000 for making and using a false document in connection with the TARP funds the Shreveport Federal Credit Union received from the Treasury. She pled guilty to this crime in December 2021. In December 2016, Godfrey-Smith signed a document stating the credit union was financially healthy, when in fact the credit union was in dire fiscal condition. Due to its dismal financial condition, the credit union was placed into a conservatorship in April 2017 and was liquidated in October 2017. The U.S. Attorney's Office for the Western District of Louisiana was responsible for the prosecution of this case.

[18] SIGTARPs March 31, 2023 analysis of Treasury's most recent MHA data; Treasury, Housing Transaction Report, March 2023

Former CEO of TARP Bank Sentenced for Participating in a Bribery Scheme in Connection with Loans Guaranteed by the Small Business Administration

On October 6, 2022, Edward Shin was sentenced to fourteen months imprisonment, three years of supervised release, and ordered to forfeit $5,506,050 for his role in a bribery scheme as the former CEO of Noah Bank. Shin caused the Bank to issue millions of dollars of SBA-guaranteed and commercial loans to companies in which he held a secret financial interest.

These charges were brought about by a joint investigation with SIGTARP, FDIC-OIG, HSI, and SBA-OIG. This case was prosecuted by the United States Attorney's Office for the Southern District of New York.

Kansas Business Owner Sentenced for Defrauding a TARP Recipient Bank

K. Kevin James owned and operated several construction companies in Kansas. These companies secured a line of credit with Blue Valley Bank, a TARP recipient bank. Beginning in 2009 through 2011, K. Kevin James participated in a scheme to provide falsified financial statements for the construction companies to Blue Valley Bank misrepresenting the true financial condition of the construction companies. In May 2011, the James' construction companies filed for bankruptcy, resulting in a loss of over $3 million to Blue Valley Bank. On November 14, 2022, K. Kevin James was sentenced to 12 months imprisonment and two years of supervised release, and ordered to make $6,159,892 in restitution. The case was prosecuted by the U.S. Attorney's Office for the District of Kansas.

Illinois Real Estate Developer Sentenced for Scheme to Defraud TARP Bank

On December 28, 2022, See Wong, the owner of a real estate development company in Illinois was sentenced to sixteen months in prison and two years of supervised release for wire fraud for defrauding a bank while it was in TARP. He was also ordered to pay $1,659,457 in restitution. To receive construction loans to build condominiums in Chicago, the banking contracts required the defendant to put buyer deposits into an escrow account at the bank. Instead, he diverted deposits to fund his portion of construction costs and a personal loan to a friend. Victim purchasers lost approximately $1 million, and the bank lost approximately $1.8 million. SIGTARP was joined in the investigation by the FBI. The U.S. Attorney's Office for the Northern District of Illinois prosecuted the case.

Two Defendants Convicted in Operation Phantom Bank

SIGTARP's investigation of TARP recipient Saigon National Bank resulted in the guilty pleas of two additional defendants. On December 2, 2022, Jack Nguyen, pled guilty to money laundering charges and is scheduled to be sentenced on April 24, 2023. On January 20, 2023, co-defendant Lien Tran also pled guilty to money laundering charges and is scheduled for sentencing in July 2023.

"Operation Phantom Bank" was a long-term money laundering investigation conducted by SIGTARP and its law enforcement partners, the FBI and Internal Revenue Service-Criminal Investigation. This case resulted in six indictments that charged a total of 25 defendants. Convictions to date include a former shareholder of Saigon Bank, an East West Bank Vice President, a high-level Mexican money launderer, the former president of the Chinese Consolidated Benevolent Association, and several domestic money launderers with ties to Armenian Power and Chinese Triads organized crime groups. One additional defendant is pending trial on money laundering charges and two additional defendants are currently fugitives, one located in Hong Kong and the other in Lichtenstein. This case is being prosecuted by the U.S. Attorney's Office in the Central District of California.

New Jersey Defendant Sentenced for Role in Scheme to Defraud Bank and Bank Regulators

On January 31, 2023, Gary Ketchum, who conspired with the former CEO of First State Bank to defraud the bank and its regulator, the FDIC, was sentenced to three years of probation and ordered to forfeit $175,000. Ketchum participated in a scheme in which material misrepresentations were made to obtain millions of dollars in loans from First State Bank, which were fraudulently made into a capital infusion by other co-conspirators to deceive the FDIC on the financial strength of the bank. First State Bank previously applied for TARP funding to bolster their financial position, but later withdrew their application. This case was prosecuted by the U.S. Attorney's Office in New Jersey.

Co-Conspirator Sentenced for Participating in a Bribery Scheme with Former Bank CEO In Connection with Loans Guaranteed by the Small Business Administration

On February 2, 2023, James Kim was sentenced to one year of supervised release and ordered to forfeit $3,670,000 for his role in a bribery scheme with the former CEO of Noah Bank in connection with hundreds of thousands of dollars in loans guaranteed by the Small Business Administration (SBA), and with causing the Bank to issue millions of dollars of SBA-guaranteed and commercial loans to companies in which the former CEO had a secret financial interest.

These charges were brought about by a joint investigation with SIGTARP, the Federal Deposit Insurance Corporation – Office of Inspector General (FDIC-OIG), Homeland Security Investigations (HSI), and the SBA Office of Inspector General (SBA-OIG). This case was prosecuted by the United States Attorney's Office for the Southern District of New York.

Office of Inspector General Department of the Treasury

The Department of the Treasury (Treasury) Office of Inspector General (OIG) performs independent, objective reviews of specific Treasury programs and operations with oversight responsibility for one federal banking agency – the Office of the Comptroller of the Currency (OCC). That federal banking agency supervises approximately 1,100 financial institutions.

Introduction

Treasury OIG was established pursuant to the 1988 amendments to the Inspector General Act of 1978. The Treasury Inspector General is appointed by the President, with the advice and consent of the Senate. Treasury OIG performs independent, objective reviews of Treasury programs and operations, except for those of the Internal Revenue Service (IRS), the Troubled Asset Relief Program (TARP), and those programs and activities under the jurisdictional oversight of the Special Inspector General for Pandemic Recovery (SIGPR). Treasury OIG also keeps the Secretary of the Treasury and Congress fully informed of problems, deficiencies, and the need for corrective action. Treasury OIG is comprised of four components: (1) Office of Audit, (2) Office of Investigations, (3) Office of Counsel, and (4) Office of Management. Treasury OIG is headquartered in Washington, DC.

Treasury OIG has oversight responsibility for OCC, which supervises approximately 778 national banks, 257 federal savings associations, and 49 federal branches and agencies of foreign banks. The total assets under OCC's supervision are $15.9 trillion. Treasury OIG also oversees four offices created by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) which are (1) the Office of Financial Research, (2) the Federal Insurance Office, (3) the Office of Minority and Women Inclusion within Treasury's Departmental Offices, and (4) the Office of Minority and Women Inclusion within OCC.

Treasury OIG is also responsible for audit and investigative oversight of Treasury programs providing financial assistance to address the economic impacts of Coronavirus Disease 2019 (COVID-19). Since March 2020, more than $645 billion of financial assistance, overseen by Treasury OIG, has been authorized by the *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act)[19] enacted on March 27, 2020; the *Consolidated Appropriations Act, 2021*[20] enacted on December 27, 2020, and the *American Rescue Plan Act*[21] enacted on March 11, 2021. Through these pieces of legislation, Treasury provides financial assistance to the transportation industry for the continuation of salaries and benefits; to all 50 States, units of local government, U.S. territories, and tribal governments to provide economic relief including rental and mortgage assistance and support for small businesses; and to community development financial institutions to inject emergency capital investment into low-income communities to address the ongoing pandemic. Treasury established the Office of Recovery Programs to administer the pandemic relief funds. The enormity of these programs requires continued coordination between the Office of Audit, the Office of Investigations, and the Office of Counsel to handle complaints concerning thousands of recipients and sub-recipients that received financial relief.

Treasury Management and Performance Challenges Related to Financial Regulation and Economic Recovery

In accordance with the Reports Consolidation Act of 2000, the Treasury Inspector General annually provides the Secretary of the Treasury with his perspective on the most serious management and performance challenges facing the Department. In a memorandum to the Secretary dated October 14, 2022, the Deputy Inspector General reported four management and performance challenges that were directed towards financial regulation and economic recovery. Those challenges are discussed below and include: COVID-19 Pandemic Relief; Cyber Threats; Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement; and Climate Initiatives Risk.[22] The memorandum also reported a concern about regulating digital assets.

Challenge 1: COVID-19 Pandemic Relief

The COVID-19 pandemic continues to affect the health and economic stability of communities worldwide. In the early stages of the COVID-19 outbreak, Congress passed legislation in succession to address the public health crisis and the economic fallout affecting individuals, businesses, and many industry sectors. The *Coronavirus Preparedness and Response Supplemental Appropriation Act of 2020*, signed into law on March 6, 2020, authorized $8.3 billion in emergency funding to address health and medical care. [23] Shortly thereafter, the *Families First Coronavirus Response Act* was enacted on March 18, 2020, which provided

[19] Public Law 116-136 (March 27, 2020).
[20] Public Law 116-260 (December 27, 2020).
[21] Public Law 117-2 (March 11, 2021).
[22] The Treasury Inspector General's memorandum included one other challenge not directly related to financial regulation and economic recovery: Information Technology Acquisition and Project Management.
[23] Public Law 116-123 (March 6, 2020).

approximately $104 billion to address the financial stress of individuals and households.24 The *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act) passed on March 27, 2020, and provided over $2.4 trillion in health and economic relief to hospitals and healthcare providers, individuals and households, businesses and employees, as well as, states, local and tribal governments, and federal agencies, among others. As the public health crisis continued into late 2020 and 2021, Congress legislated additional relief in passing the *Consolidated Appropriations Act, 2021* (CAA, 2021) on December 27, 2020, and the *American Rescue Plan Act of 2021* (ARP) on March 11, 2021. These laws provided another $900 billion and $1.9 trillion of economic stimulus, respectively.

Treasury has been instrumental to the implementation of economic relief provisions of the CARES Act, CAA, 2021, and ARP. As a result, Treasury's responsibilities and workloads expanded enormously. Treasury is tasked with disbursing over $655 billion[25] in aid to more than 35,000 recipients, including state, local, territorial, and tribal government entities, in a relatively short period of time and with limited staffing. The Department is challenged with (1) filling and transitioning key leadership positions for pandemic programs not fully established, (2) quickly establishing internal controls, guidance, and methodologies for monitoring, reporting, and oversight of funds disbursed, (3) data collection, quality, and reliability, and (4) lack of funding to sustain operations. In addition, Treasury must carry the administrative and monitoring responsibilities in its new role resolving Single Audit findings and potentially serving as cognizant agency for a significant number of entities [26] under the Office of Management and Budget's (OMB) *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*.[27]

Many of the pandemic recovery programs and provisions of the CARES Act, CAA, 2021, and ARP are within the oversight purview of Treasury OIG and include programs that support transportation industry workers; renters and homeowners; and state, local, territorial, and tribal government entities through direct financial assistance. The pandemic programs Treasury is responsible for, and their challenges are discussed below.

Financial Assistance Programs - Air Carrier Worker Support and Other Transportation Services

Payroll Support Programs

To maintain pay and benefits of airline industry workers, Treasury implemented the Air Carrier Worker Support Program provisions of the CARES Act that authorized up to $63 billion of direct financial assistance for passenger air carriers, cargo air carriers, and contractors. Using existing resources and contractor support, Treasury quickly stood up the Payroll Support

[24] Public Law 116-127 (March 18, 2020).
[25] Amount excludes Economic Impact Payments distributed by the Internal Revenue Service and support to small businesses under the Paycheck Protection Program administered by the Small Business Administration.
[26] Single Audit Act of 1984 (P.L 98-502; October 19, 1984), as amended by the Single Audit Act Amendments of 1996 (P.L 104-156; July 5, 1996).
[27] https://www.ecfr.gov/current/title-2/part-200

Program (PSP1). This financial support for air carrier workers was extended twice by CAA, 2021 and ARP which provided additional assistance to passenger air carriers and contractors for up to $16 billion and $15 billion, respectively. Using the mechanisms that established PSP1, Treasury implemented the Payroll Support Program Extension (PSP2) and the Payroll Support Program 3 (PSP3) to make corresponding payments.

