JULY 2025

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 or Council) 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 comprises eight Inspectors General (IG) responsible for oversight of agencies and programs in the financial sector, 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, FSOC issued its *Report on Nonbank Mortgage Servicing* which describes the growth of the nonbank mortgage servicing sector and the critical roles that nonbank mortgage servicers play in the mortgage market, and a *Study on the Effects of Size and Complexity of Financial Institutions on Capital Market Efficiency and Economic Growth* pursuant to Section 123 of Dodd-Frank, which updates the study issued in 2016. Additionally, FSOC and the Brookings Institution hosted a conference on Artificial Intelligence (AI) and financial stability which brought together public and private sector participants to discuss the evolving role of AI in the financial system and the potential implications for U.S. financial stability. As FSOC focuses on new and evolving risks and challenges, CIGFO continues its role and remains diligent in fulfilling its 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 July 2024, CIGFO convened a working group to assess FSOC's revised *Guidance on Nonbank Financial Company Determinations*, which is expected to be completed in the spring of 2026. CIGFO member Inspectors General and CIGFO, as a collective body, perform a valuable role during Presidential transitions. Based on its experience and unique perspective, CIGFO is a valuable source of information about key financial oversight issues that will confront the new Administration. In December 2024, CIGFO released an updated Presidential Transition Handbook as a guide on CIGFO's roles and authorities as well as transition issues and interactions. This handbook is provided as Appendix A.

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 efforts by the Department of the Treasury and other federal financial regulators to gather information on the development and application of AI within the financial sector, various legal cases and rulings regarding challenges to the *Corporate Transparency Act* and Financial Crimes Enforcement Network rules implementing elements of the Act; as well as legislative activities that could impact the financial regulatory system. Treasury's Office of

Cybersecurity and Critical Infrastructure Protection briefed CIGFO on managing AI and specific cybersecurity risks in the financial services sector.

In March 2025, FSOC welcomed new leadership to the Council and the Chairperson established the following priorities for the Council: enhancements to the member agencies' supervisory and regulatory frameworks, as well as other efforts to position banks and other regulated entities to foster innovation and otherwise support economic growth.

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/

Loren Sciurba
Acting Chair, Council of Inspectors General on Financial Oversight
Deputy Inspector General, Department of the Treasury

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

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. 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 year, 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:

- Efforts by the Department of the Treasury (Treasury) and other federal financial regulators to request information on the uses, opportunities, and risks presented by the development and application of artificial intelligence within the financial sector.
- Various legal cases and rulings regarding challenges to the *Corporate Transparency Act* (CTA) and Financial Crimes Enforcement Network (FinCEN) rules implementing elements of CTA.
- Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) – Treasury's report Managing Artificial Intelligence – *Specific Cybersecurity Risks in the Financial Services Sector.*
- The *Financial Data Transparency Act* and the proposed Joint Data Standards rule issued by the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (the Board), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Consumer Financial Protection Bureau (CFPB), Federal Housing Finance Agency (FHFA), Commodity Futures Trading Commission (CFTC), U.S. Securities and Exchange Commission (SEC), and Treasury.
- Legislative matters of interest, including proposed legislation on various topics including: proposed changes to 5 USC, Chapter 4, the Inspector General Act; HR 532, the Keep the Watchdogs Running Act, and Section 4101 of the *American Financial Institution Regulatory Sovereignty and Transparency Act of 2023*.

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 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*
- 2023 – *Audit of the Financial Stability Oversight Council's Efforts to Address Climate-Related Financial Risk*
- 2024 - *Council of Inspectors General on Financial Oversight Presidential Transition Handbook (Updated)*

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.

In response to the economic disruptions caused by the COVID-19 pandemic, 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 played 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.

Joint Work

Federal Information Security Modernization Act of 2014 Capstone Report

The United States faces persistent and increasingly malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. We worked with CIGIE and other OIGs to report on information security program

trends across the government. Federal agencies have strengthened the maturity of their information security programs on average in recent years. However, the share of agencies with an effective information security program has held at around 60 percent. More actions are needed in key areas—supply chain risk management, cybersecurity risk management, and configuration management—to ensure that agencies' information security programs can deal with cybersecurity threats effectively.[1]

Completed Work, April 1, 2024-March 31, 2025

Board

Major Management Challenges

- Strengthening Organizational Governance and Enterprise Risk Management
- Managing Workforce Planning and Updating the Human Capital System
- Enhancing Cybersecurity Oversight at Supervised Financial Institutions and Service Providers
- Remaining Adaptable While Supervising Financial Institutions
- Ensuring That Physical Infrastructure Effectively Meets Mission Needs
- Modernizing Information Technology Systems, Services, and Operating Models
- Ensuring an Effective Information Security Program
- Evolving With Financial Sector Innovations
- Leveraging Artificial Intelligence to Enhance Mission Delivery
- Wind-Down of COVID-19 Pandemic Emergency Lending Facilities and Their Underlying Loan Portfolios

FRB Minneapolis Followed Its Paycheck Protection Program Liquidity Facility Collateral Risk Management Processes and Can Enhance Monitoring and Collection Processes

The PPPLF advanced about $200 billion to lenders to keep credit flowing to small businesses during the COVID-19 pandemic. Just over $3 billion remained outstanding as of March 31, 2024. We assessed the effectiveness of the PPPLF's processes for (1) identifying and managing at-risk and unresolved collateral, (2) addressing nonpayment, and (3) detecting and mitigating fraudulent collateral.

FRB Minneapolis, which administers the PPPLF, followed its risk management process for at-risk, unresolved, and potentially fraudulent collateral used to back PPPLF loans. However, the PPPLF did not fully develop and document measures to address nonpayment. Also, we noted measures to reduce financial risk if the Board implements a similar liquidity facility in the future.

[1] Joint contributors to this report include the OIGs for the U.S. Securities and Exchange Commission, the U.S. Department of Commerce, the U.S. Department of Defense, and the U.S. Department of Homeland Security.

Our report contains one recommendation to help FRB Minneapolis strengthen its processes related to repayment of outstanding advances. FRB Minneapolis concurred with our recommendation.

The Board and the Reserve Banks Generally Met the Revised Timing Goals for Certain Fair Lending Matters

In January 2021, the Board implemented a revised review process for submitting and reviewing high-risk redlining matters to improve efficiency. *Redlining* is illegal discrimination that occurs when a lender provides unequal access to credit, or unequal terms of credit, because of the race, color, national origin, or other prohibited characteristics of the residents of the area where the prospective borrower resides, plans to reside, or seeks to obtain a mortgage on a residential property. We assessed the Board's implementation of its revised review process for high-risk redlining matters from examinations opened in 2022 and 2023, including delegating certain matters to the Federal Reserve Banks.

We assessed the timeliness of the revised review process and found that the Board and the Reserve Banks generally met their revised timing goals for submitting and reviewing high-risk redlining matters. Therefore, our report does not have any recommendations.

The Bank Exams Tailored to Risk Process Promotes Risk-Focused Supervision of Community Banking Organizations, but Training Can Be Enhanced

The Board seeks to ensure that the institutions under its supervisory authority, including community banking organizations, operate in a safe and sound manner and comply with all applicable federal laws and regulations. We assessed the Board and Reserve Banks' application of the Bank Exams Tailored to Risk (BETR) process for community banking organizations.

We found that the BETR process allows Reserve Bank examination staff to tailor their supervisory activities to promote risk-focused supervision and effective resource allocation; however, additional training will enhance examiners' ability to use BETR to scope examinations and will increase the effectiveness of the BETR process. Management should also consider creating guidance on using BETR for institutions with unique business models or novel activities.

Our report contains two recommendations designed to enhance the effectiveness of the Board and Reserve Banks' BETR process. The Board concurs with our recommendations.

Results of Security Control Testing of the Board's Embargo Application

The Board's web-based embargo application allows authorized members of the media to access documents that are not yet posted to the Board's public website. To meet FISMA requirements, we reviewed selected information security controls for the application.

Overall, the security controls we tested for the embargo application were effective. For example, the Board ensured that privileged access was provisioned on a need-to-know basis. In addition, required embargo application events were logged and retained in accordance with Board requirements. However, the Board can strengthen access and configuration management controls for the embargo application.

Our report includes one recommendation and one matter for management consideration. The Board concurred with our recommendation. Given the sensitivity of the information in our review, our full report is restricted.

The Board Can Enhance Its Approach to the Cybersecurity Supervision of Community Banking Organizations

Cyber threats are continually evolving and becoming more complex. The Board and the Federal Reserve Banks assess community banking organizations' (CBO) cybersecurity as part of their information technology (IT) supervisory activities. We assessed the effectiveness of the Board's and the Reserve Banks' cybersecurity supervision approach for CBOs.

We found that the Board can enhance its approach to the cybersecurity supervision of CBOs. Specifically, we found that the Information Technology Risk Examination, or InTREx, work programs are not up to date and do not reflect the evolving IT and cybersecurity risk environment. We also found that the selected Reserve Banks' approaches to CBO IT training vary and that the Federal Reserve System does not provide clear training expectations for generalist examiners assigned to conduct CBO IT examinations. Finally, we found that the Reserve Banks we reviewed had varying practices for completing and retaining IT Profile documents, which examiners use to assess the technology risk of institutions and scope CBO IT examinations.

Our report contains five recommendations designed to enhance the Board's approach to its cybersecurity supervision of CBOs. The Board concurred with our recommendations.

2024 Audit of the Board's Information Security Program

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

The Board's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. Since our review last year, we found that the Board has

taken steps to strengthen its information security program, for example, by updating its personnel security processes to help ensure position risk designations are documented and used in personnel security processes.

However, the Board can strengthen its information security program. Specifically, the Board should develop a supply chain risk management strategy; define a review and escalation process for alerts generated by the Board's data loss prevention (DLP) tool; consistently document system interconnections and required documentation; perform vulnerability scanning on mobile devices and applications; annually test, review, and approve the incident notification and breach response plan to maintain organizational cyber resiliency; provide role-based privacy training to help ensure that individuals are knowledgeable and aware of their privacy roles and responsibilities; perform targeted phishing exercises to increase the cyber awareness of the Board's executives and those with significant security responsibilities; and ensure that contractual requirements for the Board's cloud service providers for the timely reporting of incidents are consistent with federal requirements.

Fourteen recommendations from our prior FISMA audit reports remain open. This report contains nine new recommendations. The Board concurs with our recommendations. We believe that if sufficient progress is not made to address our open recommendations, the Board's information security program maturity rating could decline in 2025.

Ongoing Work as of March 31, 2025
Board

Evaluation of the Board's and the Reserve Banks' Practices for Following Up on Supervisory Findings That Address Safety and Soundness Issues

The Federal Reserve System communicates supervisory findings through matters requiring attention (MRAs) and matters requiring immediate attention (MRIAs). According to the *Commercial Bank Examination Manual, MRAs* are matters that the System expects a banking organization to address over a reasonable amount of time, and *MRIAs* are matters of significant importance and urgency that the System expects a banking organization to address immediately. The Board expects examiners to follow up on MRAs and MRIAs to assess a banking organization's progress and to validate that the organization has implemented satisfactory corrective actions. We plan to assess the effectiveness of the Board's and the Reserve Banks' practices for following up on supervisory findings that address safety and soundness issues.

Evaluation of the Board's Insider Risk Management Activities

The Federal Reserve System generates and collects economic information that is considered sensitive because it can significantly influence financial market activity. We will assess the insider risk management activities of the Board, focusing on the design and effectiveness of the Board's approach to deter, detect, and mitigate insider risks.

2025 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 their respective agency's information security program and practices. To meet FISMA requirements for 2025, 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 selected 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 2025 FISMA reporting metrics for inspectors general.

Completed Work, April 1, 2024-March 31, 2025
CFPB

The CFPB Can Improve Its Process for Onboarding Depository Institutions That Transition to Its Oversight

A key mission of the CFPB is overseeing compliance with federal consumer financial laws and regulations for depository institutions with over $10 billion in assets. From 2017 through 2023, 90 depository institutions crossed the $10 billion threshold and transitioned to the CFPB's oversight. We assessed the CFPB's process for transitioning these depository institutions.

We found that the CFPB did not timely or effectively complete most of the transitions we reviewed, in some cases taking over a year to complete key onboarding steps. The agency also took varying approaches to coordinating with the prudential regulators. We attribute these issues to the CFPB not having established a program for onboarding depository institutions that transition to its oversight.

Our report contains four recommendations to enhance the CFPB's onboarding of depository institutions. The CFPB concurs with our recommendations.

The CFPB Can Enhance Certain Aspects of Its Examiner Commissioning Program

CFPB examiners assess supervised institutions' compliance with federal consumer financial laws. Examiners must successfully complete the Examiner Commissioning Program to receive their commissions, which signifies technical expertise in their duties. We assessed the CFPB's approach to examiner commissioning.

We found that the CFPB can make its commissioning program more consistent in terms of opportunities, mentoring, and other support for examiners. It can also provide examiners specific, actionable feedback following a key component of the commissioning program.

Finally, the CFPB should consider formalizing an approach for diversifying assessment panels and periodically collect qualitative information to alleviate concerns about the program's fairness.

Our report includes three recommendations to enhance the CFPB's commissioning program. The CFPB concurred with our recommendations.

The CFPB Effectively Designed a Process to Allocate Surplus Civil Penalty Funds and Monitored Contractor Payments to Victims

The CFPB maintains the Civil Penalty Fund (CPF) to compensate people harmed by companies that violate consumer financial protection laws and allows the CFPB, under certain circumstances, to use excess CPF funds for consumer education and financial literacy programs. As of September 2023, the CPF had collected $3.4 billion and held a balance of $1.9 billion. We assessed (1) the process design for allocating CPF funds for the purpose of consumer education and financial literacy programs and (2) the effectiveness of processes for overseeing the contractors' distributing payments to victims.

The CFPB's process for allocating CPF funds prioritizes victim compensation over consumer education and financial literacy programs. Prioritizing victim compensation, including maintaining a reserve to compensate future victims, and using operating funds for consumer education programs allows the agency to pay all eligible victims and continue to fund consumer education initiatives. In addition, the CFPB provided effective oversight of contractors, ensuring that eligible victims received accurate payments. We identified $11 million in unspent funds that was allocated to consumer education and financial literacy programs; as a result, during our audit the CFPB deallocated those funds and made them available for future victim compensation.

Our report does not contain recommendations.

The CFPB Effectively Monitors Consumer Complaints but Can Enhance Certain Processes

The CFPB collects, investigates, and monitors consumer complaints about financial products and services. The number of these complaints has grown significantly in recent years, reaching nearly 1.3 million in 2022. We assessed the effectiveness of the Office of Consumer Response's processes for reviewing and monitoring the timeliness, accuracy, and completeness of company responses to consumer complaints in accordance with its established directives and procedures.