Treasury OIG will continue to audit PSP1 recipients' certifications and plans to initiate audits of certifications submitted by PSP2 recipients. Treasury OIG is not mandated to audit the applicants' certifications to receive PSP3 payments authorized under ARP. However, Treasury disbursed financial assistance to passenger air carriers and contractors based on information submitted by recipients on their PSP2 certifications, which we will audit. That said, Treasury OIG plans to assess Treasury's calculation of award amounts under PSP3 and Treasury's post-award monitoring of recipients under PSP1, PSP2, and PSP3. It is incumbent upon Treasury to implement and maintain strong internal controls over recipients' compliance with signed terms and conditions for receiving financial assistance. That is, Treasury's compliance monitoring function is essential to ensuring that recipients use funds for the continuation of salaries and benefits as intended.

Coronavirus Economic Relief for Transportation Services

Congress expanded financial support to non-air carrier transportation service providers under the Coronavirus Economic Relief for Transportation Services (CERTS) provisions of CAA, 2021. Treasury established the CERTS Program that provides $2 billion in non-competitive grants to eligible companies that certify revenue loss of 25 percent or more due to the COVID-19 pandemic. In consultation with the Department of Transportation, Treasury provided initial guidelines on May 6, 2021, that included among other things that the priority use of funds must be for payroll, although operating expenses and debt accrued to maintain payroll are eligible uses. It is incumbent upon Treasury to establish and maintain strong internal controls over recipients' compliance with grant agreements. Although there is no mandate directing Treasury OIG to audit CERT recipients, we plan to audit Treasury's administration of the program.

Financial Assistance Programs - State, Local, U.S. Territorial, and Tribal Governments

Coronavirus Relief Fund

The $150 billion Coronavirus Relief Fund (CRF), established under Title VI of the Social Security Act, as amended by Title V of the CARES Act, continues to be a large endeavor for both Treasury and our office. Treasury disbursed the entire $150 billion in direct payments to states, units of local government, the District of Columbia, U.S. territories, and tribal governments. Disbursement of funds was a complicated undertaking given the number of recipients at varying levels of government and other payment requirements of the CARES Act. The CARES Act created a unique challenge in distinguishing between the programmatic administrative responsibility for payments made from the CRF and the Treasury OIG's

independent oversight. Although Treasury is authorized to make payments, the CARES Act assigned Treasury OIG with responsibility for monitoring and oversight of the receipt, disbursement, and use of funds. Additionally, Treasury OIG has authority to recoup funds if it is determined that recipients fail to comply with uses of funds for COVID-19 related costs under Section 601 (d), "Uses of Funds," of the Social Security Act, as amended.[28]

Treasury also has a fundamental role to clarify its policy[29] over the uses of funds when interpretation matters arise. As recipients are still in the process of reporting on and closing out their awards, we anticipate that questions will continue to arise that will require interpretation. Providing as much clarity as possible is essential for ensuring recipients understand the compliance requirements and are accountable and transparent in how they report uses of funds. Treasury OIG has received over 500 complaints regarding recipient, and in some instances sub-recipient, uses of CRF proceeds that require continued collaboration between the Department and our office.

Coronavirus State and Local Fiscal Recovery Funds

The Coronavirus State and Local Fiscal Recovery Funds provisions of ARP provide state, local, U.S. territorial, and tribal governments another $350 billion under the Coronavirus State Fiscal Recovery Fund and the Coronavirus Local Fiscal Recovery Fund (together referred to as SLFRF); $10 billion under the Coronavirus Capital Projects Fund (CPF); and $2 billion under the Local Assistance and Tribal Consistency Fund (LATCF).

SLFRF

Administering SLFRF poses challenges given the volume of recipients that Treasury must oversee that include all 50 states, U.S. territories, tribal governments, and local government recipients with population sizes of 250,000 or more, and approximately 26,000 Non-Entitlement Units (NEU). States and U.S. territories were required to establish a process for NEUs to provide pre-pandemic budget and other critical information and documentation before distributing funds. In addition to the volume of NEUs for Treasury to oversee, reconciliation between states' and U.S. territories' disbursements to NEUs and recipient performance reporting may be challenging. That is, performance reporting for NEU funding is the responsibility of the NEUs and not the states and U.S. territories where accountability for the disbursement of funds resides. Furthermore, due to increased pandemic funding many NEUs are now required to have a Single Audit or alternate compliance examination engagement over which Treasury may have agency cognizance as detailed below related to challenges with Treasury's ongoing compliance monitoring of SLFRF recipients and related administrative issues.

[28] Section 601 (d), Use of Funds, to cover only those costs of the state, tribal government, or unit of local government that (1) are necessary expenditures incurred due to the public health emergency with respect to COVID–19; (2) were not accounted for in the budget most recently approved as of the date of enactment of this section for the State or government; and (3) were incurred during the period that begins on March 1, 2020, and ends on December 31, 2021, as extended by the CAA, 2021.

[29] *Coronavirus Relief Fund Guidance for State, Territorial, Local, and Tribal Governments* Federal Register, Vol. 86, No. 10; January 15, 2021.

While Treasury has built a portal for recipient communication and reporting, there are still challenges obtaining sufficient quality data from SLFRF recipients. Treasury allows for lengthy narrative responses as part of the data collection that may be more cumbersome to review and lack critical data details. Confirming data quality and timely providing data to the public and oversight community has been challenging for Treasury. To effectively administer and monitor SLFRF recipients' compliance, Treasury must have access to sufficient data that accurately reflects how recipients have expended SLFRF awards. As Treasury continues to receive quarterly and annual reports on SLFRF recipients' uses of funds, it is critical that Treasury continues to refine mechanisms to ensure the data is complete, accurate, reliable, and transparent in reflecting how recipients have expended SLFRF awards.

Treasury management has expressed difficulty finding the staff needed to administer and monitor the SLFRF program. The Office of Recovery Programs had a number of key leadership positions that were either vacant or temporarily staffed throughout fiscal year 2022.

CPF

As of September 2022, Treasury awarded $1.4 billion to 13 states[30] from the $10 billion of CPF available to address infrastructure challenges, such as reliable internet, that low to moderate income and rural communities have experienced during the COVID-19 pandemic. Although Treasury issued recipient reporting guidance for states, U.S. territories, and Freely Associated States in August 2022, Treasury still needs to inform eligible tribal government recipients of their reporting obligations to provide full accountability and transparency as to how CPF awards are used. To do this, Treasury needs to begin collecting sufficient and accurate CPF data.

LATCF

Treasury has been delayed in standing up the LATCF program, which was appropriated $2 billion for fiscal years 2022 and 2023 to make COVID-19 assistance payments to eligible revenue sharing counties and Tribes. Treasury issued LATCF guidance, including general reporting requirements to eligible recipients, and as of September 30, 2022, both tribal governments and revenue counties are able to apply for funds. Now, Treasury will need to prepare for the collection of sufficient and accurate LATCF data for monitoring recipients' compliance with the program.

With the overlap of recipients of CRF, SLFRF, CPF, and LATCF, Treasury OIG expects that there will be confusion between the uses of funds requirements, and reporting mechanisms that may be a challenge for recipients going forward. Given the volume of recipients and varying requirements under these programs, Treasury will need to ensure that there are sufficient resources for the remaining distribution of funds and ongoing monitoring of recipient reporting and compliance with terms and conditions for funds received.

[30] Treasury announced awards for Louisiana, New Hampshire, Virginia, West Virginia, Kansas, Maine, Maryland, Minnesota, Arkansas, Connecticut, Indiana, Nebraska, and North Dakota.

Furthermore, with the level of funding under both CRF and SLFRF, Treasury may have agency cognizance over many smaller local governments (particularly NEUs) and tribal governments now required to have a Single Audit for the first time. To minimize recipient burden, Treasury developed alternate reporting requirements for smaller SLFRF recipients, which would otherwise be subject to Single Audit. In the Compliance Supplement for 2022, Treasury provides the option of an alternate compliance examination engagement for SLFRF recipients meeting certain eligibility requirements. Treasury has been working with OMB and the audit community to find a solution for receiving these reports as the Federal Audit Clearinghouse (FAC) was not designed to collect non-audit products. Treasury plans to collect these reports directly for fiscal year 2021 compliance examinations and is continuing to work with the FAC to receive these reports for fiscal year 2022. While the alternative compliance examination engagement addresses the burden to these smaller government entities and auditors, Single Audit and alternative compliance examination procedures may be new to thousands of SLFRF recipients, so there will be much more guidance and oversight required of Treasury in its cognizance role and related to the Compliance Supplement. Treasury must be prepared to use results of Single Audits and alternate compliance examinations as part of its compliance monitoring of recipients and will need the appropriate level of staffing to address these issues on such a large scale. As discussed in more detail under the accountability and transparency section below, Treasury is evaluating whether it will have cognizance over thousands of non-federal recipients of SLFRF and any impacts it faces to carry out its ongoing administration and monitoring of SLFRF recipients.

Emergency Rental Assistance and Homeowner Assistance Programs

To provide assistance to vulnerable households at risk of housing instability, Congress established two Emergency Rental Assistance (ERA) Programs and a Homeowner's Assistance Fund (HAF) availing over $56 billion to households in need. Division N, Title V, Subtitle A, of CAA, 2021, created the initial ERA Program (ERA1) and ARP created a supplemental ERA Program (ERA2) and HAF.

ERA1

Treasury established ERA1 and has disbursed most of the $25 billion appropriated by CAA, 2021. The monies have been disbursed to states (including Washington, DC), U.S. territories, tribal governments (with a provision for the Department of Hawaiian Home Lands), and units of local government with populations of 200,000 or greater to pay for rent, utilities, and other housing-related expenses and arrears. In addition to disbursing the funds, Treasury provided guidance on ERA1 fund usage and set up a Portal where government recipients are to report on their spending.

CAA, 2021 requires that Treasury OIG conduct monitoring and oversight of the receipt, disbursement, and use of ERA1 funds. Treasury OIG will conduct oversight with audits of Treasury's (1) establishment and implementation of the program, (2) payments of funds, and (3) guidance and management over the program and will use the data reported in Treasury's ERA Portal to inform our monitoring function; thus, it is imperative that Treasury ensures recipients' compliance to Treasury ERA guidance when reporting to Treasury's ERA Portal. Treasury OIG is also authorized to require repayment of funds to Treasury when we determine a recipient failed to comply with ERA1 requirements.

ERA2

For ERA2, Treasury has disbursed most of the $21.55 billion appropriated in ARP. Similar to ERA1, ERA2 provides funding for eligible renter households' rent, utilities, and other housing-related expenses and arrears, but does not include tribal governments as eligible grantees. ERA2 funds are to remain available until September 30, 2027. Treasury has also provided ERA2 guidance for the state, territory, and local, government recipients. Treasury OIG is tasked with oversight of the program and will conduct ERA2 oversight with a similar methodology to ERA1 oversight.

HAF

ARP also created HAF to prevent mortgage delinquencies, defaults, foreclosures, loss of utility services, and displacement by covering mortgage-related expenses, utility expenses, and arrears for homeowners experiencing financial hardship after January 21, 2020. Treasury has disbursed most of the $9.9 billion authorized to states (including the District of Columbia and Puerto Rico), tribal governments (including the Department of Hawaiian Home Lands), Guam, American Samoa, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands. The funds are available until September 30, 2025, and Treasury provided guidance on HAF. ARP mandates that Treasury OIG provide oversight of the funds, which will include audits of Treasury's (1) establishment and implementation of the fund, (2) payments of funds, and (3) guidance and management over the program.

While Treasury has issued relevant guidance for each of the programs, it is essential its program offices continue to be responsive to recipients to clarify guidance and to provide insight into the eligible uses of the funds Treasury distributed. Clear and timely guidance and responsiveness to recipient questions are also critical in enabling program recipients to administer their programs and disburse funds to households in need without delay.

State Small Business Credit Initiative

The State Small Business Credit Initiative (SSBCI), which was originally created in the Small Business Jobs Act of 2010 to increase availability of credit for small businesses, ended in 2017. However, Section 3301 of ARP reauthorized SSBCI and provided $10 billion in funding for the program. Under SSBCI, participating states, U.S. territories, and tribal governments may obtain funding for programs that partner with private lenders to extend credit to small businesses.

Additionally, ARP modified SSBCI in a number of ways including the following set-asides: (1) $500 million in allocations to tribal governments in proportions determined appropriate by the Secretary of the Treasury; (2) $1.5 billion in allocation to states, U.S. territories, and tribal governments for business enterprises owned and controlled by socially and economically-disadvantaged individuals (SEDI); (3) $1 billion to be allocated as an incentive for states, U.S. territories, and tribal governments that demonstrate robust support for SEDI businesses; (4) $500 million to be allocated to very small businesses with fewer than 10 employees; and (5) $500 million to provide technical assistance to certain businesses applying for SSBCI or other state or federal programs that support small businesses.

Primary oversight of the use of SSBCI funds is the responsibility of the participating state, U.S. territory or tribal government. The participants are responsible for providing Treasury with quarterly assurances that their programs approved for SSBCI funding comply with program requirements. However, Treasury faces challenges in holding participants accountable for the proper use of funds, as it has not clearly defined the oversight obligations of the states, U.S. territories, and tribal governments or specified minimum standards for determining whether participants have fulfilled their oversight responsibilities. In the past, Treasury has also not required participating states to collect and review compliance assurances made by lenders and borrowers or defined what constitutes a material adverse change in a state's financial or operational condition that must be reported to Treasury. As a result, Treasury may have difficulty finding recipients to be in default of program requirements and holding recipients accountable.

Community Development Investment Programs[31]

Emergency Capital Investment Program

As authorized under CAA, 2021, Treasury has invested most of the $9 million available under the Emergency Capital Investment Program (ECIP) in Community Development Financial Institutions (CDFI) and Minority Deposit Institutions, providing capital to low-to-moderate income community financial institutions that support small businesses and consumers. Treasury has experienced challenges in fully implementing ECIP. As reported in our audit of ECIP's implementation, Treasury had not completed key documentation, such as policies and procedures to include a post-investment compliance and monitoring plan to fully implement and administer investments.[32] With investments now underway, it is more imperative that Treasury develop and implement policies and procedures to govern its post–investment activities. Because of the demands for resources within the Office of Recovery Programs, Treasury may continue to experience further delays and challenges administering the ECIP.

CDFI Rapid Response Program

Treasury has disbursed nearly half of the $3 billion, authorized under the CAA, 2021, under the CDFI Fund Rapid Response Program (CDFI RRP), to deliver immediate assistance to low-income communities

[31] Treasury OIG is required to submit to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate, and the Secretary of the Treasury, not less frequently than 2 times per year, a report relating to the oversight provided including any recommendations for improvements to the Community Development Investment programs.

[32] OIG, *Audit of Treasury's Implementation of the Emergency Capital Investment Program* (OIG-22-028; March 8, 2022)

through competitive grants to CDFIs. However, as reported in our audit of the CDFI RRP implementation,[33] the CDFI Fund did not include the award term and condition for integrity and performance matters in its assistance agreement template. Treasury OIG will confirm that CDFI Fund included the required language in the executed assistance agreements with CDFI RRP grant recipients as part of our ongoing mandated audits of the CDFI RRP.

CDFI Equitable Recovery Program

Awards granted under CDFI Fund Equitable Recovery Program (CDFI ERP) are intended for low- or moderate-income minority communities that have significant unmet capital or financial service needs, and were disproportionately impacted by the COVID-19 pandemic. This program is challenging for the CDFI Fund to administer because of unique and complex program materials for the application process and award administration needed to address program policy priorities in order to meet the statutory intent. In addition, CDFI Fund plans to implement designation of minority lending institutions as defined under the CAA, 2021 separately from the award of ERP funds.

Accountability and Transparency

In the context of this overarching challenge, Treasury OIG recognizes the breadth and scope of Treasury's responsibilities as it impacts programs, operations, and activities regardless of jurisdictional oversight boundaries. Along with administering and delivering economic relief, Treasury must manage the unprecedented oversight that pandemic relief funding is subject to. As noted above, Treasury is evaluating whether it will have cognizance over thousands of non-federal recipients of SLFRF and be required to carry out a larger administrative and monitoring role to ensure compliance under OMB's Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards. Among its responsibilities as a Federal awarding agency, Treasury must follow-up on audit findings to ensure that recipients take appropriate and timely corrective action and issue management decision letters.[34] Many recipients are smaller governments, which for the first time are subject to Single Audit or the alternative compliance examination available to eligible recipients meeting eligibility requirements. Regardless of cognizance, Treasury will have to work with recipients to resolve Single Audit and alternative compliance examination findings specific to each of its pandemic relief programs.

In addition to Treasury OIG's ongoing work on pandemic programs, Treasury is subject to additional Congressional oversight bodies, the Special Inspector General for Pandemic Recovery[35] (SIGPR), the Government Accountability Office (GAO), and the Pandemic Response Accountability Committee

[33] OIG, *Audit of the Community Development Financial Institutions Fund's Implementation of the CDFI Rapid Response Program* (OIG-22-023; December 21, 2021).

[34] 2 CFR § 200.521, "The management decision must clearly state whether or not the audit finding is sustained, the reasons for the decision, and the expected auditee action to repay disallowed costs, make financial adjustments, or take other action. If the auditee has not completed corrective action, a timetable for follow-up should be given..." (https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/subpart-F/subject-group-ECFR4424206eaecf751/section-200.521)

[35] SIGPR was authorized under the CARES Act to oversee loans, loan guarantees, and other investments provided by Treasury and must report to congress quarterly on the SIGPR's activities and Treasury's loan programs. SIGPR terminates five years after enactment of the CARES Act (March 27, 2025).

(PRAC). Treasury is also accountable for providing transparency over the expenditure of pandemic relief funds. Many reporting requirements of sections 15010 and 15011 of the CARES Act were extended under the CAA, 2021, PRAC amendments. Most notably, Treasury is responsible for reporting obligations and expenditures of large covered funds (over $150,000) to the PRAC. While Treasury OIG continues to collect and report CRF data to the PRAC under an agreement with the Department, Treasury is responsible for reporting expenditures of its other pandemic relief programs. As noted above, data collection and quality are still challenges for Treasury under the various pandemic programs. The Department must balance its ongoing response to the financial impacts of the public health emergency with its responsibility to stakeholders for reporting and transparency.

Challenge 2: Cyber Threats

Cybersecurity remains a long-standing and serious challenge facing the Nation as reported by GAO as a government-wide issue in its 2021 high-risk list published biennially.[36] A reliable critical infrastructure, including information systems and networks, is vital to our national security and economic stability. Cyber threats remain a persistent concern as Treasury's information systems are critical to the core functions of government and the Nation's financial infrastructure, along with the financial sector it oversees. As cyber threats continue to evolve and become more sophisticated, subtle, and easier to perform, Treasury must fortify and safeguard its internal systems and operations while modernizing and maintaining them. Although managing known risks is an ongoing challenge, Treasury must also be ready to reinforce and/or redirect cybersecurity efforts when unforeseen events occur, such as the COVID-19 pandemic, the recent conflict in the Ukraine,[37] the 2020 SolarWinds attack,[38] or when serious flaws are discovered in software or systems that allow for remote administrative-level access.[39]

Threat actors frequently exploit vulnerable networks or systems in a string of trusted connections to gain access to government systems. Organized hacking groups leverage published and unpublished vulnerabilities and vary their methods to make attacks hard to detect and even harder to prevent. Criminal groups and nation-states are constantly seeking to steal information; commit fraud; disrupt, degrade, or deny access to information systems; or infiltrate information systems and maintain a presence to enable future actions. Through information sharing, federal agencies are better prepared to thwart potential attacks to the cyber infrastructure of the Federal government and the financial sector.

[36] GAO, *High-Risk Series, Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas* (GAO-21-119SP: March 2021).

[37] A joint Cybersecurity Advisory was issued by the Cybersecurity and Infrastructure Security Agency to "warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners." (*Alert (AA22-110A) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*; April 20, 2022)

[38] The SolarWinds attack, reported in December 2020, was a supply chain attack that used the update mechanism for legitimate software to distribute malicious software.

[39] Cybersecurity and Infrastructure Security Agency, *Emergency Directive 22-02 Mitigate Apache Log4J Vulnerability* (April 8, 2022), *Emergency Directive 22-03 Mitigate VMWare Vulnerabilities* (May 18, 2022).

The tools used to perpetrate cyber-attacks continue to become easier to use and more widespread, lowering the technological knowledge and resources needed to launch successful attacks of increasing sophistication. Such attacks include distributed denial of service, phishing, fraudulent wire payments, business email compromise, malicious spam (malspam), ransomware, and compromise of supply chains (both hardware and software). While the federal workforce shifts from a primarily telework status to a hybrid work environment, Treasury must remain cognizant of the increased risk profile of a remote workforce, which provides threat actors with a broader attack surface. Increased network traffic from remote sources provides cover for attackers to blend in with the federal workforce and launch cyber assaults. These opportunities may allow threat actors to launch a denial of service attack upon a network that can prevent remote workers from performing their duties and disrupt operations.

There is continuing concern over foreign adversaries creating and exploiting vulnerabilities in the Nation's supply chain for information and communication technology and services as evidenced by the 2020 SolarWinds attack that affected many federal agencies and private sector companies. Executive Order (EO) 13873, *Securing the Information and Communications Technology and Services Supply Chain*, was issued on May 15, 2019, to secure the supply technology and services chain by banning the import, use, or sale of technology or services designed, developed, manufactured, or supplied from persons or companies that are owned or controlled by governments defined as hostile to the United States.[40] On May 12, 2022, this EO was extended again for 1 year.[41] There are risks that Treasury's systems and resources already in use, including critical infrastructure, contain components from sources that have yet to be designated as threats. Once a source is designated as such, repairs and/or upgrades of key system components may no longer be available. Therefore, there is risk of disruption of critical operations. Treasury will need to continue to monitor developments in this area closely and plan for the possibility that its current supply chain may no longer be available.

Treasury is looked upon to provide effective leadership to financial institutions in particular, and the financial sector in general, to strengthen awareness and preparedness against cyber threats to the Nation's critical infrastructure. As such, effective public-private coordination is essential to the Nation's financial and national security. In this regard, the Office of Cybersecurity and Critical Infrastructure Protection coordinates Treasury's efforts to enhance the security and resilience of the financial services sector critical infrastructure and reduce operational risk including risks associated with cybersecurity. Given the stress that the global COVID-19 pandemic and the conflict in Ukraine place on financial institutions and the financial sector, it is important that Treasury monitors cyber risks in these areas. That said, Treasury and other federal agencies have yet to fully implement the National Institute of Standards and Technology (NIST) guidance to assist federal agencies in managing cybersecurity risks.[42] In 2018, GAO had reported that the extent of adoption of the NIST framework by critical infrastructure sectors was unknown since

[40] EO 13873, *Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019).
[41] *Notice on the Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain* (May 12, 2022).
[42] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, February 12, 2014; superseded by Version 1.1; April 16, 2018).

agencies were not measuring framework implementation.[43] With respect to Treasury, GAO had recommended that steps be taken to consult with respective sector partners to develop methods for determining the level and type of adoption by entities across the financial services sector. In its May 10, 2022, letter[44] regarding its top open recommendations, GAO acknowledged that Treasury had developed a cybersecurity profile for the sector that maps the NIST Cybersecurity Framework's (CSF) five core functions[45] to existing regulations and guidance for financial services entities but had not developed methods to determine the level and type of framework adoption; the recommendation remained open.