The CFPB uses a risk-based approach to select companies for review and prioritizes companies with the most complaints. The agency has followed its processes for conducting reviews, but we found incomplete documentation in limited cases. Further, a pilot process to provide companies with reports about their complaint handling and response performance

lacked key components: measurable objectives, a completion date, formal written guidance, and an approach to evaluate the pilot.

Our report contains three recommendations to enhance the CFPB's processes for issuing company-specific reports on response performance. The CFPB concurred with our recommendations.

2024 Audit of the CFPB's Information Security Program

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

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 taken several steps to strengthen its information security program. For example, the agency improved its security training program by incorporating threat intelligence to update its workforce on a near-real-time basis.

However, the CFPB can strengthen its information security program. Specifically, the CFPB can mature DLP processes by developing data classification policies and procedures and by configuring its DLP tool accordingly; strengthen processes to ensure timely remediation of critical and high-risk vulnerabilities; ensure that system users are periodically reinvestigated to maintain access authorizations and privileges; improve incident processes to effectively respond to a potential ransomware incident; strengthen organizational resiliency by conducting a comprehensive test of its continuity of operations plan; and ensure the accuracy of the information in its cybersecurity governance, risk, and compliance tool.
Three recommendations from our prior FISMA reports remain open. This report includes eight new recommendations. The CFPB concurs with our recommendations.

Results of the Security Controls Testing of the CFPB's Consumer Resource Center Mosaic System

The CFPB's Consumer Resource Center Mosaic system is a cloud-based system used for the agency's consumer complaint program. As part of our 2023 audit of the CFPB's information security program, we contracted with an independent firm to test selected security controls for the system. For the selected security controls tested, no areas for improvement were identified; therefore, this report does not contain recommendations. Given the sensitivity of the information in our review, our full report is restricted.

Ongoing Work, as of March 31, 2025
CFPB

Evaluation of the CFPB's Approach to Safeguarding Confidential Supervisory Information

The CFPB ensures compliance with federal consumer financial laws by supervising market participants. During examinations, CFPB examiners obtain information from supervised entities, including nonpublic, confidential information that could cause harm if lost or misused. CFPB examiners also prepare reports, working papers, and other documents and materials that contain confidential supervisory information. We are assessing the CFPB's controls for safeguarding confidential supervisory information.

2025 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 their respective agency's information security program and practices. To meet FISMA requirements for 2025, 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 selected 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 2025 FISMA reporting metrics for inspectors general.

Office of Inspector General
Commodity Futures Trading Commission

The CFTC OIG acts as an independent Office within the CFTC that is committed to detecting and preventing fraud, waste, abuse, and other violations of the law, and to promoting the economy, efficiency and effectiveness in the operations of the CFTC. The OIG promotes improvements to CFTC strategic operations, programs, and initiatives by independently, conducting value added audits, evaluations, investigations, and other reviews.

Background

The CFTC OIG was created in 1989 in accordance with the 1988 amendments to the Inspector General Act of 1978 (See 5 U.S.C. Chapter 4). The 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, evaluations, and 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.

The CFTC OIG maintains an Office of Audits, an Office of Evaluations, and an Office of Investigations and 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, evaluations, investigations, and other activities designed to identify fraud, waste, and abuse in connection with CFTC programs and operations.

Management and Performance Challenges

In accordance with the Reports Consolidation Act of 2000, the OIG identifies the most serious management and performance challenges facing the CFTC and provides a brief assessment of the CFTC's progress in addressing those challenges. The Government Performance and Results Modernization Act of 2010 defines major management challenges as programs or management functions that are vulnerable to waste, fraud, abuse, or mismanagement, and where a performance failure could seriously undermine agency mission objectives. Each challenge is related to the agency's mission and reflects both continuing vulnerabilities and emerging issues. The OIG identified the following top management and performance challenges facing the CFTC for FY 2025:

- *Pending Digital Assets Legislation: The Financial Innovation and Technology for the 21st Century Act (FIT21)*
- *Expiration of Customer Protection Fund Expense Account (Whistleblower Program)*
- *CFTC Headquarters Relocation*
- *Maturing Enterprise Risk Management Practices*
- *Maintaining a Proactive Cybersecurity Posture*

We identified the Commission's major management and performance challenges by recognizing and assessing key themes from OIG audits, evaluations, hotline complaints, investigations, and an internal risk assessment, as well as reports published by external oversight bodies, such as the Office of Personnel Management and the Government Accountability Office.

Pending Digital Assets Legislation: The Financial Innovation and Technology for the 21st Century Act (FIT21)

FIT21 (H.R. 4763, 118th Cong., 2d Session) proposed to amend the Commodity Exchange Act (CEA) to formally define digital assets and digital commodities regulated by the CFTC for the first time. In addition, FIT21 would:

- Establish new categories of CFTC registrants pertaining to digital asset transactions; Provide for CFTC regulation of new registrants;
- Require the CFTC to share certain information regarding digital commodity exchanges with the Board of Governors of the Federal Reserve, the Securities and Exchange Commission, and certain additional federal and State entities;
- Authorize the collection of fees to offset related costs;
- Codify the CFTC's LabCFTC;
- Establish a CFTC-SEC Joint Advisory Committee on Digital Assets; and
- Require certain studies prepared in coordination with the Securities and Exchange Commission

FIT21 passed the House of Representatives but did not become law. During the current administration, relevant Executive Orders have included *Strengthening American Leadership in Digital Financial Technology* (January 23, 2025) and *Establishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile* (March 6, 2025). On March 7, 2025, the first White House Digital Assets Summit took place, with attendees including the current Acting CFTC Chairman and a former CFTC Chairman. The House Financial Services Committee and the House Committee on Agriculture published *A Blueprint for Digital Assets in America* (April 4, 2025).

Expiration of Customer Protection Fund Expense Account (Whistleblower Program)

Section 748 of the Dodd-Frank Act established the CFTC Whistleblower Program and the CFTC Customer Protection Fund ("CPF" or "Fund"), which is available for the payment of awards to eligible whistleblowers and the funding of customer education initiatives. In accordance with statute, the Commission deposits certain collected monetary sanctions into the Fund as long as the balance of the Fund at the time the monetary sanction is collected is less than $100 million, and this applies even where the deposit would cause the balance of the Fund to exceed $100 million.

Following the Dodd-Frank Act, the CFTC established the Whistleblower Office (WBO) and the Office of Customer Education and Outreach (OCEO) and issued regulations. Since issuing its first award in 2014, the CFTC has granted whistleblower awards amounting to approximately $380 million. Those awards are associated with enforcement actions that have resulted in monetary sanctions totaling nearly $3.2 billion. The CFTC issues awards related to the agency's enforcement actions, as well as in connection with related actions brought by other domestic or foreign regulators, if certain conditions are met.

The CPF may be used to pay WBO and OCEO administrative expenses; however, CFTC must prioritize awards over administrative expenses. This prioritization risks depletion of the CPF, forcing a shutdown of the programs. To alleviate this risk, Congress established a CFTC CPF Fund Expenses Account, which consists of up to $10 million transferred by the CFTC from the CPF to a Fund established in the Treasury, with the amounts available "for the sole purpose of" paying WBO and OCEO administrative costs. This funding, established in 2021, was subject to

expiration dates that were extended three times in 2022, with the fund eventually set to expire on September 30, 2024. Proposed legislation would have removed the expiration date and would have raised the cap from $100 million to $300 million; however, it did not pass during the 118th Congress (S.2500). The Full-Year Continuing Appropriations and Extensions Act, 2025, P.L. 119-4 (2025), extended the deadline for the fund to expire to September 30, 2025.

Recent, Current or Ongoing Work in Financial Oversight

24-AU-01 Audit of the CFTC's FY 2024 Annual Financial Report

The objective of this Congressionally mandated audit was to render an opinion on the agency financial report (financial statements) in accordance with GAGAS. The audit was completed by an independent public accountant (IPA) with CFTC OIG Office of Audit oversight. In its audit report the IPA reported:

- the financial statements are presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles;
- CFTC maintained, in all material respects, effective internal control over financial reporting;
- CFTC's financial management systems complied substantially with the requirements of FFMIA; and
- no reportable noncompliance with provisions of laws tested or other matters. The CFTC received a "clean" opinion with no significant issues noted.

24-AU-02 Audit of the CFTC's FY 2024 Customer Protection Fund (CPF)

The objective of this Congressionally mandated audit was to render an opinion on customer protection fund financial statements in accordance with GAGAS. This audit was completed by an IPA with the Office of Audit oversight. In its audit report, the IPA reported that CFTC received a "clean" opinion with no significant issues noted.

2024-AU-05 Audit of CFTC's Enterprise Risk Management (ERM) Program

The objective of this audit was to assess the effectiveness of the CFTC's ERM process with specific attention to governance and internal control integration, and to determine CFTC's ERM program maturity using the Committee of Sponsoring Organizations of the Treadway Commission (COSO) model. In summary, the audit determined that CFTC's ERM program requires substantial enhancements to achieve an acceptable level of maturity to be operational and effective. Specifically, the audit identified three findings related to the lack of proper governance and communication, lack of comprehensive policies and procedures, and lack of sufficient resources and processes for implementation of the program within the organization. In addition, the audit identified 20 recommendations to enhance the risk identification, mitigation, and strategic alignment of the CFTC.

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. Jennifer L. Fain serves as the FDIC Inspector General.

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 deposits; examines and supervises financial institutions for safety and soundness and consumer protection; makes large, complex institutions resolvable; and manages receiverships.

The FDIC insures $10.7 trillion in domestic deposits at about 4,496 institutions and promotes the safety and soundness of these institutions by identifying, monitoring, and addressing risks to which they are exposed. The FDIC is the primary Federal regulator for approximately 2,848 of the insured institutions. The Deposit Insurance Fund (DIF) balance totaled $137.1 billion as of December 31, 2024. Active receiverships as of March 31, 2025, totaled 48, with assets in liquidation of about $27.18 billion.

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 the FDIC's Security Controls over Cloud Computing, a Material Loss Review of Republic First Bank, and the FDIC's Readiness to Resolve Large Regional Banks.

Importantly, and in connection with matters affecting the financial sector, in March 2025, our Office also published its assessment of the Top Management and Performance Challenges Facing the FDIC. This 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, wire fraud, embezzlement, money laundering, cybercrime, currency exchange manipulation, and other crimes involving banks, executives, directors, officials, insiders, and financial professionals. We are also working to detect and investigate cybercrime 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 who have perpetrated 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 201 cases associated with fraud in the CARES Act and ARP programs. We have strongly supported 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 to bring pandemic-related fraudsters to justice.

FDIC OIG Audits, Evaluations, and Reviews

During the 12-month period ending March 31, 2025, the FDIC OIG issued 9 audit and evaluation-related products and made 63 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.

Security Controls for the FDIC's Cloud Computing Environment

Cloud computing offers many potential benefits, including optimizing costs, flexibility, scalability, and enhanced security. It enables organizations to do more with less by eliminating their on-premises infrastructure with the reduction of servers and staff to support that infrastructure. While cloud computing offers many benefits, it does not eliminate the customer's responsibility to manage security risks appropriately. The FDIC continues to expand its cloud presence by migrating its mission essential and mission critical applications into the cloud. The FDIC must ensure that its systems and data within the cloud are secured and that control weaknesses are effectively addressed. Failure to do so could result in damage and harm to FDIC systems and data, hindering its ability to maintain stability and confidence in the nation's financial system.

We engaged Sikich CPA LLC (Sikich) to conduct an audit of security controls for the FDIC's cloud computing environment. The objective of this audit was to assess the effectiveness of

security controls for the FDIC's cloud computing environment. Sikich determined that the FDIC had not effectively implemented security controls in its cloud computing environment in five of nine areas, including Identity and Access Management, Protecting Cloud Secrets, Patch Management, Flaw Remediation, and Audit Logging. Due to the number of findings and similarities among them, Sikich identified six common themes of security weaknesses listed below:

1. Insecure Coding Practices: The FDIC cloud platform teams did not consistently implement secure coding practices.
2. Misconfigured Security Settings: The FDIC cloud platform teams did not consistently configure cloud platform security settings in accordance with cloud service providers and industry best practices.
3. Least Privilege: The FDIC did not consistently provision access to its cloud-based systems in accordance with the principle of least privilege.
4. Outdated Software: Cloud platforms relied on outdated software components.
5. Ineffective Monitoring: The FDIC did not adequately monitor the activity on its cloud-based systems.
6. Cloud Service Provider Vulnerabilities: Cloud service providers were solely responsible for causing certain vulnerabilities and should be responsible for their remediation.

Sikich made 7 formal recommendations and 48 related technical recommendations to improve cloud security controls in the 6 common themes of security weaknesses listed above. The FDIC concurred with all recommendations and plans to complete all corrective actions by December 30, 2026.

Material Loss Review of Republic First Bank

On April 26, 2024, the Pennsylvania Department of Banking and Securities (PA DoBS) closed Republic First Bank and appointed the FDIC as receiver. On May 21, 2024, the FDIC estimated the loss to the DIF to be approximately $667 million.

Under a contract overseen by the OIG, Sikich performed the Material Loss Review. The objectives of the engagement were to (1) determine why the bank's problems resulted in a material loss to the DIF, and (2) evaluate the FDIC's supervision of the bank, including the FDIC's implementation of the Prompt Corrective Action (PCA) requirements of section 38 of the Federal Deposit Insurance Act, and make recommendations for preventing any such loss in the future.

Sikich found that the direct cause of Republic First Bank's failure was its determination that it could no longer hold its "held-to-maturity" debt securities to maturity, requiring the Bank to reclassify them as "available-for-sale" securities. Because of insufficient liquidity, the Bank then further determined it was "more-likely-than-not" that it would have to sell these securities

before the recovery of the amortized cost, thereby requiring the Bank to recognize significant fair value losses in its net income. Once this occurred, the Bank became critically undercapitalized for PCA purposes and was closed by the PA DoBS. Sikich also found that the dysfunctional Board and management team was a significant contributing factor to the Bank's troubled condition, its inability to adjust strategies and address increasing risk, and its eventual failure.

In assessing the FDIC's supervision of the bank, Sikich determined that:

- The FDIC's November 2023 visitation for Republic First Bank lacked documented support for its conclusions related to changes to the Management rating and a proposed FDIC enforcement action; and

- The FDIC's approval of the Bank's use of brokered deposits contributed to an increase in insured deposits of approximately $300 million and that improvements to the FDIC's brokered deposit waiver process are needed to adequately assess risks to the DIF.

Sikich made four recommendations intended to improve the FDIC's supervision processes and help prevent future losses to the DIF. The FDIC concurred with three of the recommendations and partially concurred with the remaining recommendation. The FDIC planned to complete corrective actions by June 30, 2025.