The Department continues to report progress in managing risk as Treasury obtained an overall rating of "Managing Risk" across all NIST CSF categories (Identify, Protect, Detect, Respond and Recover) on the OMB Cybersecurity Risk Management Assessment for the first time in fiscal year 2021. Treasury also reported the creation of enhanced risk profiles to allow senior leadership greater visibility into the risks for all Departmental High Value Assets.[46] While addressing increases in cyber threats, Treasury will need to continue to balance cybersecurity demands while maintaining and modernizing Information Technology (IT) systems.

Challenge 3: Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement

Over the past year, the Office of Terrorism and Financial Intelligence (TFI) has remained dedicated to countering the ability of financial networks that support terrorists, organized transnational crime, weapons of mass destruction proliferators, and other threats to international security through intelligence analysis, sanctions, and international private-sector cooperation. As previously reported, identifying, disrupting, and dismantling these networks continue to be challenging as TFI's economic authorities are key tools to carry out U.S. policy. Additionally, criminals and other bad actors evolve and continue to develop more sophisticated money laundering methods in an attempt to avoid detection.

TFI's authorities are key tools in implementing U.S. policy to pressure foreign countries and regimes, such as Russia, by using designations and economic sanctions. TFI has significantly increased sanctions against Russia related to its actions against Ukraine and other malign activities. TFI's counter-terrorism designations disrupt the financial networks that support terrorist organizations. Disrupting terrorist financing depends on a whole-of-government approach and requires collaboration and coordination within Treasury and with other federal agencies. Collaboration and coordination are key to successfully identifying and disrupting all of these financial networks and meeting TFI's mission. This effort requires effective and efficient working relationships among components within TFI and the Intelligence Community. In an effort to effectively implement U.S. policy and disrupt these financial networks, officials stated that TFI is moving towards a more collaborative approach to achieve its mission. Given the criticality of Treasury's mission and its role to carry out U.S. policy, we continue to consider anti-money

[43] GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption* (GAO-18-211; February 18, 2018)
[44] GAO, *Priority Open Recommendations: Department of the Treasury* (GAO-22-105633; May 10, 2022)
[45] The NIST Cybersecurity Framework functions include: Identify, Protect, Detect, Respond and Recover.
[46] High Value Assets are assets, information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the U S.' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety.

laundering and combating terrorist financing programs and operations as inherently high-risk.

Data privacy and information sharing are challenges for the Financial Crimes Enforcement Network (FinCEN), which has experienced unauthorized disclosures of Bank Secrecy Act (BSA) information. FinCEN is required to maintain a highly secure database for financial institutions to report BSA information. FinCEN has previously identified that the success of that system depends on the financial sector's confidence that those reports are adequately protected, but data breaches threaten to undermine that confidence. The challenge for FinCEN is to ensure the BSA information remains secure in order to maintain the confidence of the financial sector, while meeting the access needs of law enforcement, regulatory, and intelligence partners. FinCEN also faces an additional challenge, to develop and implement a new secure database for small businesses to report their beneficial ownership information, as required by the Corporate Transparency Act.[47] However, FinCEN does not expect to implement the database until January 2024.

Challenge 4: Climate Initiatives Risk

In January 2021, EO 14008, *Tackling the Climate Crisis at Home and Abroad*, identified the immediate need for comprehensive action to address the catastrophic impacts of climate change. EO 14008 emphasizes that U.S. leadership, and that of federal departments and agencies, will be required to significantly enhance global action and achieve the necessary policy outcomes on climate change. Furthermore, in May 2021, the White House introduced EO 14030, *Climate-Related Financial Risk*, which aims to: (a) advance consistent, clear, intelligible, comparable, and accurate disclosure of climate-related financial risk, including both physical and transition risks; (b) mitigate that risk and its drivers, while accounting for and addressing disparate impacts on disadvantaged communities and communities of color and spurring the creation of well-paying jobs; and (c) achieve the Administration's target of a net-zero emissions economy by no later than 2050.

The Secretary of the Treasury, as the Chair of the Financial Stability Oversight Council (FSOC), will lead several efforts related to EO 14030. Taken together, these two EOs place an emphasis on ensuring climate change is at the forefront of U.S. foreign policy and national security; establishing a government-wide approach to the climate crisis; and bolstering the resiliency of our communities, states, tribes, territories, and financial institutions to position the United States to lead the global economy to a more prosperous and sustainable future. Treasury will play a significant role working with other federal agencies, foreign governments, and international financial institutions to stimulate global action on addressing climate change, environmental justice, and climate change-created economic and financial crises. In 2021, Treasury created a new Climate Hub and appointed a Climate Counselor to coordinate and lead many of its efforts to address climate change. The Treasury Climate Hub will coordinate and enhance existing climate-related activities by utilizing the tools, capabilities, and expertise from across the Department – including officials from Domestic Finance, Economic Policy, International Affairs, and Tax Policy. With a view of all Treasury climate initiatives, the Hub will enable Treasury to prioritize climate action.

Treasury is also engaged in the Administration's domestic efforts through its role as a leading banking regulator, with the Office of the Comptroller of the Currency (OCC), and its responsibilities within

[47] Public Law 116-283 (January 1, 2021).

FSOC. Internationally, Treasury represents the United States at the G7 and G20, at the Financial Stability Board, and other institutions and forums such as the International Monetary Fund. In October 2021,

FSOC issued its *Report on Climate-Related Financial Risk*, as mandated by EO 14030. In it, FSOC details the activities of each member to date to address climate-related financial risk, including Treasury, the Office of Financial Research, the Federal Insurance Office, and OCC. The report highlights challenges in efforts to comprehensively understand and address climate-related financial risk. Those challenges include the types and quality of available data and measurement tools, the ability to assess climate-related financial risks and vulnerabilities, and how best to incorporate these risks into management practices and supervisory expectations as appropriate. FSOC concluded the report with thirty-five recommendations. Many, if not most, apply to Treasury, including the Office of Financial Research, the Federal Insurance Office, and OCC. It will be important that each recommendation be addressed not only timely, but collectively with the other FSOC members to ensure a cohesive response.

Furthermore, OCC has implemented multiple initiatives to address climate change and climate-related financial risk. They have partnered with other Federal banking regulators to work collaboratively in understanding the risks and development of climate-related risk management. OCC has also engaged with international groups to share best practices. Internally, OCC established a Climate Risk Implementation Committee chaired by a Climate Change Risk Officer to assess climate risks and advise management on OCC policy, banking supervision, and research. These collaborations will continue to be important in developing a common understanding of climate-related financial risks and their impact to ensure the continued safety and soundness of the banking system. OCC also continues to work with FSOC and other member agencies to understand the broader implications of climate-related financial risks and their potential impact on financial stability.

Other Matter of Concern

Although we are not reporting digital assets as a management and performance challenge, we are highlighting it as an area of concern.

Treasury supports responsible innovation and seeks to maximize the gains from this new technology while protecting against possible risks to consumers, financial stability, and illicit finance. In the absence of sufficient oversight and regulatory safeguards, the increase in use of digital assets could pose risks to consumers, investors, and the broader financial system.

In March 2022, the President convened experts from across the Administration to ensure a coordinated and comprehensive approach to digital assets policy and charged Treasury with a leadership role in this work. EO 14067, *Ensuring Responsible Development of Digital Assets*, establishes the following policy objectives with respect to digital assets: (1) protect consumers, investors, and businesses in the United States; (2) protect the United States and global financial stability and mitigate systemic risk; (3) mitigate the illicit finance and national security risks posed by misuse of digital assets; (4) reinforce United States leadership in the global financial system and in technological and economic competitiveness, including through the responsible development of payment innovations and digital assets; (5) promote access to safe and affordable financial services; and (6) support technological advances that promote responsible development and use of digital assets.

In September 2022, Treasury published a report on the future of the U.S. money and payments systems, in which Treasury encourages continued work on innovations to promote a system that is more competitive, efficient, and inclusive – and that also helps maintain and build on the United States' global financial leadership.[48] The report recommends advancing policy and technical work on a potential U.S. central bank digital currency (CBDC), so that the United States is prepared if a CBDC is determined to be in the national interest. Treasury also published a report on the implications of digital assets for consumers, investors and businesses, laid out a detailed Action Plan to prevent digital assets from being used for financial crimes, such as money laundering and terrorism financing, and sent a framework to the President for international engagement on digital asset issues. In October 2022, FSOC released a report on potential financial stability risks, and recommended steps to address gaps in the regulation of digital assets in the United States.[49] Following the publication of these reports, Treasury has a number of responsibilities, including participating in an interagency working group regarding a potential CBDC and working with other agencies to prepare resources for consumers. The Office of Domestic Finance, Office of Terrorism and Financial Intelligence, and Office of International Affairs will be primarily driving this work, in coordination with other parts of Treasury and the interagency working group, as appropriate.

In-Progress Work on Financial Oversight

OCC's Supervision of Federal Branches of Foreign Banks (In Progress)

We initiated an audit of OCC's supervision of federal branches of foreign banks. The objective of this audit is to assess OCC's supervision of federal branches and agencies of foreign banking organizations operating in the United States.

OCC's Controls over Purchase Cards (In Progress)

We initiated an audit of OCC's controls over purchase cards. The objective for this audit is to assess the controls in place over OCC's purchase card use and identify any potential illegal, improper, or erroneous transactions.

OCC's Crisis Readiness (In Progress)

We initiated an audit of OCC's crisis readiness. The objective for this audit is to assess OCC's readiness to address crises that could impact OCC's operations and the institutions it supervises.

[48] Treasury Report, *The Future of Money and Payments: Report Pursuant to Section 4(b) of Executive Order 14067* (September 2022).
[49] Financial Stability Oversight Council. *Report on Digital Asset Financial Stability Risks and Oversight* (October 2022).

Corrective Action Verification (CAV) Material Loss Review of Washington Federal Bank for Savings (In Progress)

We initiated an audit to assess whether OCC's management has taken corrective actions in response to the six recommendations made in the Department of the Treasury (Treasury) Office of Inspector General audit report, Material Loss Review of Washington Federal Bank for Savings (OIG-19-009, issued November 6, 2018).

Office of Financial Research Workforce Reshaping Efforts (In Progress)

We initiated an audit of Treasury's Office of Financial Research's implementation of its workforce reshaping efforts and its compliance with applicable laws, regulations, policies, and procedures.

CDFI Fund's Implementation of the CDFI Equitable Recovery Program (In Progress)

We initiated an audit to assess the implementation of the CDFI Fund's CDFI Equitable Recovery Program including making funds available, and establishing policies, procedures, as well as other program guidance and documentation.

CDFI Fund's Award and Post Aware Administration of the CDFI Rapid Response Program (In Progress)

We initiated an audit to assess the compliance of the CDFI Fund's award process for ensuring accuracy of rapid response program (RRP) payments, and the design and implementation of the post-award administration to include the CDFI RRP recipient monitoring process.

Failed Bank Reviews

In 1991, Congress enacted the Federal Deposit Insurance Corporation Improvement Act amending the Federal Deposit Insurance Act (FDIA). The amendments require that banking regulators take specified supervisory actions when they identify unsafe or unsound practices or conditions. Also added was a requirement that the Inspector General for the primary federal regulator of a failed financial institution conduct a material loss review when the estimated loss to the Deposit Insurance Fund is "material." FDIA, as amended by Dodd-Frank, defines the loss threshold amount to the Deposit Insurance Fund triggering a material loss review as a loss that exceeds $50 million for 2014 and thereafter (with a provision to temporarily raise the threshold to $75 million in certain circumstances). The act also requires a review of all bank failures with losses under these threshold amounts for the purposes of (1) ascertaining the grounds for appointing Federal Deposit Insurance Corporation (FDIC) as receiver and (2) determining

whether any unusual circumstances exist that might warrant a more in-depth review of the loss. As part of the material loss review, OIG auditors determine the causes of the failure and assess the supervision of the institution, including the implementation of the prompt corrective action provisions of the act.[50] As appropriate, OIG auditors also make recommendations for preventing any such loss in the future.

From 2007 through March 2023, FDIC and other banking regulators closed 548 banks and federal savings associations. One hundred and forty-four (144) of these were Treasury-regulated financial institutions; in total, the estimated loss to FDIC's Deposit Insurance Fund for these failures was $36.5 billion. Of the 144 failures, 58 resulted in a material loss to the Deposit Insurance Fund, and our office performed the required reviews of these failures. During the period covered by this annual report, we did not perform a material loss review or limited review of any bank failures.

OIG Investigative Accomplishments

The Office of Investigations, under the leadership of the Assistant Inspector General for Investigations, performs investigations and conducts initiatives to detect and prevent fraud, waste, and abuse in programs and operations within Treasury OIG's jurisdictional boundaries, and investigates threats against Treasury personnel and assets in designated circumstances as authorized by the Inspector General Act. The Office of Investigations also manages the Treasury OIG Hotline to facilitate reporting of allegations involving these programs and operations.

Significant Investigations

Subject Sentenced in Bank Fraud Investigation

On June 1, 2022, a subject was sentenced to 84 months' incarceration, 36 months' probation, and $8.4 million in restitution. The subject provided false documents to a financial institution and fraudulently obtained millions in loans under false pretenses. The United States Attorney's Office (USAO) for the Northern District of Oklahoma prosecuted our joint investigation with Internal Revenue Service - Criminal Investigation, Federal Bureau of Investigation (FBI), and Federal Deposit Insurance Corporation – Office of Investigations.

[50] Prompt corrective action is a framework of supervisory actions for insured institutions that are not adequately capitalized. It was intended to ensure that action is taken when an institution becomes financially troubled in order to prevent a failure or minimize the resulting losses. These actions become increasingly severe as the institution falls into lower capital categories. The capital categories are well-capitalized, adequately capitalized, undercapitalized, significantly undercapitalized, and critically undercapitalized.

Former Bank President Sentenced

On June 28, 2022, the OIG completed its report of investigation for a case that was initiated upon receipt of information from the FBI regarding a bank president who allegedly embezzled bank funds, and stole from customer accounts to include a non-profit, and elderly citizens' accounts. Our investigation determined the bank officer fraudulently paid for personal expenses with others' bank funds. The subject pled guilty to Theft by a Bank Officer and was sentenced to 24 months' probation, a $4,000 fine, and forfeiture of $16,000. The USAO for the Eastern District of Texas prosecuted the joint Treasury OIG and FBI case.

Investigation of Bank Fraud and Identity Theft in North Carolina

On October 11, 2022, the final subject in a joint OIG and Fayetteville, North Carolina (NC) Police Department investigation was sentenced. Eleven subjects conspired to defraud financial institutions by depositing forged, counterfeit, or stolen checks using stolen identities as part of an elaborate bank fraud scheme. The subjects were convicted and sentenced to a total of 552 months in prison, 852 months' of probation, and $600,000 in restitution. The case was prosecuted by the USAO for the Eastern District of NC.

The following update is related to significant investigative activities from prior annual reports**.**

Subject Sentenced for Access Device Fraud Using Stolen Credit Cards

As reported in previous annual reports, our investigation of an organized criminal group using stolen credit cards issued by Treasury-regulated financial institutions to purchase $400,000 in gift cards from stores, identified five subjects for prosecution. One subject pled guilty in U.S. District Court, District of Maryland, to Access Device Fraud for using stolen credit cards to purchase gift cards.

One subject, a former grocery store employee, was sentenced to 24 months of probation, a $100 special assessment, and ordered to pay $12,000 in restitution. To date, two additional subjects have been indicted.

Update: On November 1, 2022, the OIG completed its report of investigation for a case involving access device fraud in a joint Treasury OIG and U.S. Postal Inspection Service investigation. Of the five subjects identified for prosecution three were sentenced and two were declined for prosecution. The last two subjects were criminally charged and pled guilty to conspiring to use stolen credit cards in order to facilitate the purchase of approximately $400,000 in commercial gift cards. The final two subjects sentenced to a total of 22 months home detention, 72 months of probation, and $364,000 in restitution. The USAO for the District of Maryland, Greenbelt Division, prosecuted the case.

Appendix A:
CIGFO Guidance in Preparing for and Managing Crises

Council of Inspectors General on Financial Oversight

Guidance in Preparing for and Managing Crises

June 2022

CIGFO-2022-01

This page is intentionally blank

Table of Contents

This page is intentionally blank

June 2022

The Honorable Janet Yellen
Chair, Financial Stability Oversight Council
Washington, D.C. 20220

Dear Madam Chairwoman:

I am transmitting to you the Council of Inspectors General on Financial Oversight (CIGFO) report titled, *CIGFO Guidance in Preparing for and Managing Crises*

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) authorizes CIGFO to convene working groups of its members to address issues within its jurisdiction. Accordingly, CIGFO convened a Working Group in August 2020 to compile forward-looking guidance for the Financial Stability Oversight Council (FSOC) and its members to consider in preparing for and managing a crisis. This effort was undertaken at a critical time in our nation, precipitated by the COVID-19 pandemic.

This guidance is intended to be a compilation of lessons learned drawn from the experiences of federal agencies during prior crises and any learned during the current pandemic. This forward-looking guidance will facilitate effective crisis response as FSOC fulfills its mission to identify threats to the financial stability of the country, promote market discipline, and respond to emerging threats to the stability of the U.S. financial system.

This guidance does not assess the degree to which the FSOC member agencies employ any of the actions presented herein. Rather, the purpose of this guidance is to compile information and activities that agencies and CIGFO Offices of Inspector General identified as integral to pre-crisis planning and crisis management so that FSOC and its member agencies can evaluate its existing efforts and initiate new ones, as needed, consistent with each organization's mission. We are not making any recommendations to FSOC as a result of this effort.

I would like to take this opportunity to thank the FSOC members for their support, especially those Treasury officials who assisted with this effort.

CIGFO looks forward to working with you on this and other issues. In accordance with the Dodd-Frank Act, CIGFO is also providing this report to Congress.

Sincerely,

/s/

Richard K. Delmar
Acting Chair, CIGFO
Deputy Inspector General, Department of the Treasury

This page is intentionally blank

Guidance in Preparing for and Managing Crises

The Council of Inspectors General on Financial Oversight (CIGFO) provides oversight of the Financial Stability Oversight Council (FSOC). CIGFO members include nine Inspectors General (IG) with oversight authority for the federal member agencies of FSOC.[1] In August 2020, CIGFO convened a Working Group to develop guidance for FSOC and its member agencies to consider in preparing for and managing future crises.

CIGFO derived this guidance from the crisis response experiences of both the contributing CIGFO Office of Inspector General (OIG) Working Group members (CIGFO Working Group) and the federal agencies they oversee.[2] CIGFO OIGs identified practices and lessons learned by their respective agencies from prior crises and the current pandemic.[3] The CIGFO Working Group analyzed these submissions and summarized the practices and lessons learned from the financial regulators into this guidance. In addition, the Working Group reviewed previous reports issued by the International Monetary Fund (IMF) and the U.S. Government Accountability Office (GAO) regarding crisis preparedness actions and recommendations for FSOC. The Working Group also interviewed FSOC officials. This guidance does not assess the degree to which the FSOC member agencies employ any of the actions presented herein. Rather, the purpose of this guidance is to compile information and activities that agencies and OIGs identified as integral to pre-crisis planning and crisis management so that FSOC and its member agencies can evaluate their existing efforts and initiate new ones, as needed, consistent with each organization's mission.

In 2010, in the wake of the 2007-2009 Great Recession, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) was enacted to "promote the

1 The nine CIGFO members include the Inspectors General from the Board of Governors of the Federal Reserve System (FRB), Commodity Futures Trading Commission (CFTC), U.S. Department of Housing and Urban Development (HUD), Department of the Treasury (Treasury), Federal Deposit Insurance Corporation (FDIC), Federal Housing Finance Agency (FHFA), National Credit Union Administration (NCUA), Securities and Exchange Commission (SEC), and the Special Inspector General for the Troubled Asset Relief Program (SIGTARP).

2 The Working Group project was performed in accordance with CIGIE's Quality Standards for Federal Offices of Inspector General (Silver Book). These quality standards, as contained in the Agile Products Toolkit https://www.pandemicoversight.gov/media/file/agile-products-toolkit0pdf), include independence, analysis, evidence review, indexing and referencing, and supervision.

3 The CIGFO Working Group collected information from the OIGs for the FRB (including information relating to the Consumer Financial Protection Bureau (CFPB)), CFTC, Treasury, FDIC, FHFA, NCUA, SEC, and SIGTARP.

financial stability of the United States."[4] As a part of this effort, the Dodd-Frank Act created the FSOC, whose members include the federal financial regulatory agencies.[5] The Act conferred upon FSOC the authority to respond to emerging threats and to identify risks to the financial stability of the United States.[6] To meet these responsibilities, the Dodd-Frank Act assigned FSOC with, among other duties: (1) collecting information from member agencies; (2) facilitating information sharing and coordination among the member agencies; and (3) recommending to the member agencies general supervisory priorities and principles that reflect member agency discussions.[7]

During the past two years, FSOC has served as a forum for federal and state regulators to collect information, analyze risks, share information, and coordinate their responses to the economic shock caused by the Coronavirus Disease 2019 (COVID-19).[8] However, FSOC's coordination role is not limited to responding to emerging threats, such as COVID-19. FSOC is also authorized to identify risks to the United States' financial stability that could arise outside of the financial services marketplace, such as those that could arise from a future crisis. FSOC has an opportunity to serve in this coordination role by collecting and sharing information relating to crisis preparedness and then identifying the risks to the financial stability of the United States associated with the failure to prepare for future crises. Using this coordination role to focus on crisis preparedness and identifying risks associated with agencies' crisis preparedness is a role that FSOC has not undertaken -- notwithstanding multiple recommendations by different oversight authorities.

For example, both the IMF and GAO have recommended that FSOC enhance its crisis preparedness role. In 2015, the IMF recommended that FSOC assume a formal crisis preparedness and management role. This recommendation remains unimplemented, and the IMF reiterated this recommendation to FSOC in its August 2020 *United States Financial System Stability Assessment* [9] In addition, GAO recommended in a December 2020 report that FSOC conduct scenario-based exercises intended to evaluate capabilities for responding to crises.[10] FSOC neither agreed nor disagreed with the GAO recommendation. On January

4 Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010).

5 FSOC is composed of 15 members: 10 voting members and 5 nonvoting members. Voting members include the chair of FSOC (Treasury Secretary); heads of FDIC, FRB, OCC, NCUA, SEC, CFTC, FHFA, and CFPB; and an independent insurance expert appointed by the President. Nonvoting members include the directors of Treasury's Office of Financial Research (OFR) and Federal Insurance Office (FIO), and state regulatory representatives, one each for insurance, banking, and securities. 12 U.S.C. § 5321.