FDIC Readiness to Resolve Large Regional Banks

Readiness to resolve large regional banks is key to the FDIC's mission of maintaining stability and public confidence in the U.S. financial system. In Spring 2023, the FDIC responded to the unanticipated failures of Silicon Valley Bank (SVB), Signature Bank of New York (Signature), and First Republic Bank (First Republic), three of the largest bank failures in FDIC history. The FDIC resolved each bank through a purchase and assumption agreement, facilitated in part by a systemic risk exception for SVB and Signature.

We conducted an evaluation to assess the FDIC's readiness to resolve large regional bank failures under the Federal Deposit Insurance (FDI) Act, prior to the failures of SVB, Signature, and First Republic.

We determined that the FDIC's readiness to resolve large regional banks under the FDI Act was not sufficiently mature to facilitate consistently efficient response efforts in a potential crisis failure environment. We found that at the time of the Spring 2023 failures, the FDIC had not ensured that it fully met its human and technology resource needs or that it sufficiently coordinated resources among its Divisions and Offices. As a result, the FDIC did not satisfy

the readiness activities for planning, training, exercises, evaluation, and monitoring consistent with best practices. The FDIC could have been more effective in demonstrating its readiness to resolve large regional bank failures by:

- completing, communicating, and coordinating the regional resolution framework guidance;
- improving large regional bank resolution plans;
- training key staff on their resolution roles;
- conducting interdivisional exercises to test resolution procedures; and
- periodically evaluating and monitoring large bank resolution readiness.

Improving operational readiness will enhance the FDIC's ability to conduct resolutions in the most efficient and effective manner, reduce strain on staff, and strengthen interdivisional relationships. To that end, we made 11 recommendations to the FDIC to address the findings in our report. The FDIC concurred with all of our recommendations and plans to complete corrective actions by June 30, 2026.

Top Management and Performance Challenges

This year, we issued our Top Management and Performance Challenges report at a time when the Federal Government, including the FDIC, was undergoing significant restructuring and reform that continued to unfold. The pace of change and fluidity regarding the status and composition of the FDIC made it difficult to assess the full impact of these changes on the FDIC and its mission. The Top Challenges that we identified were based on the status, makeup, and processes in place at the FDIC as of March 14, 2025. In such an evolving environment, we acknowledged that the FDIC was likely to undergo significant changes that may impact these identified Top Challenges and the FDIC's response to them. We identified the following eight challenges:

Enhancing Governance: Effective governance allows the FDIC to integrate its Divisions and Offices to ensure that roles, responsibilities, and actions are coordinated and synchronized to address enterprise risks to the FDIC mission. Further, development of effective metrics allows the FDIC Board and senior leaders to understand and measure how FDIC actions and activities progress the FDIC towards programmatic and mission goals and to avoid wasteful spending of the DIF.

Establishing Effective Human Capital Management: With significant staffing changes underway, the FDIC will need to assess its current staff skillsets against its statutory obligations and identify ways to address critical skill gaps. As the FDIC undertakes that assessment, the FDIC should also continue to consider the standards necessary to ensure that the FDIC has an accountable workplace culture.

Ensuring Readiness to Execute Resolution and Receivership Responsibilities: The FDIC should stand ready to execute its resolution and receivership powers to maintain financial stability. The FDIC must not lose sight of its readiness mission as it undertakes the restructuring and reshaping of its staff and processes.

Identifying and Addressing Emerging Financial Sector Risks: Identification of financial risks as they emerge provides time for banks to take corrective action and for the FDIC to implement supervisory actions such as guidance and enforcement actions, as needed. Prior financial crises have shown that recognition of risk once fully manifested in bank financial statements is generally too late for bank management and FDIC supervisory processes to mitigate such risk.

Assessing Operational Resilience in the Financial Sector: It is critical that the FDIC maps the interconnections of banks and their third parties to understand and examine potential operational points of failure and possible cyber intrusion and contagion. Such maps would also assist the FDIC when assessing resolution risks. Currently, there are instances where multiple banks rely on the same third party. An operational issue at one such third party has the potential to affect many banks. Further, the FDIC should have effective processes and staff with required skillsets to assess operational risks and take supervisory actions as needed.

Improving Contract Management: Contracting supports both day-to-day and crisis activities. The FDIC should have appropriate processes and internal controls to ensure that the FDIC receives goods and services it contracted for and that FDIC employees follow these processes and controls to reduce DIF operating expenses. Further, the FDIC should assess and monitor for potential or actual contracting conflicts of interest.

Ensuring IT Security and Scalability: It is paramount for the FDIC to continue to ensure the availability, confidentiality, integrity, and scalability of FDIC systems and data for its day-to-day mission and during crises.

Guarding Against Harmful Scams: Scams that seek to take advantage of consumers are increasing and becoming ever more sophisticated. Scammers attempt to trick individuals into disclosing their banking information, sending money to them, or making unauthorized payments by posing as a legitimate entity such as a bank, or by falsely claiming affiliation with the FDIC or the FDIC OIG. Additionally, consumers may be easily duped by misrepresentations of FDIC insurance and misuse of the FDIC name and logo. A challenge for the FDIC is to be mindful of such schemes, continue to take steps to protect consumers, and take actions to address violations as appropriate.

FDIC OIG Investigations

Our Office is committed to partnerships with other OIGs, the Department of Justice (DOJ), USAOs, and other state and local law enforcement agencies in pursuing criminal acts affecting

banks and in helping to deter fraud, waste, abuse, and misconduct involving 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 and task forces 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, 2025, included the following: 145 indictments; 122 convictions; 115 arrests; and potential monetary recoveries (fines, restitution, asset forfeitures, settlements, special assessments) of more than $3.0 billion.

Among other cases, we continue to investigate Paycheck Protection Program cases of individuals defrauding the Government guaranteed-loan program that was intended to help those most in need during the pandemic crisis. Notably, during the period April 1, 2024 through March 31, 2025, the FDIC OIG's efforts related to the Federal Government's COVID-19 pandemic response resulted in 57 indictments and informations; 34 arrests; and 55 convictions involving fraud in the CARES Act Programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases alone totaled in excess of $217.6 million.

Examples from the past year illustrating the varied nature of our impactful investigations follow.

Former Bank President and CEO of Failed Bank Sentenced

On August 19, 2024, former Heartland Tri-State Bank (HTSB) President and Chief Executive Officer (CEO) Shan Hanes was sentenced to 293 months in prison for his role in embezzling $47.1 million of HTSB funds, that were ultimately lost in a cryptocurrency scheme known as "pig butchering." This scheme led to the failure of HTSB, with a loss to the DIF of $54.2 million, and a complete loss of equity for investors. Hanes was remanded into the custody by the Federal Bureau of Prisons at the conclusion of the hearing. On November 4, 2024, the USAO for the District of Kansas announced that the FBI was able to recover $8 million so that the victims of the fraud would receive financial relief.

On July 28, 2023, HTSB was closed by the Kansas Office of the State Bank Commissioner and the FDIC was subsequently named Receiver. Hanes previously pleaded guilty to one count of embezzlement on May 23, 2024.

Beginning on or about May 30, 2023, and continuing through at least July 7, 2023, Hanes allegedly embezzled funds from HTSB by causing at least 11 wire transfers from the bank to purchase cryptocurrency and to make investments in gold for his own personal benefit. In total, approximately $47.1 million was fraudulently transferred from HTSB. Additionally, in an effort to cover up the scheme, Hanes allegedly stole money from accounts associated with investment clubs, churches, and other programs and accounts for which he had signature authority. Once Hanes had leveraged all available funds, he attempted to disguise the first of many wires to look like an associated transaction related to a U.S. Department of Agriculture loan involving a local farmer.

Source: *FDIC Division of Resolutions and Receiverships.*
Responsible Agencies: *FDIC OIG, FBI, Federal Reserve Board (FRB) OIG, and Federal Housing Finance Agency OIG.*
Prosecuted by *the USAO, District of Kansas.*

Kabbage Agrees to Pay up to $120 Million to Resolve Allegations That It Defrauded the Paycheck Protection Program

On May 13, 2024, it was announced that bankrupt lender Kabbage, Inc. d/b/a KServicing, had agreed to resolve allegations that it knowingly submitted thousands of false claims for loan forgiveness, loan guarantees, and processing fees to the U.S. Small Business Administration (SBA) as part of the Paycheck Protection Program (PPP), in violation of the False Claims Act. Kabbage is now winding down its operations as KServicing Wind Down Corp. after filing for Chapter 11 bankruptcy in the District of Delaware in October 2022. The resolution consists of two separate settlements with KServicing Wind Down Corp., that together provide the United States with an allowed, unsubordinated, general unsecured bankruptcy claim for recovery of up to $120 million. The amount the government will recover on this claim will depend on the ultimate amount of assets available to the bankruptcy estate for distribution to unsecured creditors.

The first settlement, which provides the United States with a claim for recovery of up to $63.2 million, resolves allegations that Kabbage systemically inflated tens of thousands of PPP loans, causing the SBA to guarantee and forgive loans in amounts that exceeded what borrowers were eligible to receive under program rules. As part of the settlement, KServicing Wind Down Corp. admitted and acknowledged that Kabbage double-counted state and local taxes paid by employees in the calculation of gross wages; failed to exclude annual compensation in excess of $100,000 per employee; and improperly calculated payments made by employers for leave and severance. The United States alleged that Kabbage was aware of its errors as early as April 2020, yet Kabbage failed to remedy all incorrect loans that had already been disbursed and continued to approve additional loans with miscalculations. The resolution also provides for Kabbage to receive a $12.5 million credit for payments it previously returned to the SBA during the Department's investigation of this alleged misconduct. Half of the $63.2 million settlement amount is considered restitution, or about $25.4 million.

The second settlement, which provides the United States with a claim for recovery of up to $56.7 million, resolves allegations that Kabbage knowingly failed to implement appropriate fraud controls to comply with its PPP and Bank Secrecy Act/Anti-Money Laundering obligations. In particular, the United States alleges that Kabbage removed underwriting steps from its pre-PPP procedures in order to process a greater number of PPP loan applications and maximize processing fees. The government further alleged that Kabbage knowingly set substandard fraud check thresholds despite knowledge of SBA's concerns that fraudulent borrowers might seek to benefit from the PPP; relied on automated tools that were inadequate in identifying fraud; devoted insufficient personnel to conduct fraud reviews; discouraged its fraud reviewers from requesting information from borrowers to substantiate their loan requests; and submitted to the SBA thousands of PPP loan applications that were fraudulent or highly suspicious for fraud. Half of the $56.7 million settlement amount is considered restitution, or about $28.4 million.

Prior to becoming an SBA approved lender, Kabbage acted as an Agent completing PPP loan applications on behalf of banks and financial institutions throughout the United States. Celtic Bank was Kabbage's primary banking partner which was already a partner in the SBA's 7(a) program and originated Kabbage's small business loans and served as Kabbage's initial intermediary.

Source: *USAO, District of Massachusetts.*
Responsible Agencies: *FDIC OIG, FBI, SBA OIG, FRB OIG, DOJ's Fraud Section, DOJ's Civil Commercial Litigation Branch, and the USAOs for the District of Massachusetts and the Eastern District of Texas.*

Par Funding CEO Sentenced to 186 Months for RICO Conspiracy, Securities Fraud, Obstruction of Justice, Tax Violations, and Related Charges

On March 26, 2025, in the Eastern District of Pennsylvania, Joseph LaForte, 54, of Philadelphia, Pennsylvania, the former Chief Executive Officer (CEO) of Par Funding, was sentenced to 186 months in prison and 3 years of supervised release, to include 12 months of home confinement. LaForte was also ordered to forfeit various assets, including a private jet and an investment account totaling approximately $20 million, along with a $120 million forfeiture money judgment. He was further ordered to pay $314 million in restitution and a $50,000 fine. The former CEO previously pleaded guilty in September 2024 to the Racketeer Influenced and Corrupt Organizations Act (RICO) charge, securities fraud, tax crimes, and perjury. He also pleaded guilty to obstruction of justice for his role in aiding and abetting his brother, James LaForte's, violent assault on one of the Par Funding receivership's Philadelphia attorneys, and to a gun possession charge for firearms found in his former residence during the execution of a search warrant.

On March 13, 2025, in the Eastern District of Pennsylvania, Joseph's brother, James LaForte, 48, of New York, New York, was sentenced to 137 months' imprisonment, followed by 3 years of supervised release to include 12 months' home confinement. In addition, he was

ordered to pay $2,488,645 in restitution, representing the portion of investor proceeds that he illegally diverted from Par Funding's numerous investors. James LaForte pleaded guilty in September 2024 to racketeering conspiracy, securities fraud, and extortionate collection of debt, as well as obstruction of justice, for his violent assault on one of the Par Funding receivership's Philadelphia attorneys, and retaliation, for threatening several government witnesses. In January 2025, the Court found the Par Funding fraud scheme caused an actual fraud loss of approximately $404,000,000, which it reduced to $288,395,088 after factoring in credit for collateral seized from Par Funding by federal authorities when the investigation became public in July 2020 when the Securities and Exchange Commission placed Par Funding in receivership.

Joseph LaForte served as the undisputed leader of a years-long criminal enterprise consisting of his co-defendants and others. The principal purpose of this enterprise was to generate money for its leadership and members, primarily by defrauding the investors in Par Funding, which the enterprise controlled until it was placed in receivership. From at least 2016 through July 2020, Par Funding orchestrated a scheme to raise investor funds through unregistered securities offerings for the cash advance company they controlled, Complete Business Solutions Group, Inc. (CBSG). The defendants raised over $500 million from investors. CBSG made opportunistic loans, some of which charged more than 400 percent interest, to small businesses across the United States. CBSG allegedly used a network of unregistered sales agents and affiliated entities to sell promissory notes to the public while lying to or misleading investors about CBSG/Par Funding's business, how investor funds would be used, and the criminal background and role of its founder, Joseph Laforte.

The fraudulent proceeds were laundered through TD Bank and other financial institutions. In addition, the ill-gotten gains were utilized to obtain mortgage loans and purchase property through TD Bank and other financial institutions in a separate mortgage fraud scheme.