6 Section 112(a)(1) of the Dodd-Frank Act, 124 Stat. at 1394 (codified at 12 U.S.C. § 5322(a)(1)).

7 Section 112(a)(2) of the Dodd-Frank Act, 124 Stat. at 1395 (codified at 12 U.S.C. § 5322(a)(2)).

8 Treasury Department, Press Release, *Financial Stability Oversight Council Releases Annual Report* (Dec. 3, 2020).

9 International Monetary Fund, *United States Financial System Stability Assessment* (August 2020) at 80, App. VII at 105 (reiterating the 2015 IMF recommendation to assign a formal crisis preparedness and management coordinating role to FSOC and noting that the earlier recommendation remains unimplemented).

10 U.S. Government Accountability Office, *Financial Stability: Agencies Have Not Found Leveraged Lending to Significantly Threaten Stability but Remain Cautious Amid Pandemic* (GAO-21-167) (Dec. 2020) at 58.

26, 2021, the CIGFO Working Group requested information regarding the actions that FSOC had taken or intended to take to address the IMF and GAO recommendations.

Subsequent to the issuance of a Discussion Draft of this guidance on June 7, 2021, FSOC informed the CIGFO Working Group that it was in the process of compiling its Article IV responses to the IMF recommendations[11] and would share them with the CIGFO Working Group when the IMF report is published. On July 22, 2021, FSOC shared the U.S. Authorities' Article IV responses[12] with the CIGFO Working Group. FSOC asserted that its role "is not intended to serve as the primary responder during times of financial crisis. Rather, its purpose is to identify potential vulnerabilities and emerging threats to financial stability, and to develop recommendations for addressing those risks." On June 14, 2021, FSOC also reiterated its earlier statements regarding the GAO report (December 2020)[13] in letters to various congressional committees but did not describe any additional specific actions that FSOC had initiated or intended to initiate to address the GAO recommendation.[14]

FSOC and its member agencies have an opportunity to work together to plan for future crises. Our guidance outlined herein can serve as a reference tool for both FSOC and its member agencies. For FSOC, this information can be used to assist in fulfilling its coordination role and to help it identify risks to the financial stability of the United States by considering: (1) the type of crisis planning materials that are available for collection and dissemination to and from member agencies, (2) the threats posed to the United States' financial stability relating to potential gaps in crisis planning activities, and (3) the appropriateness of prioritizing crisis planning, consistent with member agencies' discussions. For member agencies, this guidance provides information about crisis readiness practices that can be used to: (1) reinforce and supplement current crisis readiness practices; (2) identify potential gaps in current crisis readiness plans; and (3) assist in designing and managing future crisis programs.

11 Under Article IV of the IMF's Articles of Agreement, the IMF holds bilateral discussions with members, usually every year. FSOC's Article IV responses are included in the IMF report.

12 International Monetary Fund, *United States 2021 Article IV Consultation – Press Release; Staff Report; and Statement by the Executive Director for the United States* (July 2021); Appendix IV "*Implementation of 2020 FSAP [Financial Sector Assessment Program] Recommendations*" contains the U.S. Authorities' self-assessment of the status of implementation for the recommendations of the 2020 FSAP and is not necessarily the assessment of IMF staff. https://www.imf.org/en/Publications/CR/Issues/2021/07/22/United-States-2021-Article-IV-Consultation-Press-Release-Staff-Report-and-Statement-by-the-462540

13 The GAO report recommended that FSOC, in consultation with its members, "should incorporate regular scenario-based exercises designed to evaluate individual FSOC member and collective capabilities for responding to crises into its risk-assessment activities. These could include tabletop exercises that assume increased financial risks under plausible macroeconomic and financial conditions that may require multiple regulators to respond." GAO, *Financial Stability: Agencies Have Not Found Leveraged Lending to Significantly Threaten Stability but Remain Cautious Amid Pandemic*, at 58 (GAO-21-167) (December 2020). In its December 2020 response to the GAO recommendation, FSOC explained that it leverages the work and expertise of its member agencies (i.e., heads of federal and state financial regulatory agencies) and that a number of financial regulators organize tabletop exercises in which FSOC staff regularly participate. FSOC further noted that it initiates additional activities, beyond those of its individual member agencies, including rigorous analyses for interagency discussion. *Id.* at 82.

14 Instead, FSOC's correspondence to six congressional committees reiterated that it participates in tabletop exercises organized by its member financial regulators and engages in independent activities to supplement the work of member agencies, including generating rigorous analyses for interagency discussion.

Prudent crisis preparedness can help agencies manage an array of potential crises. According to the World Economic Forum, risks that could affect the world economy and the financial stability of the United States include environmental risks caused by extreme weather events such as floods and hurricanes; natural disasters such as earthquakes and tsunamis; climate change that could amplify credit, liquidity, and counterparty risk that challenge financial management; technological risks such as large-scale cyberattacks or malware causing economic damages; violent protests; and geopolitical risks such as terrorist attacks and the deployment of nuclear, chemical, biological or radiological weapons.[15] At the FSOC meeting on March 31, 2021, the Chair of FSOC, the Secretary of the Treasury, stated during the Open Session:

> Climate change is obviously the big one. It is an existential threat to our environment, and it poses a tremendous risk to our country's financial stability. . . . Our financial system must be prepared for the market and credit risks of these climate-related events . . . . On all these fronts, the [Financial Stability Oversight] Council has an important role to play, helping to coordinate regulators' collective efforts to improve the measurement and management of climate-related risks in the financial system.[16]

Such events could lead to the disruption of key infrastructure elements for extended periods of time, including:

- Limited or no electrical power,
- Limited or no email or internet communications,
- Disrupted food and water supplies, and
- Disrupted transportation routes.

In particular, the current COVID-19 pandemic environment has highlighted the financial system's reliance on electrical and cyber connections where human contact is limited. It is important for FSOC and the financial regulators to be able to respond to such emerging threats, but also be prepared to identify risks that may exist relating to the organizations' overall crisis preparedness.

The crisis preparedness and management practices identified and summarized by the CIGFO Working Group OIGs were based upon agency planning documents to address market disruptions; contingency and crisis plans; stress tests; testing of market coordination procedures; retrospective analyses of regulator responses to prior crises; business resiliency management analyses; a prioritized supervision framework

15 The World Economic Forum is an international organization established in 1971 for public-private cooperation. The Global Risks Report 2018 identified a list of hazardous risks that could affect the world economy and thereby potentially affect insured depository institutions.

16 Secretary Janet L. Yellen, Financial Stability Oversight Council meeting (Mar. 31, 2021) https://home.treasury.gov/news/press-releases/jy0092

in response to the COVID-19 pandemic; crisis management plans; economic impact analyses following a crisis; plans for cyber incident response; lesson learned reviews; strategic plan initiatives to improve crisis management and response capabilities; audits of agency responses to emerging risks; international peer reviews of agency approaches to supervision and regulation following financial crises; and audits to assess regulatory activities under Presidential Policy Directive 21.[17] The guidance derived from these sources broadly fall into the following categories:

1. Collaboration and Pre-Crisis Planning Activities
    - Define agency mandates, roles, and responsibilities
    - Facilitate information sharing proactively
    - Strive for a shared view of market conditions
    - Implement continuous monitoring activities

2. Agencies' Crisis Readiness Plan Elements
    - Establish individual roles and responsibilities related to plans
    - Describe triggering events
    - Identify relevant legal authorities and tools, and potential emergency actions
    - Develop communication plans and options
    - Prioritize system capacity, and cyber and information security (aligned with existing continuity capabilities)
    - Provide for testing, evaluation, review, revision, and training
    - Provide for reporting

3. Agencies' Crisis Management
    - Implement leadership response
    - Coordinate among member agencies
    - Communicate to internal and external stakeholders
    - Assess resources
    - Supervise markets and regulated entities
    - Deploy response programs
    - Evaluate lessons learned

CIGFO intends this guidance to assist FSOC and its member agencies with coordinating and planning for future crises in order to help identify and mitigate risks to the financial stability of the United States associated with potential gaps in crisis preparedness. We provide this guidance in support of FSOC and its member agencies' ongoing efforts, recognizing that some activities are already broadly in practice, while other activities presented here can promote new initiatives that enhance the wider crisis planning effort. A list of the documents collected from the FSOC federal member agencies and their OIGs that were considered by the CIGFO Working Group in compiling the guidance is provided in Appendix III.

17 The Presidential Policy Directive 21, released on February 12, 2013, established a national policy on critical infrastructure security and resilience, which is a shared responsibility among federal, state, local, tribal, and territorial entities, and public and private owners and operators of critical infrastructure. The policy's goals are to enhance overall coordination and collaboration and clarify the functions, roles, and responsibilities related to critical infrastructure.

Collaboration and Pre-Crisis Planning Activities

A proactive crisis readiness effort involves working collaboratively to coordinate crisis readiness efforts across federal and state agencies and consulting with international agencies and organizations as needed. Pre-crisis preparations rely on: (1) identifying risks and conducting scenario analyses on options for how best to contain them before they escalate into crises, and (2) developing plans ahead of time that outline how an agency will respond to crises in case they materialize, known as crisis readiness planning. Member agencies may have different but overlapping missions, goals, responsibilities, and communication strategies. For these reasons, pre-planning and coordination among FSOC members is critical and includes the following actions:

- ***Define Agency Mandates, Roles, and Responsibilities***. Having a well-defined mandate and clear roles and responsibilities ensures the broad coverage of different risk categories while preventing the duplication of agency efforts, both prior to and during a crisis. Clarity in such roles and responsibilities is critical, especially because of the complexity and overlapping responsibilities among FSOC member agencies. Documenting and understanding agency mandates and roles during pre-crisis planning can assist FSOC and member agencies in conveying consistent messages to regulated entities during a crisis.

- ***Facilitate Information Sharing Proactively.*** Promoting proactive information sharing relating to crisis preparations among the agencies facilitates coordination and prevents duplication of efforts.

- ***Strive for a Shared View of Market Conditions.*** Striving to share a common view of the overall condition and risks within the financial markets is essential (including as emerging risks are identified). Coordination of interdisciplinary subject matter experts enables agencies to: (1) take a holistic view of oversight areas and associated risks; (2) develop focused guidance; (3) share information across internal and external components; and (4) communicate consistently when a crisis arises.

- ***Implement Continuous Monitoring Activities.*** Monitoring vulnerabilities to the stability of the U.S. financial sector is critical.[18] The goal of pre-crisis monitoring activities in preparing for a crisis is to limit and mitigate risks. Such monitoring activities include:

  - » Establishing risk committees to proactively evaluate risks to the financial system by capturing the collective views of multiple agencies, categorizing risks by severity, and reporting the consensus perspective

18 Financial Stability Oversight Council, Department of the Treasury, 2020 Annual Report (2020).

throughout the FSOC community;

» Conducting market surveillance to monitor for market disruption risk and requiring regulated entities to disclose market disruptions;[19]

» Monitoring and updating counterparty credit risk to enable FSOC and member agencies to quickly and accurately assess risk exposures;

» Performing stress tests to identify sources of strain and establish strategies for addressing liquidity shortfalls in emergencies;

» Generating risk assessments that account for a range of crisis scenarios that could affect financial stability and their impact and probability; and

» Conducting supervisory reviews of regulated entities' preparedness and resilience to crisis events.[20]

Thereafter, using the results of these monitoring activities helps to identify the array of risks to be addressed in crisis readiness plans.

Agencies' Crisis Readiness Plan Elements

Crisis readiness plans outline how an agency will operate in, and respond to, an array of crisis scenarios. Crisis readiness plans create an overarching crisis management framework for strategic decision making, communication, and coordination. Such a plan or management framework can include: (1) an agency-wide, all-hazards readiness plan, and (2) agency-wide hazard-specific readiness plans, as needed, that integrate divisional plans containing requirements unique to certain types of crises. Effective crisis readiness planning includes input from and consultation with relevant agency stakeholders. Some agencies have made crisis preparedness an explicit goal in their strategic plans. At a minimum, these plans achieve greater impact when they include the following elements:

- ***Establish Roles and Responsibilities.*** Identify and establish the roles and responsibilities of the individuals and groups involved in a crisis response. This includes identifying a high-level crisis leadership team and describing its responsibilities. A crisis leadership team that includes an organization's senior leadership can achieve greater impact. This team is equipped with both an enterprise-wide perspective and

19 Market surveillance includes a broader view of how risks and interconnections tie to nonfinancial businesses and the real economy.

20 Supervisory reviews should be founded on detailed written standards for cyclical, process-oriented reviews of a regulated entity's preparedness and business resiliency plans to ensure that the regulated entity has a clearly defined path to continue mission critical operations during a widespread disruption, such as a natural disaster or the loss of a critical computer system.

the authority to facilitate the efficient sharing of relevant information during a crisis and in managing the operational readiness tasks. Prior to crises, agencies also designate the staff responsible for implementing each aspect of a crisis response plan to ensure that relevant staff understand how to execute their roles and are prepared to do so when the need arises.

- ***Describe Triggering Events***. Defining what constitutes a crisis that would trigger initiation of the crisis response plan is important. When triggering events activate the crisis plan, the responsible crisis leadership officials would then undertake affirmative steps to initiate the plan.

- ***Identify Relevant Legal Authorities and Tools, and Compile a List of Potential Emergency Actions.*** Prior to a crisis, it is important to document a list of available legal tools and authorities to assist in crisis response. During a crisis, agencies may not have the luxury of time and resources to identify their relevant legal tools and authorities. Therefore, it is beneficial during steady state that an agency conducts scenario planning and analysis that thoroughly vets all legal authorities. This list of available legal authorities can include potential emergency actions that leadership may consider in response to various crisis events, as well as regulatory authorities available to, among other things, provide liquidity to financial institutions, support financial market infrastructures, facilitate the restructuring of troubled institutions, and provide regulatory relief. Such preparedness efforts also can include considering legal authorities that empower agencies with multiple options and flexibility to award and administer contracts and hire and deploy staff in response to a crisis. Agencies can also identify any legal authorities or tools they do not have but may need to manage risk or respond to a crisis and take action to seek those additional legal authorities or tools.

- ***Develop Communication Plans and Options***. A checklist of potential internal and external communication actions for leadership to consider in response to a crisis can be included in the plan. Communication both during and after the crisis event is integral to a crisis response. The checklist can include options for: (1) developing and implementing a communications strategy to promote transparency (i.e., statements by the agency head, Frequently Asked Questions, webcasts, interviews, links to temporary relief, exemptive orders, and staff guidance); (2) creating communication templates or leveraging existing communication templates; and (3) identifying potential communication media – for example creating or using existing public-facing websites, creating call centers, and preparing training materials and/or a library of program response materials.

- ***Prioritize System Capacity, and Cyber and Information Security (Aligned with Existing Continuity Capabilities)*** Crisis readiness plans can also include an evaluation of mission critical systems and equipment to assess the agency's ability to handle a crisis. An effective information security program that meets federal standards includes an incident response plan that establishes procedures for staff to follow during cyber incidents. The information security response plan documents the triggers, procedures, roles and responsibilities, including forming an incident assessment group, and resources for eradicating and/or limiting the expansion of an information security incident and minimizing its effects. The incident response plan includes an incident recovery plan that identifies individuals responsible for initiating the recovery plan, defines criteria that must be met to return compromised services and technology to the network, and explains how to document the decisions and actions taken for future reference. The incident response plan also addresses how to coordinate communication with internal and external stakeholders about response and restoration activities. These plans and options are aligned with agencies' business continuity plans and encompass forecasting budget and staffing resources to address crisis response activities prospectively before a crisis occurs.

- ***Provide for Testing, Evaluation, Review, Revision, and Training***. Crisis readiness plans can also include a process to review, test, and revise crisis readiness plans on a recurring basis.[21] Training can ensure that agency personnel have the requisite knowledge, skills, and abilities to execute the crisis management tasks. Training can explain the delegations of authority and options for potential actions. It is important that an agency establish feedback mechanisms to assess the lessons learned from training, simulation exercises, and actions undertaken during an actual crisis event to systematically incorporate improvements into the crisis readiness plans. Periodic reviews and readiness plan updates can also reflect any changes in the operational environment, system resources, leadership structure, and the evolution of industry standards, laws, and regulations.

- ***Provide for Reporting***. Plans can also provide a mechanism to regularly report to key decision makers about the agency's crisis readiness.

Agencies' Crisis Management

Crisis planning and crisis management work in tandem. Once agency leadership determines that a crisis exists, senior agency leaders consult and modify, as needed, the crisis readiness plans developed during the

21 For example, agencies can conduct exercises of the crisis readiness plan under different emergency scenarios. These periodic exercises, usually occurring at least annually, are followed by an after-action review to capture observations and identify areas for improvement.

pre-crisis planning period. These actions equip FSOC member agency leaders to create the crisis management strategy. The crisis management strategy dictates the response to a crisis. Key elements that contribute to effectively managing a crisis include clear leadership response, coordination, communication, resource assessments, supervisory activities, and implementation of response or rescue programs.

- ***Implement Leadership Response.*** Consistent with the roles and responsibilities outlined in their crisis readiness plans, agencies deploy a leadership response in which strategic decision-making and coordination occur at the senior agency level, and operational and tactical authorities remain within appropriate business areas to ensure efficient management of incidents. The senior crisis management team can serve to provide strategic leadership, set response priorities, inform and/or consult with key governance bodies, and escalate policy issues as appropriate. Meanwhile, a crisis communication team may coordinate with crisis leadership and support consistent, timely, and effective communication with stakeholders.

- ***Coordinate Among Member Agencies***. For specific crises, using pre-existing working groups or establishing interagency working groups and sub-working groups fosters the exchange of ideas, and helps to facilitate decision-making and determine plans for action and communications. Working groups can assist leadership by providing crisis support and helping to facilitate the crisis management process, gather status updates, develop situation reports, facilitate an understanding of business functional and operational impacts across the organization, gather information from external subject matter experts and government authorities, and provide situational awareness. The working group, or sub-working group, also can include a team to review available data, assumptions, and methodologies in use and recommend a consistent analytical framework across agencies. Standardizing data is critical to the agencies' collective analysis of the economic and financial impacts of the crisis, including the effects of the policy actions taken in response to the crisis.

- ***Communicate to Internal and External Stakeholders***. Publicly communicating individual agency's responses to the crisis promotes transparency. Public communications provide insight into each agency's efforts and how it is continuing to fulfill its mission. Agencies consider the options for communicating to agency employees, regulated entities, and the public. Internally, agencies may consider interdivisional instructions for team notifications in the event deployments become necessary on short notice. Internal communication provides updated information relevant to employees via direct communication and/or a webpage. Communications are coordinated with crisis leadership, as previously noted.

External communication provides for statements by agency leaders, interviews, guidance, websites, and call centers as potential communication channels. In addition, interagency guidance and interagency statements can be effective tools to clarify a supervisory approach and convey that message clearly to institutions and markets.

- ***Assess Resources.*** Managing surge staffing by onboarding new employees at a pace that aligns with the crisis demands on workforce capacities is essential. Senior leaders responsible for crisis management consider the need to meet both budget and staffing increases, commensurate with crisis demands. Understanding the possible options available in advance can help to expedite the potentially large-scale hiring and onboarding of new staff to address crisis response activities, such as administering response programs or responding to institutional failures. Leaders use flexible hiring and staffing approaches, as presented in the crisis planning phase. This may also necessitate flexible hiring and contracting processes during crisis management. Pay, benefit, and interim work schedule flexibilities, for example, can be useful in expediting the hiring process during a crisis. As a part of the resource assessment, if changes to the workforce occur as a result of the crisis, like it did during the COVID-19 pandemic, it is important to design training that could be quickly transitioned to virtual sessions and to provide remote access to all employees. Supporting a remote workforce required agencies to provide technical guidance to assist in securely connecting to agency systems. Future crises may present different challenges requiring agencies to assess additional support alternatives for their workforce.

- ***Supervise Markets and Regulated Entities.*** Coordinating and prioritizing supervisory activities on those markets and entities that pose the greatest risk is critical.[22] Adapting supervisory approaches, such as: (1) focusing on monitoring and outreach to help financial institutions and market participants understand the challenges and risks of the environment, and (2) allowing temporary changes to examination activities to minimize disruptions. Such changes might include granting additional time to resolve existing noncritical supervisory findings. During a crisis, agencies can communicate with other federal and state regulators to avoid duplicative efforts and to coordinate efforts in executing revised supervisory approaches. Notably, large interconnected financial institutions often require heightened supervisory attention due to the greater complexity of their operations and the outsized risks that they can pose to the U.S. economy.

22 To accomplish the goal of focusing supervisory activity on those markets and entities that pose the greatest risk, an agency conducting prioritized assessments ranks the risks under its jurisdiction and analyzes staff capacity to prioritize how to deploy limited resources. Another goal of this approach is to increase the efficiency and effectiveness of information flow collected by the agencies related to operational changes and regulatory challenges, and to coordinate with other federal and state regulatory agencies.

- ***Deploy Response Programs.*** Response programs typically involve government investments, loans, guarantees, or repayment modifications, and are designed to address the unique circumstances of a particular crisis. Programs should be transparent, and decisions relating to them should be documented to ensure that the process is clear and understandable, and that there is an appropriate level of oversight. Having specific, measurable goals for federal rescue programs, and aligning funding accordingly, is necessary. Effective program design clearly identifies the metrics by which success will be measured and how management will monitor and report the agency's progress in meeting these goals. In managing the program, agency managers also monitor the program's activities, which ensures that funds are used as intended. Regular assessments and communication, to include the exit path and end date for response programs, are also useful.

- ***Evaluate Lessons Learned.*** Following a crisis and return to steady state, initiating after-action reviews to examine the cause(s) for any implementation issues, analyzing the effectiveness of the agency's crisis management process, identifying opportunities for improvement, and acting on those opportunities for improvement is helpful. It is important that agencies coordinate these efforts and collaborate to produce post-event analyses and reports. Based on the observations in the after-action reviews, agency leadership should consider initiating improvement planning. Improvements should consider the applicability to all crisis readiness plans, not just to the hazards and crisis plans utilized during the preceding crisis.

Conclusion

The foregoing guidance is intended to assist FSOC and its member agencies in coordinating, sharing information, and planning for future crises. For FSOC, this guidance can be used to collect and disseminate crisis readiness information to member agencies as well as to assist with assessing the risks to the United States' financial stability associated with agencies' crisis readiness preparedness. For member agencies, this guidance can be used to assist with planning for future crises. The crisis preparedness and management practices identified and summarized in this guidance as well as the crisis preparedness actions previously recommended by the IMF and GAO can inform FSOC and its member agencies and help to preserve the financial stability of our nation during future crises.

On March 23, 2022, FSOC provided a written response to this guidance document.[23] FSOC's response is included as Appendix II.

23 Prior to issuance of this report, CIGFO and FSOC engaged in pre-decisional discussions to ensure a full understanding of the report's guidance before CIGFO received FSOC's final management response.

APPENDIX I

Abbreviations

Act/Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
COVID-19	Coronavirus Disease 2019
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CIGFO	Council of Inspectors General on Financial Oversight
FDIC	Federal Deposit Insurance Corporation
FHFA	Federal Housing Finance Agency
FIO	Federal Insurance Office
FRB	Board of Governors of the Federal Reserve System
FSOC	Financial Stability Oversight Council
GAO	U.S. Government Accountability Office
HUD	U.S. Department of Housing and Urban Development
IG	Inspector General
IMF	International Monetary Fund
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
OFR	Office of Financial Research
OIG	Office of Inspector General
SEC	U.S. Securities and Exchange Commission
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
Treasury	Department of the Treasury

APPENDIX II

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

March 23, 2022

The Honorable Richard K. Delmar
Acting Chair, Council of Inspectors General
on Financial Oversight
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Re: Audit Follow-Up Regarding Financial Stability Oversight Council

Acting Chair Delmar:

I write in response to the Council of Inspectors General on Financial Oversight's (CIGFO) report containing draft guidance to the Financial Stability Oversight Council (FSOC) and its member agencies on preparing for and managing crises.