Source: *USAO, Eastern District of Pennsylvania.*
Responsible Agencies: *FDIC OIG, FBI, and Internal Revenue Service-Criminal Investigation (IRS-CI).*
Prosecuted by *the USAO, Eastern District of Pennsylvania.*

TD Bank Sentenced for Bank Secrecy Act and Money Laundering Conspiracy Violations and Agreed to a $1.8B Resolution

On November 7, 2024, TD Bank N.A. (TDBNA), the 10th largest bank in the U.S. and its parent company TD Bank US Holding Company (TDBUSH) (together with TDBNA, TD Bank) were sentenced to 5 years of probation. The judge accepted all the terms of the plea agreement and TDBNA was ordered to pay a $500,000 fine and $400 special assessment. TD BUSH was ordered to pay a special assessment of $800 and was given a credit to the criminal fine in the amount of $500,000 for the special assessment of TDBNA and $5.5 million claw back credit. As part of the plea agreement, TD Bank has agreed to forfeit $452,432,302.00 and pay a criminal fine of $1,434,513,478.40, for a total financial penalty of $1,886,945,780.40. TD Bank has also agreed to retain an independent compliance monitor for 3 years and to remediate and enhance its anti-money laundering (AML) compliance program. TD Bank has

separately reached agreements with the FRB, the Office of the Comptroller of the Currency, and the Financial Crimes Enforcement Network, and the DOJ will credit $123.5 million of the forfeiture toward the FRB's resolution.

Between January 2014 and October 2023, TD Bank had long-term, pervasive, and systemic deficiencies in its U.S. AML policies, procedures, and controls but failed to take appropriate remedial action. Instead, senior executives at TD Bank enforced a budget mandate, referred to internally as a "flat cost paradigm," requiring that TD Bank's budget not increase year-over-year, despite its profits and risk profile increasing significantly over the same period. Although TD Bank maintained elements of an AML program that appeared adequate on paper, fundamental, widespread flaws in its AML program made TD Bank an "easy target" for perpetrators of financial crime.

Over the last decade, TD Bank's federal regulators and TD Bank's own internal audit group repeatedly identified concerns about its transaction monitoring program, a key element of an appropriate AML program necessary to properly detect and report suspicious activities. Nonetheless, from 2014 through 2022, TD Bank's transaction monitoring program remained effectively static, and did not adapt to address known, glaring deficiencies; emerging money laundering risks; or TD Bank's new products and services. For years, TD Bank failed to appropriately fund and staff its AML program, opting to postpone and cancel necessary AML projects prioritizing a "flat cost paradigm" and the "customer experience."

Throughout this time, TD Bank intentionally did not automatically monitor all domestic automated clearinghouse (ACH) transactions, most check activity, and numerous other transaction types, resulting in 92 percent of total transaction volume going unmonitored from January 1, 2018, to April 12, 2024. This amounted to approximately $18.3 trillion of unmonitored transaction activity. TD Bank also added no new transaction monitoring scenarios and made no material changes to existing transaction monitoring scenarios from at least 2014 through late 2022; implemented new products and services, like Zelle, without ensuring appropriate transaction monitoring coverage; failed to meaningfully monitor transactions involving high-risk countries; instructed stores to stop filing internal unusual transaction reports on certain suspicious customers; and permitted more than $5 billion in transactional activity to occur in accounts even after the bank decided to close them.

TD Bank's AML failures made it "convenient" for criminals, in the words of its employees. These failures enabled three money laundering networks to collectively transfer more than $670 million through TD Bank accounts between 2019 and 2023. Between January 2018 and February 2021, one money laundering network processed more than $470 million through the bank via large cash deposits into nominee accounts. The operators of this scheme provided TD Bank employees gift cards worth more than $57,000 to ensure employees would continue to process their transactions. And even though the operators of this scheme were clearly depositing cash well over $10,000 in suspicious transactions, TD Bank employees did not identify the conductor of the transaction in required reports. In a second scheme between March 2021 and March 2023, a high-risk jewelry business moved nearly $120 million

through shell accounts before TD Bank reported the activity. In a third scheme, money laundering networks deposited funds in the U.S. and quickly withdrew those funds using ATMs in Colombia. Five TD Bank employees conspired with this network and issued dozens of ATM cards for the money launderers, ultimately conspiring in the laundering of approximately $39 million. The DOJ has charged over two dozen individuals across these schemes, including two bank insiders. TD Bank's plea agreement requires continued cooperation in ongoing investigations of individuals.

The DOJ reached its resolution with TD Bank based on several factors, including the nature, seriousness, and pervasiveness of the offenses, as a result of which TD Bank became the bank of choice for multiple money laundering organizations and criminal actors and processed hundreds of millions of dollars in money laundering transactions. Although TD Bank did not voluntarily disclose its wrongdoing, it received partial credit for its strong cooperation with the DOJ's investigation and the ongoing remediation of its AML program. TD Bank did not receive full credit for its cooperation because it failed to timely escalate relevant AML concerns to the DOJ during the investigation. Accordingly, the total criminal penalty reflects a 20 percent reduction based on the bank's partial cooperation and remediation.

Source: *Based on a request for assistance from the USAO, District of New Jersey, and IRS-CI.*
Responsible Agencies: *FDIC OIG, IRS-CI, and Drug Enforcement Administration.*
Prosecuted by *the USAO, District of New Jersey, and the Money Laundering and Asset Recovery Section (MLARS) of the DOJ.*

***

View full reports and investigative press releases and learn more about the FDIC OIG at

www.fdicoig.gov

Follow us on X, formerly known as Twitter at FDIC_OIG.

LinkedIn: www.linkedin.com/company/fdicoig

Office of Inspector General
Federal Housing Finance Agency

The Federal Housing Finance Agency (FHFA or Agency) 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, inspections, and compliance reviews of the Agency's programs and operations, as well as criminal investigations into fraud and abuse impacting those programs and operations. Our robust reporting and enforcement efforts protect the interests of the American taxpayers, and keep our stakeholders fully and currently informed of our work.

Overview

The Housing and Economic Recovery Act of 2008 established FHFA in July 2008. FHFA regulates and supervises Fannie Mae and Freddie Mac (the Enterprises) and their affiliate, Common Securitization Solutions, LLC (CSS), as well as the Federal Home Loan Banks (FHLBanks)[2] and the FHLBanks' fiscal agent, the Office of Finance. FHFA is responsible for ensuring the regulated entities operate in a safe and sound manner so that they serve as reliable sources of liquidity and funding for housing finance and community investment. As of December 31, 2024, the Enterprises collectively reported more than $7.7 trillion in assets and the FHLBanks reported almost $1.3 trillion. Since September 2008, FHFA also has served as the Enterprises' conservator.

OIG's Risk-Based Oversight Strategy

FHFA's dual roles as the regulated entities' supervisor and the Enterprises' conservator present unique challenges for OIG. These dual responsibilities put FHFA in a position different from that of other financial regulators, and OIG structures its oversight program to rigorously examine the Agency's exercise of both responsibilities. As part of that oversight, OIG focuses its work on the areas of greatest risk to FHFA and the regulated entities through our audits, evaluations, compliance reviews, inspections, and investigations.

[2] Collectively, the Enterprises, CSS, and the FHLBanks are the "regulated entities." 12 USC § 4502(20).

Management and Performance Challenges

An integral part of OIG's oversight is to identify and assess FHFA's top management and performance challenges and align our work with these challenges. We annually assess and report to the FHFA Director our view of the Agency's most significant management and performance challenges that, if not addressed, could adversely affect FHFA's accomplishment of its mission. Our memorandum identifying FHFA's most significant management and performance challenges for Fiscal Year (FY) 2025 is available on our website.

FHFA's most significant management and performance challenges for FY 2025 are:

- Managing risk in the Enterprises' multifamily lines of business
- Supervising the regulated entities' model risk management
- Managing vulnerability within FHFA's information security programs and at the regulated entities
- Addressing people risk at FHFA and at the regulated entities
- Overseeing the regulated entities' reliance on counterparties and third parties
- Achieving certain supervisory goals for the FHLBank System and member credit risk management

Many of these challenges reiterate themes we identified in prior years.

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. Our body of work published between April 1, 2024, and March 31, 2025, provides important insights across FHFA's programs and operations, including the entities under the Agency's purview.

Enterprises

FHFA's Division of Enterprise Regulation (DER) serves as regulator and supervisor for the Enterprises and their affiliate, CSS. During the relevant period we assessed the effectiveness of DER's supervision of Freddie Mac's multifamily business line. Specifically, in EVL-2025-002, we evaluated DER's efforts to ensure Freddie Mac addressed known risk management deficiencies, including adverse examination findings issued by FHFA. We concluded that DER took supervisory actions to address multifamily risk management deficiencies at Freddie Mac. Nevertheless, the Enterprise's multifamily business continues to operate in market conditions that present challenges, which warrants DER's ongoing attention.

FHLBank System

FHFA also serves as supervisor and regulator of the FHLBank System. Specifically, the Agency's Division of Federal Home Loan Bank Regulation (DBR) is responsible for ensuring the FHLBanks' safe and sound operation. In AUD-2024-008, we determined that DBR provided sufficient oversight of the FHLBanks' Office of Finance's debt issuance and servicing functions. Similarly, in AUD-2025-001, we found that DBR provided sufficient oversight of the FHLBanks' use of market risk modeling to ensure the management of market risk.

During the Spring of 2023, three banks failed, and another voluntarily liquidated, in the largest U.S. bank failures since the 2008 financial crisis. All four were FHLBank members. In EVL-2024-003, we found that DBR examiners shifted their supervisory focus in 2023 to address the shortcomings in the FHLBanks' credit risk management policies and practices that were exposed by the member failures. However, we made four recommendations where DBR could apply lessons learned from that experience. FHFA agreed with our recommendations.

Agency Operations

Our body of work encompasses not only FHFA's oversight of the regulated entities but also the Agency's internal operations. In COM-2025-002, we assessed the Agency's incoming consumer communications and found deficiencies. Specifically, FHFA did not respond to nearly one in five of the consumer communications we tested and was untimely in responding to other communications, among other issues. We issued three recommendations, which the Agency accepted.

We also assessed FHFA's adherence to procedures for reporting certain information about cyber security incidents to the Department of Homeland Security's Computer Emergency Readiness Team. In COM-2024-009, we found that FHFA generally followed its Cyber Incident Reporting Procedures. We offered one recommendation for improvement, which FHFA accepted.

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's investigations are conducted in strict accordance with professional guidelines established by the Attorney General of the United States and also with the Council of the Inspectors General on Integrity and Efficiency'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.

The Office of Investigations is the primary federal law enforcement organization that specializes in deterring and detecting fraud perpetrated against the Enterprises, which collectively held more than $7.7 trillion worth of assets as of December 31, 2024. 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 had almost $1.3 trillion in assets as of December 31, 2024, and, in some instances, cases involving banks that are members of the FHLBanks.

Notable Criminal Cases

Former CEO Sentenced in Multimillion-Dollar Embezzlement Scheme Resulting in a Bank Failure, Kansas

During this reporting period, in the District of Kansas, former Chief Executive Officer (CEO) of Heartland Tri-State Bank Shan Hanes was sentenced to 293 months in prison, three years of supervised release, and was ordered to pay over $55 million in restitution and over $8 million in forfeiture for engaging in a multimillion-dollar embezzlement scheme that caused the failure of Heartland Tri-State, a member bank of the FHLBank of Topeka.

Hanes initiated 11 outgoing wire transfers totaling $47.1 million of Heartland's funds to a cryptocurrency wallet. The funds were then transferred to multiple cryptocurrency accounts controlled by unidentified third parties. The $47.1 million loss caused the failure of Heartland Tri-State and caused bank investors to lose $9 million.

Real Estate Developer and Former Attorney Sentenced to Over a Combined 37 Years in Multimillion-Dollar Embezzlement Conspiracy Resulting in the Failure of a Bank, Illinois

During this reporting period, in the Northern District of Illinois, a real estate developer and former attorney were sentenced for their roles in an embezzlement conspiracy that led to the 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. As a result of OIG's investigation:

- Marek Matczuk was sentenced to 155 months in prison, three years of supervised release, and ordered to pay over $5.9 million in restitution and over $6 million in forfeiture.
- Robert Kowalski was sentenced to 300 months in prison, three years of supervised release, and ordered to pay over $7.5 million in restitution, $83,875 jointly and severally, and over $9 million in forfeiture.

For more than a decade, Matczuk was part of a conspiracy that embezzled millions of dollars in bank funds. The embezzled funds were disguised as purported real estate development loan disbursements to Matczuk and others. Much of the embezzled money was transferred to attorney Robert Kowalski and other individuals outside the bank without all of the required documentation and often without any documentation. Matczuk, Kowalski, and one other conspirator were convicted by federal juries while 10 other defendants have pleaded guilty in connection with this investigation.

Former Bank President Sentenced for Fraud Scheme Resulting in Bank Failure, Nebraska

On August 1, 2024, in the District of Nebraska, Jack Poulsen was sentenced to 18 months in prison, five years supervised release, and ordered to pay $815,000 in restitution for his role in a fraud scheme that contributed to the failure of Ericson State Bank, a member bank of the FHLBank of Topeka.

Poulsen was the bank president from 2010 to 2019 and a Board of Directors (Board) member. He was responsible for overseeing all bank affairs and managing day-to-day operations and for keeping other Board members informed of the bank's financial condition. Poulsen had lending authority but was required to seek approval from the bank's loan committee for any loans exceeding $250,000. He was not allowed to be the loan officer on loans for which he would have a personal conflict of interest, including loans made to parties or entities related to him.

According to court records, in 2012, the bank began a lending relationship with an individual related to Poulsen. This individual and his business entities received numerous loans and opened several accounts with the bank. In 2015, Poulsen began interfering with these insider-related loans and accounts for the purpose of hiding their unsoundness from the Board. These actions included advancing more bank funds on insider-related loans than the approved loan amounts; manipulating data contained in the bank's computer system by advancing payment due dates and loan maturity dates to conceal the past-due status of the insider-related loans from the Board; and advancing loans over the approved note amounts and applying the funds to conceal overdrafts on the insider-related checking accounts from the Board. Poulsen's actions continued until his removal from both positions in September 2019.

Former Bank Senior Vice President Sentenced in Loan Fraud Scheme, Oklahoma

On December 13, 2024, in the Western District of Oklahoma, John Padilla was sentenced to 16 months in prison, three years of supervised release, and ordered to pay over $1 million in restitution for his role in a loan fraud scheme.

According to court records, Padilla, senior vice president and commercial loan officer for BancFirst, an FHLBank member bank, had delegated loan authority for up to $350,000. Padilla recruited borrowers to apply for loans that were under his delegated loan authority. Most of these borrowers were not creditworthy and without Padilla would not have been approved for the loans, and many were Padilla's friends and associates. Padilla explained that he would

purportedly use the loan proceeds to invest in his real estate venture and then pay the borrowers a percentage of the profit. Padilla also assured these borrowers that he would make all the payments toward the outstanding balance on each loan.

Padilla often listed fictitious collateral on these loan applications to secure the loans knowing that the collateral did not exist. Padilla also instructed these borrowers what to represent as the purpose of the loan, even though he received and used most of the loan proceeds almost exclusively to support his personal gambling habit.

Further, Padilla regularly used loan proceeds from unauthorized loans he had approved to make payments toward earlier unauthorized loans, enabling the scheme to continue undetected.

Two Conspirators Sentenced in Mortgage and Short Sale Fraud Scheme, California

On March 31, 2025, in the Eastern District of California, two conspirators were sentenced for their respective roles in a mortgage and short sale fraud scheme.

Jyoteshna Karan was sentenced to 40 months in prison, three years of supervised release, and ordered to pay over $3 million, jointly and severally, and in forfeiture.

Praveen Singh was sentenced to 24 months in prison, three years of supervised release, and ordered to pay over $3 million, jointly and severally, and in forfeiture.

According to court documents, Singh and Karan obtained loans from lenders to purchase real property by making material misrepresentations regarding borrower income, assets, employment status, and intent to occupy the property. After obtaining the property, Singh and Karan allowed the loans to become distressed and then enlisted straw buyers, including relatives, to execute fraudulent short sales. This scheme allowed Singh and Karan to obtain debt relief through the short sales. In some cases, Karan and Singh profited from short sales on other properties where they were not the original purchaser.

Fannie Mae suffered over $1 million in losses because of this scheme.

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

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

Background

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 mortgage insurers in the world, FHA protects lenders against losses when homeowners, multifamily property owners, and healthcare facilities default on their loans. FHA has insured approximately 54.366 million single-family loans since its inception in 1934.[3] FHA reported that in fiscal year (FY) 2024, it served a total of 766,942 forward mortgage borrowers.[4] This included 603,040 purchase mortgages with over 82 percent going to first-time home buyers. In FY 2024, FHA endorsed a total of $231.53 billion in forward mortgages, which was a moderate increase from FY 2023. As of February 2025, FHA's portfolio also included 3,798 insured residential care facility and 82 hospital loans.[5] As of October 2024, FHA had a combined insurance portfolio valued at $1.5 trillion.[6] FHA receives limited congressional funding and is primarily self-funded through mortgage insurance premiums.

Ginnie Mae is a self-financing, U.S. Government corporation within 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 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

[3] https://archives.hud.gov/budget/fy25/2025_CJ_Program_-_FHA.pdf, page 29-1
[4] 2024FHAAnnualReportMMIFund.pdf, pages 5 and 17
[5] https://www.hud.gov/sites/default/files/Housing/documents/FHACommMortPortFebruary2025.pdf, pages 10 and 15
[6] 2024FHAAnnualReportMMIFund.pdf, page 73

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 free up funds that lenders use to originate more loans. In fiscal year 2024, Ginnie Mae issued $423.4 billion in MBSs, pushing the total MBS outstanding to a historic high of $2.64 trillion.[7]

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, including through our Top Management Challenges for FY 2025 report highlighting the following areas most related to the financial sector:

Mitigating Counterparty Risks in Mortgage Programs – FHA and Ginnie Mae must work with outside entities, including property owners, banks, nonbank lenders, and issuers. Each one 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 limit loss to the Federal Government and minimize disruption to the mortgage market.

Managing Fraud Risk and Improper Payments – Fraud poses a significant risk to the integrity of Federal programs and erodes public trust in government. Beyond the monetary loss to taxpayers, fraud against HUD programs reduces HUD's ability to meet the needs of vulnerable communities with critical housing needs. HUD is challenged to develop more robust fraud risk assessments and fraud risk frameworks in its programs and integrate program accountability measures.

In addition, HUD OIG issued an updated list of Priority Open Recommendations for FY 2025. HUD OIG is in close communication with HUD as it attempts to resolve the most significant open recommendations identified by HUD OIG which, if implemented, will have the greatest impact on helping HUD achieve its mission.

HUD OIG tracks HUD's progress in addressing all HUD OIG recommendations, including those designated as priorities, on a Recommendations Dashboard.

[7] Ginnie Mae Annual Report 2024, page 5

HUD OIG Oversight Related to the Financial Sector

For the period April 1, 2024, through March 31, 2025, HUD OIG completed the following key oversight reports related to the financial sector.

Servicers Followed the COVID-19 Foreclosure Moratorium Requirements but Could Have Better Communicated the Requirements to Borrowers

HUD OIG conducted an audit of the FHA, Office of Single-Family Housing's moratorium on foreclosures during the COVID-19 pandemic to determine whether servicers followed the requirements of the moratorium. The review also focused on whether delinquent borrowers were notified that as a condition of the moratorium, foreclosures would be paused if the borrower remained in the home. HUD OIG found that while servicers followed the COVID-19 pandemic foreclosure moratorium requirements, they could have communicated the requirements more effectively to delinquent borrowers who were subject to foreclosure proceedings. Because HUD did not require servicers to notify borrowers directly about the foreclosure moratorium and explain that occupancy would pause the foreclosure process, borrowers may not have realized they were protected from foreclosure by remaining in their homes. As a result, servicers missed an opportunity to inform as many as 25 of 88 borrowers sampled, who vacated their homes. HUD OIG made three recommendations to assist HUD in protecting the FHA fund and borrowers from foreclosure. **(HUD OIG Report, 2024-KC-0002, Office of Single Family Housing)**

HUD's FHA Appraiser Roster is Generally Reliable but Opportunities to Improve Data Management Exist

HUD OIG conducted an audit of HUD's management of its FHA appraiser roster to determine whether the roster was accurate and reliable. The audit found that HUD's FHA appraiser roster was generally reliable; however, HUD could improve its data management by removing ineligible appraisers with expired licenses or disciplinary actions within specified timeframes and better maintaining historical information and supporting documentation. HUD OIG made two recommendations to HUD to improve data management practices for the roster. **(HUD OIG Report, 2024-NY-0001, Office of Single Family Housing)**

HUD Addressed Multifamily Mortgage Application Processing Delays, but Additional Action is Needed to Manage Future Backlogs

HUD OIG audited HUD's Office of Multifamily Housing Programs' efforts to address multifamily mortgage application processing delays. When applications for these loans are delayed, it slows the production and availability of affordable multifamily housing units. During the COVID-19 pandemic, HUD took action to eliminate a backlog of more than 500 applications waiting to be assigned to underwriters for review. HUD OIG did this audit to assess HUD's efforts in receiving and screening applications and assigning them to underwriters. The audit found that HUD took steps to address delays in assigning applications to underwriters, but its methods and systems could be improved to help it manage applications

and future challenges. HUD used several methods to address delays, including implementing (1) a nationwide queue, (2) an application completeness screening, (3) priority application processing, (4) use of contract underwriters, (5) workload sharing, and (6) an option to bypass initial feasibility reviews for certain applications (one-step processing). Although HUD eliminated the nationwide queue in November 2022, it was unable to transition successfully to a state-of-the-art processing platform. As a result, HUD still uses multiple systems, email, and other manual methods to process applications. HUD OIG found that this process creates a future risk that HUD cannot process applications as quickly and effectively as possible. With a more integrated system and a plan for which methods will be used when applications exceed underwriter capacity, HUD can more easily identify, monitor, and address processing delays; evaluate its performance and processes; and manage future challenges, such as fluctuations in application volume. **(HUD OIG Report, 2024-NY-0002, Office of Multifamily Housing Programs)**

Carrington Mortgage Misapplied FHA's Foreclosure Requirements

HUD OIG conducted an audit to determine whether Carrington complied with FHA's requirements for loss mitigation before initiating and continuing foreclosure. The audit found that Carrington did not follow FHA's requirements for more than 18 percent of its foreclosures in 2022. Based on a statistically valid sample drawn from a universe of 7,998 FHA-insured loans totaling $907 million, Carrington did not complete the required loss mitigation activities before initiating or continuing foreclosure for an estimated 1,451 loans. HUD OIG made several recommendations to HUD to help Carrington better service its delinquent FHA-insured loans facing foreclosure that minimized the costs to the borrowers. **(HUD OIG Report, 2025-KC-1002, Single Family Housing)**

MidFirst Bank Misapplied FHA's Foreclosure Requirements

HUD OIG conducted an audit to determine whether MidFirst Bank complied with FHA requirements for loss mitigation before initiating and continuing foreclosure. The audit found that MidFirst Bank did not follow FHA's requirements for more than 14 percent of its foreclosures in 2022. Based on a statistically valid sample drawn from a universe of 7,363 FHA-insured loans totaling $890 million, MidFirst did not complete the required loss mitigation activities before initiating or continuing foreclosure for an estimated 1,038 loans. HUD OIG made several recommendations to HUD to help MidFirst better service its delinquent FHA-insured loans facing foreclosure by minimizing costs to the borrowers while helping them stay in their homes. **(HUD OIG Report, 2025-KC-1001, Single Family Housing)**

CMG Mortgage, Inc., Did Not Have a Sufficient Quality Control Program for FHA-Insured Loans

HUD OIG conducted an audit of CMG Mortgage, Inc., to evaluate its quality control (QC) program for originating and underwriting Single Family FHA-insured loans. The audit found that CMG's QC program for originating and underwriting FHA-insured loans (1) did not select the proper number of loans for review and maintain complete and accurate data to document its loan selection process; (2) did not always complete key review steps and sometimes missed material deficiencies; and (3) did not adequately mitigate and report loan review findings, which included self-reporting loans to HUD when required. HUD OIG made several recommendations to HUD to help ensure that CMG's QC program achieves its intended purpose of protecting HUD and itself from unacceptable risk, guarding against fraud, and facilitating timely and appropriate corrective action. **(HUD OIG Report, 2025-NY-1001, Single Family Housing)**

loanDepot.com Did Not Have a Sufficient Quality Control Program for FHA-Insured Loans

HUD OIG conducted an audit of loanDepot.com to evaluate its QC program for originating and underwriting Single Family FHA-insured loans. The audit found that loanDepot's QC program for originating and underwriting FHA-insured loans was not sufficient. Specifically, loanDepot (1) did not select the proper number of loans for review and maintain complete and accurate data to document its loan selection process; (2) missed material deficiencies; and (3) did not adequately assess, mitigate, and report loan review findings, which included self-reporting loans to HUD when required. These issues occurred because loanDepot had insufficient controls over its QC program. HUD OIG made several recommendations to HUD to help ensure that loanDepot achieves its intended purpose of protecting the FHA insurance fund and lender from unacceptable risk, guarding against fraud, and ensuring timely and appropriate corrective action. **(HUD OIG Report, 2025-NY-1002, Single Family Housing)**

Audit of Government National Mortgage Association's Fiscal Years 2024 and 2023 Financial Statements

HUD OIG contracted with the independent public accounting firm Sikich CPA LLC to audit the financial statements of Ginnie Mae as of and for the years ending September 30, 2024, and 2023, and to provide reports on Ginnie Mae's (1) internal control over financial reporting, and (2) compliance with laws, regulations, contracts, grant agreements, and other matters. The audit found that Ginnie Mae's financial statements as of and for the fiscal year ending September 30, 2024, were presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles; no material weaknesses or significant deficiencies for fiscal year 2024 in internal control over financial reporting, based on limited procedures performed; and no reportable noncompliance for fiscal year 2024 with provisions of applicable laws, regulations, contracts, and grant agreements or other matters. **(HUD OIG Report, 2025- FO-0001, Government National Mortgage Association)**

Audit of FHA's Fiscal Years 2024 and 2023 Financial Statements

HUD OIG contracted with the independent public accounting firm of Sikich CPA LLC to audit the financial statements of FHA as of and for the fiscal years ending September 30, 2024, and 2023, and to provide reports on FHA's (1) internal control over financial reporting, and (2) compliance with laws, regulations, contracts, and grant agreements and other matters. The Audit found that FHA's financial statements as of and for the fiscal year ending September 30, 2024, were presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles; no material weaknesses or significant deficiencies for fiscal year 2024 in internal control over financial reporting, based on limited procedures performed; and no reportable noncompliance for fiscal year 2024 with provisions of applicable laws, regulations, contracts, and grant agreements or other matters. **(HUD OIG Report, 2025-FO-0002, Office of Housing)**

Investigative Activity and Outcomes

HUD OIG also helps protect HUD from counterparty risk by conducting investigations of alleged fraud negatively affecting the FHA insurance funds and securing recoveries. HUD OIG also investigates misconduct involving the FHA loan and Ginnie Mae mortgage-backed securities programs. For the period April 1, 2024, through March 31, 2025, HUD OIG Office of Investigation completed 72 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 over $48 million (criminal, civil, and administrative recoveries). The following are significant investigative cases involving financial fraud:

Putnam County Man Sentenced to Prison for FHA Fraud Scheme

On July 29, 2024, a defendant was convicted at a jury trial for committing false statements. The defendant submitted falsified bank statements to a lender to obtain an FHA-insured mortgage. The defendant was sentenced to 18 months in prison, 3 years of supervised release, and ordered to pay restitution in the amount of $65,302 to HUD.

Loan Originator Convicted in $2.6 Million Mortgage Fraud Scheme

On September 6, 2024, a defendant was convicted at a jury trial for bank fraud. From January 2012 through December 2013, the defendant engaged in a scheme to fraudulently obtain approximately $2.6 million in federally guaranteed mortgage loans in connection with the purchase of 14 properties. The defendant recruited buyers and caused them to make false representations to lenders about, among other things, the source of their down payments and their intention to occupy the properties as their primary residences. The defendant provided or caused others to provide funds to the buyers for use as down payments, knowing that the lenders would be falsely led to believe that the money belonged to the buyers. After closing and

the issuance of the government-insured mortgage loans, the defendant made payments to the buyers – describing them as "grants" – and then pocketed payments from the sellers without notifying the lenders.

James B Nutter & Company to Pay $2.4 Million for Allegedly Causing False Claims for Federal Mortgage Insurance

On September 20, 2024, a former FHA-approved lender agreed to pay $2.4 million to resolve allegations that it violated the False Claims Act and the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 by knowingly underwriting home equity conversion mortgages insured by FHA that did not meet program eligibility requirements. Between January 2007 and December 2010, the defendant knowingly violated FHA underwriting requirements when it allowed inexperienced temporary staff to underwrite FHA-insured loans and submitted loans for FHA insurance with underwriter signatures that were falsified or affixed before all documentation was reviewed as complete by the underwriter.

Three Bay Area Real Estate Professionals Sentenced to Federal Prison for Their Roles in $55 Million Mortgage Fraud Conspiracy

On November 26, 2024, two former realtors and a loan officer were sentenced in U.S. District Court for the Northern District of California for conspiracy to commit wire fraud. Between May 2019 and August 2023, the defendants and co-conspirators obtained more than $55 million in residential mortgage loans for homebuyers in Northern California by creating fraudulent child support income and supporting documentation to qualify buyers for residential mortgage loans. The scheme caused two FHA-approved lenders to repurchase loans that had been sold on the secondary mortgage market at a loss, obligating HUD to pay partial claims to keep its FHA-backed mortgages from foreclosure. The defendants were collectively sentenced to 50 months in prison, 108 months of supervised release, and ordered to pay a total of $906,534.08 in restitution.