As noted in CIGFO's draft "Guidance in Preparing for and Managing Crises," FSOC plays an important role in promoting information sharing and collaboration to address potential risks to financial stability.

It is vital for the government to be prepared to act in the event of unpredictable crises that affect the financial sector. For that reason, banking and market regulatory agencies regularly engage with their domestic and international counterparts in many of the activities described in CIGFO's guidance, to prepare for financial crises. Their efforts since the financial crisis in 2008-09 have considerably strengthened the mechanisms for coordination and crisis planning. This work now occurs across many venues at all levels of the agencies' seniority, including tabletop exercises for how to respond and recover to financial and cyber incidents; discussions at FSOC regarding potential financial stability risks; participation in crisis management groups with domestic and foreign supervisors; and information-sharing regarding cyber resilience at the Financial and Banking Information Infrastructure Committee. We applaud these existing efforts by the agencies.

FSOC has the statutory authority to facilitate information sharing and coordination among financial regulators regarding threats to U.S. financial stability. In implementing this authority, FSOC has avoided duplicating regulators' existing planning processes related to potential crises. Instead, FSOC's work to fulfill its mission complements the efforts of its members. FSOC's activities in response to the financial market dislocations early in the COVID-19 pandemic are a prime example of how FSOC can help agencies respond to a crisis and share information about evolving developments at financial firms and in financial markets. During that period of market instability, FSOC convened frequent meetings among staff and principals of member agencies to share information about agencies' actions to support market functioning and ease liquidity constraints. FSOC also plays an important role in addressing climate-related financial risks;

FSOC's recently published *Report on Climate-Related Financial Risk*[1] is another example of FSOC fulfilling its information-sharing and collaboration role. FSOC recently fulfilled the first recommendation in the climate report by forming a new staff-level committee, the Climate-related Financial Risk Committee, to coordinate, share information, and facilitate the development of common approaches and standards in order to increase the resilience of the financial sector to climate risks.

To address the issues raised by the draft CIGFO guidance, Treasury will recirculate the guidance to all of the FSOC member agencies and will encourage agencies that have not developed an approach to crisis management to do so and to coordinate, as appropriate, with other federal or state regulators. In addition, when the Council discusses potential responses to mitigate potential risks to financial stability, we will seek to collaborate regarding agencies' crisis-management planning and tools that are relevant to those risks. We will also remain vigilant in fulfilling FSOC's statutory purposes of identifying risks to financial stability, promoting market discipline, and responding to emerging risks to the stability of the U.S. financial system.

We appreciate your support of FSOC and its member agencies' work in this area, and we remain committed to working closely with CIGFO on this and other reviews.

Sincerely,

Sandra Lee Digitally signed by Sandra Lee Date: 2022.03.23 20:51:04 -04'00'

Sandra Lee
Deputy Assistant Secretary
Financial Stability Oversight Council

[1] The report is available at https://home.treasury.gov/system/files/261/FSOC-Climate-Report.pdf.

2

APPENDIX III

SOURCES USED BY THE CIGFO WORKING GROUP TO DEVELOP GUIDANCE

COLLABORATION AND PRE-CRISIS PLANNING ACTIVITIES

Commodity Futures Trading Commission. (2020, October 20). *CFTC and BoE Sign New MOU for Supervision of Cross-Border Clearing Organizations* [Press Release 8289-20]. https://www.cftc.gov/PressRoom/PressReleases/8289-20

Commodity Futures Trading Commission. (2019, February 25). *Joint Statement by UK and US Authorities on Continuity of Derivatives Trading and Clearing Post-Brexit* [Press Release 7876-19]. https://www.cftc.gov/PressRoom/PressReleases/7876-19

Commodity Futures Trading Commission. (2020). [redacted]. (hereinafter "[redacted]")

Department of the Treasury Office of Inspector General. (2013). *Safety and Soundness: OCC Identification of Emerging Risks* https://oig.treasury.gov/sites/oig/files/Audit_Reports_and_Testimonies/OIG13037.pdf

Federal Deposit Insurance Corporation. (2012). *Effectively Managing FDIC's Resources – Meeting the Challenges of the Financial Crisis, 2008-2011*. (hereinafter "FDIC, Managing FDIC's Resources")

Federal Housing Finance Agency. (2019). *AB 2019-01 Business Resiliency Management* https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Business-Resiliency-Management.aspx

Federal Housing Finance Agency. (2018). *AB 2018-07 Federal Home Loan Bank Liquidity Guidance* https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Federal-Home-Loan-Bank-Liquidity-Guidance.aspx

Federal Housing Finance Agency. (2013). *AB 2013-01 Contingency Planning for High-Risk or High-Volume Counterparties* https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/AB-2013-01-CONTINGENCY-PLANNING-FOR-HIGH-RISK-OR-HIGH-VOLUME-COUNTERPARTIES.aspx

Financial Stability Oversight Council. (2020). *2020 Annual Report* https://home.treasury.gov/system/files/261/FSOC2020AnnualReport.pdf

Office of the Comptroller of the Currency. (2013). *An International Review of OCC's Supervision of Large and Midsize Institutions* https://www.occ.gov/news-issuances/news-releases/2013/nr-occ-2013-184a.pdf

Office of the Special Inspector General for the Troubled Asset Relief Program. (2014). *What Makes a Bank Systemically Important?*, Written Testimony of Christy L. Romero before the U.S. Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on Financial Institutions and Consumer Protection. https://www.sigtarp.gov/sites/sigtarp/files/Testimony/SIGTARP_testimony_TBTF_and_SIFI_regulation_July_16_2014.pdf

CRISIS READINESS PLAN ELEMENTS

Board of Governors of the Federal Reserve System (2020). [redacted] (hereinafter "[redacted]")

Board of Governors of the Federal Reserve System (2019). [redacted]. (hereinafter "[redacted]")

Board of Governors of the Federal Reserve System (2018). [redacted].

[redacted] *supra*

FDIC, Managing FDIC's Resources, *supra*

Federal Deposit Insurance Corporation. (2020). *FDIC Chairman Letter to Representative Maxine Waters*. (hereinafter "FDIC Chairman Letter")

Federal Deposit Insurance Corporation. (2018). *Atlanta Region Critical Event Management Plan.*

Federal Deposit Insurance Corporation Office of Inspector General. (2020). *The FDIC's Readiness for Crises [EVAL-20-004]* https://www.fdicoig.gov/sites/default/files/publications/EVAL-20-004.pdf

Federal Housing Finance Agency. (2017). *AB 2017-02 Information Security Management* https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Information-Security-Management.aspx

Federal Housing Finance Agency. (2018). *AB 2018-06 Liquidity Risk Management* https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Liquidity-Risk-Management.aspx

National Credit Union Administration. (2020). [redacted]. (hereinafter "[redacted]")

U.S. Securities and Exchange Commission (2020). [redacted]. (hereinafter "[redacted]")

U.S. Securities and Exchange Commission (2020). [redacted].

U.S. Securities and Exchange Commission. (2020) *SEC Coronavirus (COVID-19) Response* https://www.sec.gov/sec-coronavirus-covid-19-response (hereinafter "SEC COVID Response")

U.S. Securities and Exchange Commission. (2018). *U.S. Securities and Exchange Commission Strategic Plan Fiscal Years 2018-2022* https://www.sec.gov/files/SEC_Strategic_Plan_FY18-FY22_FINAL.pdf

CRISIS MANAGEMENT

Consumer Financial Protection Bureau. (2020). [redacted].

FDIC Chairman Letter, *supra*

FDIC, Managing FDIC's Resources, *supra*

Federal Deposit Insurance Corporation. (2017). *Crisis and Response, An FDIC History, 2008-2013* https://www.fdic.gov/bank/historical/crisis/

Federal Deposit Insurance Corporation. (2017). *Draft Debt Ceiling Contingency Planning Summaries*

Federal Housing Finance Agency. (2020). *(FNM-DER-2020-023) (FRE-DER-2020-027) Operational Risks Associated with Coronavirus Disease 2019 (COVID-19)*

FRB 2020 [redacted], *supra*

[redacted] *supra*

NCUA [redacted], *supra*

Office of the Special Inspector General for the Troubled Asset Relief Program. (2012). *Factors Affecting Implementation of the Hardest Hit Fund Program [SIGTARP 12-002]* https://www.sigtarp.gov/sites/sigtarp/files/Audit_Reports/SIGTARP_HHF_Audit.pdf

Office of the Special Inspector General for the Troubled Asset Relief Program. (2009). *Initial Report to the Congress* https://www.sigtarp.gov/sites/sigtarp/files/Quarterly_Reports/SIGTARP_Initial_Report_to_the_Congress.pdf

Office of the Special Inspector General for the Troubled Asset Relief Program. (2011). *Legal Fees Paid Under the Troubled Asset Relief Program: An Expanded Report [SIGTARP 11-004]* https://www.sigtarp.gov/sites/sigtarp/files/Audit_Reports/G%2009%20OFS%20Contracting%20Final%2011-004%2009-28-2011.pdf

Office of the Special Inspector General for the Troubled Asset Relief Program. (2011). *Quarterly Report to Congress* https://www.sigtarp.gov/sites/sigtarp/files/Quarterly_Reports/October2011_Quarterly_Reportto_Congress.pdf

SEC COVID Response, *supra*

SEC [redacted] *supra*

U.S. Securities and Exchange Commission (2020). [redacted] [redacted].

APPENDIX IV

CIGFO Working Group

Federal Deposit Insurance Corporation Office of Inspector General, Co-Lead		
Jay Lerner, Inspector General, Federal Deposit Insurance Corporation		
Terry Gibson	Cynthia Hogue	Stacey Luck
Rigene Mabry	Michael Reed	
Special Inspector General for the Troubled Asset Relief Program, Co-Lead		
Melissa Bruce, Acting Special Inspector General, Troubled Asset Relief Program		
Jenniffer Wilson	Marc Geller	Jennifer Kim
James Lloyd	Gabriele Tonsil	
Department of the Treasury Office of Inspector General		
Richard Delmar, Deputy Inspector General, Department of the Treasury and Acting CIGFO Chair		
Deborah Harker	Susan Barron	Jeffrey Hawkins
Andrew Morgan	Tayla Haughton	Kajuana Britt
Katherine Draper	Sheila Arguello	Timothy Cargill
Jackquelynne Foley		
Department of Housing and Urban Development, Office of Inspector General		
Rae Oliver Davis, Inspector General, Department of Housing and Urban Development		
Lisa Sweeney	Greg Soames	
Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau Office of Inspector General		
Mark Bialek, Inspector General, Board of Governors of the Federal Reserve System and Consumer Financial Protection Bureau		
Michael VanHuysen	Jason Derr	Laura Shakarji
Margaret An	Matt Gibbons	
Federal Housing Finance Agency Office of Inspector General		
Brian Tomney, Inspector General, Federal Housing Finance Agency		
Marla Freedman	Robert Taylor	James Lisle
April Ellison	Michael Rivera	
National Credit Union Administration Office of Inspector General		
James Hagen, Inspector General, National Credit Union Administration		
Marvin Stith		
U.S. Securities and Exchange Commission Office of Inspector General		
Carl Hoecker, Inspector General, U.S. Securities and Exchange Commission		
Rebecca Sharek	Kelli Brown-Barnes	Douglas Carney
Lucia Fuentes Bermudez		
U.S. Commodity Futures Trading Commission Office of Inspector General		
A. Roy Lavik, Inspector General, U.S. Commodity Futures Trading Commission		

This page is intentionally blank