Chicago Businessman Sentenced to More Than 17 Years in Prison for Bilking Elderly Homeowners in Reverse Mortgage Scheme

On January 16, 2025, a former licensed loan originator and home repair general contractor was sentenced in U.S. District Court for the Northern District of Illinois for committing a home equity conversion mortgage (HECM) fraud scheme. From approximately 2008 to 2015, the defendant orchestrated a home repair and reverse mortgage loan fraud scheme that targeted financially vulnerable, elderly homeowners by getting them to sign up for repair work that was, in some instances, falsely promised to be funded by the government. The defendant deceived victims into applying for a reverse mortgage on their homes. Other times, the elderly homeowners would be informed they were obtaining a reverse mortgage, and the defendant would convince them to sign over the entirety of their loan proceeds but then never completed the promised work. The defendant pocketed more than $6 million in loan proceeds

and, in most cases, never performed substantive repairs. The defendant was sentenced to 17 years in prison, five years of supervised release, and ordered to pay more than $2.7 million in restitution.

Additional Investigative Cases Related to the Financial Sector

- Third Mortgage Professional Pleads Guilty to Mortgage Fraud Scheme (May 20, 2024)
- Real Estate Professional Pleads Guilty to $55 Million Mortgage Fraud Conspiracy (August 7, 2024)
- Real Estate Executive Sentenced for Conspiracy To Falsify Financial Statements (September 19, 2024)
- Illinois Man Sentenced in Scheme to Fraudulently Obtain Over $800K in Mortgages (January 17, 2025)
- Brooklyn Business Owner Convicted of Multi-Million Dollar Real Estate Fraud Scheme (November 22, 2024)

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

Under the IG Act, the OIG conducts independent audits, investigations, and other activities and keeps the NCUA Board and the Congress informed of our 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, which could relate to the broader financial sector:

- Managing Interest Rate Risk
- Managing Credit and Liquidity Risks
- Cybersecurity - Protecting Systems and Data
- Risks Posed by Third-Party Service Providers
- Implementation of Artificial Intelligence

We also issued several audit reports that could relate to the broader financial sector, including an audit assessing the NCUA's Bank Secrecy Act (BSA) program. The audit determined that the NCUA could improve the BSA examination steps within its Modern Examination and Risk Identification Tool examination system to ensure examiners complete and document all necessary steps during examinations; its reporting process to the Financial Crimes Enforcement Network by documenting and communicating any revised agreements between the agencies through agency policy and updating the data reports it uses for reporting to reduce or eliminate the need for manual reconciliation; and its BSA Enforcement Manual to ensure it contains current guidance and communicates information consistent with other agencies' policies.

A second audit that could relate to the broader financial sector was our audit of the NCUA's revised process to charter new federal credit unions. Our audit found that the NCUA should implement automated systems for the chartering process to streamline and enhance the efficiency of the chartering process; the deferral process for charter applications needed to be described on the NCUA website, including the number of times the NCUA may defer an application before denying it for insufficient information; and that the NCUA Board and management needed an established internal process to set expectations when handling charter applicants inquires.

A third audit assessed the NCUA's compliance with its examiner-in-charge rotation policy and procedures and determined that, in general, the NCUA rotated examiners-in-charge. However, we identified instances where the NCUA did not comply with its rotation limits policy. In addition, we determined supervisory examiners did not create any written approved exceptions to the rotation policy during our audit scope period.

A fourth audit assessed the NCUA's Central Liquidity Facility (CLF). The CLF is a mixed ownership government corporation within the NCUA owned by its member credit unions and managed by the NCUA Board. The CLF's purpose is to improve general financial stability by providing member credit unions with a source of loans to meet their liquidity needs. The audit determined the NCUA operated the CLF in accordance with applicable laws and substantially complied with regulations and its own policies and procedures. We determined the annual stock adjustment done by the CLF was not entirely done in accordance with regulations as the CLF did not receive payments for adjustments to member capital stock subscriptions no later than March 31. However, we determined the financial impact of these payments not being received by March 31 was de minimis. We also determined the CLF was being used by credit unions as evidenced by its growth in members. Although we made no recommendations in our report, we suggested that management determine whether they want to pursue any action to extend the due date beyond March 31 for the annual stock adjustment payments to the CLF.

Finally, we are participating in a CIGFO working group to conduct an audit of FSOC's designation of nonbank financial companies. The audit objectives are to assess the sufficiency of the new guidance to effectively respond to financial stability threats under Section 113 of the Dodd-Frank Act; the extent that FSOC members were engaged in the development of the new guidance considering such factors as lessons learned and any identified barriers from earlier guidance; and the impact on the nonbank designation process as a result of the new guidance compared to the preexisting guidance and process.

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

The U.S. Securities and Exchange Commission (SEC 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. On November 29, 2022, the SEC issued its Strategic Plan: Fiscal Years (FY) 2022-2026, identifying its goals to (1) Protect the investing public against fraud, manipulation, and misconduct; (2) Develop and implement a robust regulatory framework that keeps pace with evolving markets, business models, and technologies; and (3) Support 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, and the Public Company Accounting Oversight 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 accomplishes its mission through six main divisions—Corporation Finance, Economic and Risk Analysis, Enforcement, Examinations, Investment Management, and Trading and

Markets—and 26 functional offices[8]. The Agency's headquarters are in Washington, DC, and it has 10 regional offices located throughout the country. As of March 2025, the SEC employed 4,732 full-time equivalent employees[9].

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 10 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 the SEC Employee Suggestion Program in September 2010. Under this program, the OIG receives, reviews, and considers 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. The OIG also recommends appropriate action with respect to such suggestions or allegations.

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.

[8] Including the Office of Inspector General.
[9] As of March 31, the SEC was processing applications received for the OPM Deferred Resignation Program, and an agency buyout/early retirement offer.

Completed Work, April 1, 2024-March 31, 2025

Evaluation of the SEC Division of Examinations' Oversight of Broker-Dealer Examinations

The SEC conducts examinations of market participants, including broker-dealers, to protect investors, ensure market integrity, and support responsible capital formation. Between fiscal years 2020 and 2023, the SEC's Division of Examinations (Division or EXAMS) completed 1,352 broker-dealer examinations, with over 90 percent conducted by the Division's Broker-Dealer and Exchange examination program (BDX). Using risk-based strategies, examinations improve compliance, prevent fraud, monitor risk, and inform policy. We conducted this evaluation to assess whether EXAMS was effectively overseeing its broker-dealer examinations. Specifically, we sought to determine whether EXAMS (1) effectively used risk-based strategies in the selection and scoping of broker-dealer examinations; (2) performed and documented broker-dealer examinations in accordance with applicable policies and procedures; and (3) monitored and assessed results of examinations to enhance oversight of broker-dealer compliance and accurately measure EXAMS' performance.

With its limited resources, EXAMS requires planning and risk assessment processes to identify entities and industry activities that pose a higher risk and to plan and scope broker-dealer examinations accordingly. However, BDX's broker-dealer examination metrics and planning appear too focused on numerical targets, and managers and staff could better document and monitor risk information in planning and scoping activities.

For example, we surveyed SEC managers and staff involved in broker-dealer examinations and about 45 percent of survey respondents agreed or strongly agreed that the quality and/or scope of broker-dealer examinations is negatively impacted in an effort to meet numerical targets. Further, the BDX records we reviewed did not always demonstrate that BDX management and examiners considered risk assessment data or other risk and priority areas when selecting exam candidates and scoping examinations.

This occurred because BDX (1) lacks program goals and objectives to help provide direction for more comprehensive planning, risk assessment, and monitoring; and (2) did not establish formal program-specific metrics or engage in the type of meaningful performance measurement and evaluation activities described in recognized leading practices. As a result, EXAMS may be unintentionally promoting practices that do not align with its stated risk-based approach. For example, we observed frequent limited scope broker-dealer examinations and waivers for important asset verification procedures. Focusing on limited scope areas and waiving asset verification may be suitable and appropriate depending on the circumstances. However, because EXAMS does not comprehensively monitor its use of limited scope examinations, asset verification waivers, or generally whether completed examinations aligned with identified program risks, it is not evident whether broker-dealer examinations are adequately covering high-risk entities and industry activities as intended.

We also reviewed a sample of 121 broker-dealer examinations and concluded that EXAMS generally complied with policies, procedures, and controls for performing and documenting

examinations and key decisions. However, we identified areas for potential improvement related to internal controls and examination processes. For example, some information related to examination scope and risk ratings assigned to regulated entities was inconsistent, incomplete, or inaccurate as EXAMS either did not implement or could further improve relevant internal procedures and guidance. Improved examination information would further help EXAMS evaluate program performance, make informed decisions, and address the aforementioned issues with BDX's broker-dealer examination planning and performance measurement.

We issued our final report addressing these topics on September 23, 2024, and made six recommendations to further strengthen EXAMS' oversight of its broker-dealer examinations and ensure those examinations fully support the SEC's mission. Management concurred with our recommendations. The report is available on our website at https://www.sec.gov/files/bdx-evaluation-public-rpt-583.pdf.

Audit of the SEC's Controls for Safeguarding Consolidated Audit Trail Data

The consolidated audit trail (CAT) tracks all activity in national market system securities throughout the U.S. markets. The CAT centralizes information about all orders throughout their life cycle and identifies the broker-dealers handling them. The SEC does not own or operate the CAT, but authorized staff and contractors can access and share CAT data to perform a variety of regulatory functions. Inadequate safeguards would pose a greater risk to the Commission and/or outside parties and could hinder the agency's ability to meet its regulatory and oversight responsibilities.

We conducted this audit to assess whether the SEC's information security controls for safeguarding CAT data within the SEC's environment complied with key government-wide standards.

The SEC implemented several Federal security controls to protect CAT data, along with additional policy-based safeguards that allow staff to access, download, and share CAT data as needed for their regulatory work. However, the agency, among other technical control weaknesses, did not implement measures to proactively detect and prevent the external release of CAT data during the period we reviewed or regularly monitor the policy-based safeguards to ensure user compliance.

During our audit, the risks of unauthorized disclosure and misuse of CAT data were elevated. Recent agency action has reduced these risks. For example, in September 2024 as part of its adoption of zero-trust cybersecurity principles, the SEC implemented automated safeguards for CAT data that prevent unauthorized external sharing of the data. Further, in February 2025, the Commission eliminated the requirement for the CAT to collect identifying information for U.S. natural person customers. We recommended additional steps to strengthen the SEC's oversight and monitoring of its CAT usage and to define the agency's new technical controls. For example,

these steps include:

- Defining the scope, processes, and frequency for the SEC's periodic CAT data usage reviews to identify, analyze, and respond to risks related to the agency's access, use, extraction, and sharing of CAT data;
- Increasing the frequency of monitoring the SEC's user access lists to ensure only authorized users have access to CAT data, user access matches approved authorizations, and user access is disabled in a timely manner once access is no longer need; and
- Finalizing responsibility for the SEC's regular monitoring of safeguards.

We issued our final report addressing these topics on March 31, 2025, and made five recommendations to strengthen the SEC's oversight and monitoring of its CAT usage and to define the agency's new technical controls. Management concurred with our recommendations. The report is available on our website at https://www.sec.gov/files/additional-oversight-monitoring-secs-cat-usage-needed-rpt-585.pdf.

Ongoing Work as of March 31, 2025

Audit of Aspects of the SEC's Rulemaking Process and Related Internal Controls

The SEC OIG has initiated an audit to assess aspects of the SEC's rulemaking process and related internal controls. The overall objective of the audit is to review the SEC's processes for (1) giving interested persons an opportunity to participate in rulemaking; and (2) assessing and documenting the impact(s) of proposed rules on competition, efficiency, and capital formation. We will also review agency actions to ensure staff with sufficient and appropriate skills, experience, and expertise are involved in formulating and reviewing proposed rules.

We expect to issue a report during the next six months.

Audit of the Division of Corporation Finance's Disclosure Operations

We have initiated an audit to assess whether the Division of Corporation Finance's Disclosure Review Program (1) concentrated its resources on critical disclosures by implementing a risk-based process for selecting and reviewing filers' periodic reports and transactional filings, and (2) met its statutory requirements for reviewing filers' financial statements within the most recent three-year period. The audit scope will include Disclosure Review Program reviews completed in FY 2023 and FY 2024.

We expect a report will be issued within the next six months.

Audit of the Division of Investment Management's Disclosure Review and Accounting Office Operations

We have initiated an audit to assess the Division of Investment Management's Disclosure Review and Accounting Office operations. Specifically, we will determine whether the Office (1) effectively

employed risk-based processes when selecting reviewable filings to review; (2) reviewed all filers at least triennially, as required by the Sarbanes-Oxley Act of 2002 (SOX); and (3) followed its disclosure review process for reviewable filings and SOX reviews, to include ensuring appropriate supervisory reviews, timely submission of comments, and an effective process for identifying inconsistencies in comments. The audit scope period will include reviewable filings from FY 2024 and SOX reviews from FY 2022 through FY 2024.

We expect a report will be issued in FY 2026.

Investigative Accomplishments

The SEC OIG Office of Investigations, OIG's law enforcement component, investigates allegations of criminal, civil, and administrative misconduct relating to SEC programs, operations, and personnel. The office pursues allegations of waste, fraud, and abuse in agency programs and activities as well as other corruption, violations of law or regulation, or serious misconduct by those involved in agency programs and operations.

Our investigative priorities focus on misconduct impacting the SEC's operational integrity; involving public corruption related to the SEC; or implicating major fraud associated with SEC programs, operations, and personnel. We work closely with other CIGFO investigative offices and law enforcement counterparts outside CIGFO to hold bad actors accountable or exonerate those falsely accused of wrongdoing.

Select Recent Financial Sector and Related Investigative Results

***Alabama man was sentenced in hack of SEC X account that spiked the value of Bitcoin*.**
In May, an Alabama man was sentenced to 14 months in prison for his role in a conspiracy that hacked into the SEC's X account and published fraudulent posts in the name of the then-SEC Chairman, to manipulate the value of Bitcoin.

***Federal investigation led to the indictment of seven individuals on securities fraud charges and government seizures of approximately $214 million*.**
Seven individuals were indicted on criminal charges as part of a federal investigation that disrupted an alleged "pump-and-dump" investment fraud scheme and resulted in government seizures of approximately $214 million. From November 2024 to February 2025, the defendants engaged in misleading promotion and coordinated trading of shares of a company incorporated in the Cayman Islands that purported to provide educational services in China. The scheme allegedly involved individuals in China posing as U.S.-based investment advisors on social media and messaging platforms and falsely promising significant returns from investments in the company. The misleading promotion and coordinated trading caused the stock price to artificially rise, at which point the defendants sold thousands of shares and made millions of dollars in profits, the indictment states. The stock price ultimately decreased significantly, at the expense of other investors, some of whom lost almost the entirety of their investment.

Federal jury convicted a Georgia man for conspiracy to commit fraud

On March 7, 2025, following a three-day trial in the United States District Court for the Eastern District of Tennessee, a jury convicted a Georgia man of conspiracy to commit mail and wire fraud, mail fraud, and wire fraud. The evidence presented at trial showed that the man participated in a scheme to defraud elderly victims. Evidence presented showed, among other things, that he and others worked to steal money from individuals intending to invest their money.

California immigration lawyer was extradited from the Kyrgyz Republic to face charges of large-scale visa fraud

In March 2025, a California woman was extradited from the Kyrgyz Republic to the United States; the first extradition from the Kyrgyz Republic to the United States. Federal criminal charges were filed in a 14-count indictment alleging she and a coconspirator committed visa fraud and related crimes to obtain immigration benefits for more than 100 foreign investors through the government's employment-based immigration visa program.

South Carolina man pleaded guilty to $13M Ponzi scheme and cyber stalking

In February 2025, a South Carolina man pleaded guilty to operating a multimillion-dollar Ponzi scheme and to stalking two social media content creators. Through multiple LLCs, he made false representations to investors by offering promissory notes that projected annual returns of 12 percent. The man paid previous investors with new investor monies because his investment product was not generating returns lulling investors into believing the product was successful, when, in fact, he was spending investor money to maintain a lavish lifestyle that included supporting female social media content creators by paying them thousands of dollars each month.

Mastermind of multimillion-dollar penny-stock scam indicted for fraud and obstruction

A federal grand jury in the District of Columbia indicted a Michigan man with defrauding investors — leading to millions of dollars in investor losses — as well as obstructing a Securities and Exchange Commission (SEC) proceeding by destroying evidence. The man allegedly organized a scheme to defraud investors in the publicly traded securities of a corporation, in which he ran the day-to-day operations, by making false and misleading statements to the public in an effort to artificially inflate the share price of, and demand for, the stock. He allegedly used an alias to promote the corporation on an investor message board and provided the false and misleading impression that he was not affiliated with the entity and was an independent investor. He later allegedly sold nearly one billion shares that he covertly acquired and then caused himself or entities under his control to receive at least $2.5 million from the sale of the shares. After learning of an SEC investigation into he allegedly deleted the contents of at least one email account used to conduct corporation business.

View full reports

and investigative press releases and learn more about the SEC OIG at

www.sec.gov/office-inspector-general

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). OCC supervises approximately 1,040 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) 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 headquartered in Washington, DC and is comprised of four components: (1) Office of Audit, (2) Office of Investigations, (3) Office of Counsel, and (4) Office of Management.

Treasury OIG has oversight responsibility for OCC, which supervises approximately 751 national banks, 240 federal savings associations, and 49 federal branches and agencies of foreign banks. The total assets under OCC's supervision are $16.0 trillion.[10] 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 (OFR), (2) the Federal Insurance Office (FIO), (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 the Coronavirus Disease 2019 (COVID-19). Since March 2020, more than $650 billion of financial assistance, overseen by

[10] Office of the Comptroller of the Currency, *2024 Annual Report* (December 2024), p. 24

Treasury OIG, has been authorized by Congress. Treasury established the Office of Recovery Programs (ORP), which was renamed the Office of Capital Access (OCA) on November 2, 2023, 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 of the Treasury (herein "Treasury" or "the Department"). In a memorandum to the Secretary dated October 15, 2024, the Acting Inspector General reported four management and performance challenges that were directed towards financial regulation and economic recovery. Those challenges are discussed below and include: Ongoing Management of COVID-19 Pandemic Relief Programs; Cyber Threats; Anti-Money Laundering/Terrorist Financing and Bank Secrecy Act Enforcement; and Crypto and Digital Assets.

Challenge 1: Ongoing Management of COVID-19 Pandemic Relief Programs

While the national emergency declaration for the COVID-19 pandemic ended in May 2023, Treasury's responsibilities and workloads remain vastly expanded. Treasury needs to ensure these programs meet the economic needs and fiscal requirements of their respective constituencies responsibly. Specifically, Treasury is responsible for certain economic relief provisions in the *Coronavirus Aid, Relief, and Economic Security Act*[11] (CARES Act), the *Consolidated Appropriations Act, 2021*[12] (CAA, 2021), the *American Rescue Plan Act of 2021,*[13] and the *Consolidated Appropriations Act, 2023*[14] (CAA, 2023). In all, Treasury was tasked with disbursing over $650 billion in aid to more than 30,000 recipients, including state, local, territorial, and tribal government entities. As such, the Department established OCA to implement and manage most of Treasury's COVID-19 pandemic programs.

The Treasury pandemic programs under Treasury OIG oversight consist of:

- Coronavirus Relief Fund (CRF)
- Air Carrier Payroll Support Programs (PSPs)
- Emergency Rental Assistance Programs (ERA1 and ERA2)

[11] Public Law 116-136 (March 27, 2020)
[12] Public Law 116-260 (December 27, 2020)
[13] Public Law 117-2 (March 11, 2021
[14] Public Law 117-328 (December 29, 2022)

- Homeowner Assistance Fund
- The Coronavirus State Fiscal Recovery Fund and the Coronavirus Local Fiscal Recovery Fund
- Coronavirus Capital Projects Fund (CPF)
- Local Assistance and Tribal Consistency Fund
- State Small Business Credit Initiative
- Emergency Capital Investment Program (ECIP)
- Community Development Financial Institutions Equitable Recovery Program

There are numerous challenges faced by Treasury in the management of these programs. Over the past year, turnover in OCA personnel and limited budgetary resources have resulted in operational weaknesses. Specifically, there has been a delay in carrying out certain required program functions, a lack of timely follow-through on implementing corrective action in response to Government Accountability Office (GAO) and Treasury OIG findings, and delays in responding to OIG requests. Taken together these deficiencies, if not corrected, may jeopardize the integrity of the operational effectiveness and efficiency, and compliance with regulations and guidance, for hundreds of billions of dollars of pandemic programs under Treasury's purview.

Treasury OIG recognizes that Treasury was initially challenged by resource and personnel constraints in standing up, in a short period of time, the multiple programs authorized by Congress in the various pandemic statutes. Further, Treasury OIG also recognizes that there have been changes in the leadership and the structure of OCA. That said, these challenges and events do not relieve Treasury from its ongoing responsibility to ensure Congress and the American taxpayer that the pandemic funds entrusted to Treasury were, and are, being used prudently and properly.

A few examples of concerns noted follow.

- Single Audit Act[15] Report Follow-up – As part of the implementation of the multiple pandemic programs, Treasury is responsible to issue management decisions related to *Single Audit Act* (Single Audit) findings for a large number of financial assistance awardees (grantees) in compliance with the Office of Management and Budget's (OMB) Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance).[16] Among those responsibilities is the requirement to issue these management decisions on Single Audit findings timely (i.e., within 6 months). Although mostly late, in calendar years 2023 and 2024 Treasury has made some progress in issuing management decisions. However, Treasury is still behind the number

[15] Public Law 104-156 (July 5, 1996) The Single Audit Act of 1984, as amended in 1996, requires entities who expend Federal funds in excess of $750,000 to obtain an annual audit of those Federal funds. It was enacted for the purpose of promoting sound financial management, including effective internal controls, with respect to Federal awards administered by non-Federal entities and to establish uniform requirements for audits.
[16] Uniform Guidance, 2 C.F.R. § 200, Subpart F, Audit Requirements.

of management decisions required and has yet to determine which grantees have failed to file or are late in filing Single Audit reports. This is a basic program responsibility.

- ERA1 Closeout Reports – The period of performance for ERA1 grantees ended in December 2022. After repeated requests from OIG since July 2023, OCA provided preliminary closeout data, in September 2024, for 619 out of 698 grantees. Final closeout reports for all grantees are critical because previously reported data by grantees to Treasury were determined by both OCA and OIG to be incomplete. In addition, this data is used by OIG to review thousands of ERA hotline complaints for identification of improper payments and fraud.

- The ERA and PSP programs have been identified as susceptible to significant improper payments.[17] OCA has been informed of the high risk of improper payments and other issues with these programs in multiple reports from GAO and OIG and meetings with OIG over several years but has yet to take sufficient corrective actions to fully address the issues. Treasury's inaction increases the risk of significant improper payments within these programs and potential non-compliance with applicable laws and regulations.

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 2023 high-risk list published biennially.[18] 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, or when serious flaws are discovered in software or systems that increase potential risk of information compromise.

Threat actors frequently probe trusted connections for weaknesses to exploit vulnerable networks or systems and 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

[17] Improper payments are payments that should not have been made, were made in incorrect amount, or were made to an ineligible recipient and are a long-standing and significant problem in the Federal government. As of May 2024, the estimated improper payments for both programs totaled over $200 million.
[18] GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas* (GAO-23-106203: April 20, 2023).

information sharing, federal agencies are better prepared to thwart potential attacks to the cyber infrastructure of the Federal Government and the financial sector.

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, compromise of supply chains (both hardware and software), frequently used in combination to maximize attack effectiveness. Increasingly, artificial intelligence (AI) is being used to support attacks, from generating realistic looking phishing emails with minimal effort to creating programs to exploit vulnerabilities. Additionally, Treasury must remain cognizant of the increased risk profile a remote workforce presents, as it 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, and denial of service attacks upon a network or service can disrupt operations and prevent remote workers from performing their duties.

There is continuing concern over foreign adversaries creating and exploiting vulnerabilities in the Nation's supply chain for information and communication technology and services. 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. On May 8, 2024, this EO was extended again for 1 year.[19] 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. The Department 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.

Furthermore, EO 14028*, Improving the Nation's Cybersecurity*, issued on May 12, 2021, calls for federal agencies to update existing plans to prioritize resources for adoption and use of cloud technology and to adopt a zero-trust architecture,[20] among other things. To achieve the goals outlined in EO 14028, OMB issued M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*[21] to provide the strategy for achieving a zero-trust architecture, and require agencies to meet specific cybersecurity standards and objectives by the end of fiscal

[19] *Notice on the Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain* (May 8, 2024).
[20] Zero-trust architecture is a method of designing a system in which all actions are presumed dangerous until reasonably proven otherwise, thereby reducing the chance of a successful attack causing further damage.
[21] OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022), (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf)

year 2024. OMB also issued M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*[22] to use only software that complies with secure software development standards. As mentioned above, Treasury management must be mindful that the efforts to secure Treasury's supply chain may hamper cloud adoption and the implementation of zero-trust architecture. In response to our fiscal year 2023 memorandum, Treasury reported progress towards implementing a zero-trust architecture by accelerating efforts to bring systems into compliance with federal mandates related to multi-factor authentication, encryption of data-at-rest, and encryption of data in-transit.

We continue to remind the Department that, in addition to Treasury's own networks and systems, management must be cognizant of, and mitigate, the risks posed by attacks made against other federal and non-federal agencies and Treasury contractors and subcontractors. Threats and risks to third parties' networks and systems also pose risks to Treasury's networks and systems, due to interconnections with other federal, state, and local agencies, and service providers to conduct its business. Management must continue thoughtful awareness of the wide threat environment and exercise due care evaluating and authorizing such internetwork connections and verify that third parties comply with federal policies and standards including any guidance issued to address new and/or expanded threats and risks. Management is also challenged with ensuring that critical data and information maintained by third-party service providers are properly protected.

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. 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.[23] In 2018, GAO reported that the extent of adoption of the NIST framework by critical infrastructure sectors was unknown since agencies were not measuring framework implementation.[24] With respect to Treasury, GAO 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 2020, GAO recommended that Treasury track the content and progress of sector-wide cyber risk mitigation efforts and prioritize their completion according to sector goals and priorities in the sector-specific plan. Additionally, Treasury should update the financial services

[22] OMB M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022), (https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf)
[23] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, February 12, 2014; superseded by Version 1.1; April 16, 2018)
[24] GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption* (GAO-18-211; February 18, 2018)

sector-specific plan to include specific metrics for measuring the progress of risk mitigation efforts and information on the sector's ongoing and planned risk mitigation efforts.[25] However, as of April 2024, GAO reported Treasury needed to finalize steps to track the financial sector's risk mitigation efforts, and to prioritize the completion of efforts according to sector-wide goals and priorities. Treasury was planning to update the financial services sector-specific plan and was working on developing sector-specific cyber performance goals. Lastly, Treasury reported to GAO that it did not believe it would be beneficial to update the sector-specific plan until the Department of Homeland Security completes its updates to the national plan and provides guidance on sector-specific plans.[26] Additionally, Treasury reported that it contributed to the development of the Cross Sector Cyber Performance Goals, with significant input from the financial sector and independent regulators. Treasury also noted that they were developing an effort focused on the benefits and challenges related to cybersecurity in the financial services sector, stemming from increased use of AI.

Last year, the Department reported that it continues to focus on network defense efforts for its High Value Assets,[27] which includes an increased emphasis on risk/vulnerability assessments as well as accelerated compliance with logging, encryption, and multi-factor authentication requirements. They also reported continued advocation for financial sector entities to participate in the Cybersecurity and Infrastructure Security Agency's Cyber Hygiene Vulnerability Scanning to receive timely notifications of vulnerable internet-facing systems. While addressing increases in cyber threats, Treasury will need to continue to balance cybersecurity demands while maintaining and modernizing Information Technology systems.

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

The Office of Terrorism and Financial Intelligence (TFI) remains 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. Additionally, criminals and other bad actors evolve and continue to develop 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 a variety of targeted financial measures to include designations and economic sanctions. TFI has significantly increased sanctions against Russia related to its actions against Ukraine and its other malign activities. TFI's counter-terrorism designations disrupt the financial networks that support terrorist organizations. Other TFI tools, such as

[25] GAO, Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts (GAO-20-631; September 17, 2020)
[26] GAO, Priority Open Recommendations: Department of the Treasury (GAO-24-107324; June 5, 2024)
[27] 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.'s national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety.

diplomatic and private sector engagement, regulatory oversight, and intelligence analysis, also play an important role. Disrupting terrorist financing depends on a whole-of-government approach and requires collaboration and coordination within Treasury, other federal agencies, the private sector, and international partners.

Collaboration and coordination are key to successfully identifying and disrupting illicit 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 Treasury's critical mission and its role to carry out U.S. policy, Treasury OIG continues to consider anti-money laundering and combating terrorist financing programs and operations as inherently high-risk.

Data privacy, security, and information sharing are challenges for the Financial Crimes Enforcement Network (FinCEN), which has experienced unauthorized disclosures of *Bank Secrecy Act* (BSA) information.[28] FinCEN is required to maintain a 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 unauthorized disclosures 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 administer a secure database as required by the *Corporate Transparency Act.*[29] This Act requires certain businesses to submit information about their beneficial owners such as legal name, date of birth, and address. That information may be shared with governmental authorities and financial institutions. FinCEN implemented the database in January 2024 and will need to securely store tens of millions of reports containing beneficial ownership information.

The Office of Intelligence and Analysis, as a member of the Intelligence Community, is required to take steps to adopt AI to improve intelligence collection and analysis.[30] The office appointed a Chief Artificial Intelligence Officer responsible for overseeing and coordinating efforts relating to AI, including the integration of acquisition, technology, human capital, and financial management aspects necessary for the adoption of AI solutions. However, various barriers, such as a lack of Office of the Director of National Intelligence guidance and Treasury's Office of Intelligence Analysis resources, as well as necessary updates to the information technology infrastructure have negatively affected their ability to take further steps to adopt AI.

TFI and its components have a wide range of responsibilities in combatting terrorists, criminals, and bad actors. Thus, it is critical that TFI has the resources and tools needed to stay ahead of sophisticated terrorists' financial networks and criminal money laundering schemes.

[28] Public Law 91-508 (October 26, 1970)
[29] Public Law 116-283 (January 1, 2021)
[30] Public Law 117-263 (December 23, 2022)

Challenge 4: Crypto and Digital Assets

Interest in, and use of, digital assets, including cryptocurrencies, and stablecoins has increased rapidly over the past decade. Multiple jurisdictions are progressing with central bank digital currency[31] research and pilots which may be based on distributed ledger technology (DLT).[32] Experimentation with DLT continues, with numerous projects at various stages of proof-of-concept development. As of September 2024, the crypto-asset market reached a combined market capitalization of over $2 trillion, up from approximately $14 billion in late 2016 but down from $3 trillion in November 2021.[33]

Decentralized finance (DeFi) platforms increased total value locked (TVL)[34] during 2024, commensurate with overall growth in crypto market capitalization.[35] In April 2023, Treasury published a risk assessment on DeFi in which Treasury explored how illicit actors are abusing DeFi services as well as the vulnerabilities unique to DeFi services.[36] Treasury made several recommendations in the report, including strengthening existing supervisory and enforcement functions to increase and harmonize compliance with regulatory requirements including those under the BSA such as the Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) program rule obligations.

While Treasury supports responsible innovation and the potential benefits of digital assets, the Financial Stability Oversight Council (FSOC)[37] reported that many crypto-asset firms may be acting outside of, or out of compliance with, applicable law(s) and may also lack sufficient risk governance and control frameworks. This increases the potential for fraud, illicit finance, sanctions evasion, operational failures, liquidity and maturity mismatches, and risk to investors and consumers, as well as contagion within the crypto-asset market.[38] Insufficient oversight or regulatory safeguards could create opportunities for illicit actors, such as cyber actors,

[31] A central bank digital currency or CBDC is generally defined as a digital liability of a central bank that is widely available to the general public. A central bank is a national bank that provides financial and banking services for its country's government and commercial banking system, as well as implementing the government's monetary policy and issuing currency.
[32] Distributed ledger technology is a decentralized record of ownership of digital assets.
[33] Cryptocurrency Prices, Charts, and Crypto Market Cap, accessed September 9, 2024.
[34] TVL is an industry reported metric that is the amount of user funds deposited or "locked" in a DeFi service. TVL is used as a measure to gauge the size of the DeFi market or the degree of adoption or acceptance by users.
[35] There is currently no generally accepted definition of DeFi, even among industry participants. There is also no consensus on what characteristics would make a product, service, arrangement or activity "decentralized." The term broadly refers to virtual asset protocols and services that purport to allow for some form of automated peer-to-peer transactions.
[36] Treasury Report, *Illicit Finance Risk Assessment of Decentralized Finance* (April 2023)
[37] FSOC was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act (P.L. 111-203). FSOC is charged with identifying risks to the nation's financial stability, promoting market discipline, and responding to emerging threats to the stability of the U.S. financial system. It is a collaborative body chaired by the Secretary of the Treasury.
[38] FSOC 2023 Annual Report, page 42.

ransomware cybercriminals, drug traffickers, and scammers who may be using digital assets and DeFi services to transfer and launder their illicit proceeds. The lack of consensus, standards, and practices among crypto industry participants regarding AML/CFT regulations as applied to digital assets or DeFi services exacerbate these issues.

Volatility in the crypto-asset market also poses risks to the traditional financial system. Financial institutions that partner with or provide traditional banking products and services to crypto-asset market participants may be impacted by this volatility. In 2023, in response to significant crypto-asset market volatility in 2022 (known as the "crypto winter"), the federal banking agencies, including the OCC, issued two joint statements highlighting risks to banks involved with crypto-assets and crypto-asset participants. Shortly following the publication of these statements, in the Spring of 2023, residual risks adjacent to the 2022 "crypto winter" contributed to the failure of Silvergate, Silicon Valley, and Signature banks (e.g., liquidity and asset/liability risk management, concentration risk management).

Several Treasury offices, including the OCC's Office of Financial Technology continue to engage with digital asset industry stakeholders, including crypto-asset industry participants, and the agency's supervised institutions to understand developments and interest in the space, educate examiners and staff, and collaborate with other Treasury offices and federal agencies.

Taken together, the growth and continued interest in digital assets and DeFi services demands that the Department adopts a holistic approach to understanding the risks and opportunities these technologies present both within and outside the established financial system.

Completed and In-Progress Work on Financial Oversight

Audit of Treasury's Soundness of Investment Decisions for Participation in the Emergency Capital Investment Program

We initiated an audit to determine if Treasury accurately allocated investments under the ECIP, to comply with applicable laws, regulations and policies and procedures. We found Treasury accurately allocated investments under the ECIP, in accordance with the CAA, 2021, and ECIP policies and procedures. Furthermore, Treasury incorporated internal controls throughout their application review and decision-making process in accordance with GAO's Standards for Internal Control in the Federal Government (Green Book).

Treasury received 212 ECIP applications from banks, Bank Holding Companies, Savings and Loans Holding Companies, and credit unions by the established September 1, 2021, deadline. From the 212 total applications, we reviewed a sample of 52 and determined that Treasury complied with the CAA, 2021, for investment decisions made under ECIP. Specifically, Treasury established and followed a 12-step ECIP application review and decision-making process to evaluate applicants and allocate ECIP investments. Accordingly, we did not make any recommendations in this report. (OIG-24-036)

Audit of Treasury's Soundness of Investment Decisions for Participation in the ECIP

We initiated an audit to assess the Community Development Financial Institutions (CDFI) Fund's award process for ensuring the accuracy of the CDFI Equitable Recovery Program (ERP) payments and the design of the post-award administration over recipient monitoring in compliance with applicable laws, regulations, and policies and procedures. We found that the CDFI Fund documented the CDFI ERP award determination process across multiple standard operating procedures (SOPs), consistent with GAO's Green Book. The CDFI Fund also accurately calculated CDFI ERP awards and administered them in accordance with the CAA, 2021 and OMB's Uniform Guidance Part 200. For applicants deemed ineligible to receive a CDFI ERP award, the CDFI Fund reviewed and documented applicants' ineligibility in accordance with the requirements in the Notice of Funds Availability and in compliance with internal policies and procedures.

Additionally, the CDFI Fund designed and implemented the CDFI ERP post-award administration process, as well as developed post-award monitoring SOPs and the CDFI ERP Assistance Agreement, in compliance with the CAA, 2021, Uniform Guidance, and GAO Green Book. Furthermore, the CDFI Fund established: (1) procedures for evaluating CDFI ERP annual compliance reports; (2) a noncompliance process; and (3) a process for closing CDFI ERP awards. Accordingly, we did not make any recommendations in our report. (OIG-24-037)

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.

Corrective Action Verification 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 Treasury OIG 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 OFR's implementation of its workforce reshaping efforts and its compliance with applicable laws, regulations, policies, and procedures.

Review of Financial Crimes Enforcement Network Beneficial Ownership Information Reporting (In Progress)
We will (1) summarize external comments and complaints and any related completed investigations conducted by the OIG related to FinCEN's collection of Beneficial Ownership Information (BOI); and (2) provide recommendations, in coordination with FinCEN, to improve BOI reporting processes to ensure the information reported to FinCEN is accurate, complete, and highly useful.

Treasury's Implementation of the Coronavirus Economic Relief for Transportations Services (CERTS) Program (In Progress)
We initiated an audit to assess Treasury's implementation activities to include the establishment of policies, procedures, and other terms and conditions of financial assistance under the CERTS Program.

Treasury's Implementation of the Coronavirus State and Local Fiscal Recovery Funds (In Progress)
We initiated an audit to assess Treasury's implementation activities, including the establishment of policies, procedures, and processes for making payments to eligible recipients, and the terms and conditions for receiving financial assistance under the Coronavirus State and Local Fiscal Recovery Fund. As part of our audit, we will review Treasury's policies and procedures to monitor recipients' uses of funds.

Treasury's Implementation of the Coronavirus Capital Projects Fund (In Progress)
We initiated an audit to assess Treasury's implementation activities to include the establishment of policies, procedures, and processes for making funds available to eligible recipients, and the terms and conditions for receiving financial assistance under the CPF. As part of this audit, we will review Treasury's policies and procedures to monitor recipients' uses of funds.

Treasury's Implementation of the Local Assistance and Tribal Consistency Fund (In Progress)
We initiated an audit to assess Treasury's implementation activities, including establishing policies, procedures, and processes for making funds available to eligible recipients, and the terms and conditions for receiving financial assistance under the Local Assistance Tribal Consistency Fund. As part of this audit, we will review Treasury's policies and procedures to monitor recipients' uses of fund.

Treasury's Closing and Funding Process for ECIP Participants (In-Progress)
We initiated an audit to assess Treasury's closing and funding process for ensuring the accuracy of ECIP investments in compliance with applicable laws, regulations, and policies and procedures.

CDFI's Compliance Monitoring of the CDFI Rapid Response Program (In-Progress)
We initiated an audit to assess the operating effectiveness of the CDFI Fund's compliance monitoring process, including noncompliance procedures and enforcement actions, performed on the CDFI Rapid Response Program.

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 the 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.[39] As appropriate, OIG auditors also make recommendations for preventing any such loss in the future.

From 2007 through March 2025, FDIC and other banking regulators closed 554 banks and federal savings associations. One hundred and forty-five (145) of these were Treasury-regulated financial institutions. Of the 145 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. We initiated one non-material loss review of the failure of the First National Bank of Lindsay, in Lindsay, Oklahoma which was closed on October 18, 2024.

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,

[39] 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.

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

Allegations of Misuse of Bank Customer Data and Violation of Contract Terms by OCC Contractor Substantiated

On December 11, 2024, the OIG completed its report of investigation for a joint case with the Board of Governors of the Federal Reserve System (the Board) OIG initiated upon receiving a complaint from the OCC alleging an OCC contractor misused bank customer data and violated terms of contracts with the OCC. The investigation discovered the contractor violated material OCC and Board contract provisions by improperly using anonymized credit card information received pursuant to OCC and Board contracts for commercial analysis products. Furthermore, the investigation found the prohibited use of OCC and Board bank data resulted in inaccurate and synthetic analyses which the contractor misrepresented in the sale of commercial products to its clients. On March 11, 2024, following the OIG's investigation and findings, the contractor entered a $37 million settlement with the U.S. Department of Justice, Civil Division and the U.S. Attorney's Office (USAO) for the Eastern District of Virginia, Civil Division for covered conduct under the Financial Institutions Reform, Recovery and Enforcement Act and False Claim Act.

Seven Subjects Sentenced for Conspiracy and Prohibition of Illegal Gambling Business

On December 17, 2024, the OIG completed its report of investigation for a joint IRS Criminal Investigation Division investigation into seven identified subjects who conspired to defraud the Department of the Treasury by operating multiple illegal gambling businesses and not reporting the proceeds to the IRS. The subjects were using OCC regulated banks to facilitate the laundering of their illegal proceeds and to evade the payment of Federal taxes. All subjects were sentenced to a total of 36 years' and 2 months' incarceration, 21 years' probation, and over $15.5 million in fines and restitution with an additional $1.46 million attained through forfeiture. The USAO for the Northern District of Ohio prosecuted the case.

Two Subjects, Including One Who Posed as a Lawyer, Sentenced for Fraud Conspiracy in Connection with Fraudulent Debt Elimination Scheme

On March 7, 2025, the OIG completed its report of investigation regarding allegations that two identified subjects conducted fraudulent in-person trainings purporting to educate victim-debtors on how to discharge consumer debt using a special bank account number that could be found on the back of their social security cards and birth certificates. The subjects were

sentenced to serve a total of 34 years' incarceration and ordered to pay $3.2 million of restitution. The USAO for the District of Maryland prosecuted the case.

Seven Subjects Sentenced for Access Device Fraud, Money Laundering, Conspiracy and Identity Theft

On December 10, 2024, the OIG completed its report of investigation regarding a joint Federal Bureau of Investigation, U.S. Department of Homeland Security, and U.S. Postal Inspection Service investigation into seven identified subjects that conspired to conduct a variety of telephone scams, including impersonation of Treasury employees, leading to fraudulently obtained funds being laundered through Wal-Mart and Sam's Club gift cards. Over 400 individuals fell victim to the frauds. All seven subjects were sentenced to a total of 9 years' and 10 months' incarceration, 20 years' probation, and $198,979.19 in restitution. The USAO for the Eastern District of Virginia prosecuted the case.

Four Subjects Sentenced for Dealing in Counterfeit Obligations, Delay and Destruction of Mail, and Bank Fraud

On January 31, 2025, the OIG completed its report of investigation for a joint investigation involving the United States Postal Service OIG; the Social Security Administration OIG; and the United States Postal Inspection Service. Initiated upon notification from the IRS Criminal Investigation Division alleging that altered Treasury checks were negotiated near Chicago, Illinois. The identified subjects defrauded financial institutions by stealing Treasury checks from the mail, altering them, and negotiating the altered checks for cash. All four subjects were sentenced to a total of 4 years' incarceration, 12 years' probation, and $179,930 in restitution and fines. The USAO for the Northern District of Illinois and the Office of the Illinois Attorney General prosecuted this case.

Jamaican Citizen Sentenced for Operating Fraudulent Debt Relief Websites

On February 21, 2025, OIG completed its investigation regarding the operation of a series of fraudulent debt relief websites. On September 19, 2024, a Jamaican citizen was sentenced to 36 months incarceration and ordered to pay $62,394 in restitution to over 50 victims of a consumer debt relief scam. Between 2016 and 2018, the subject operated a series of websites promising consumer debt relief under the American Recovery and Reinvestment Act of 2008 in exchange for payments of a portion of the debt relief. The USAO in Washington DC, along with the Department of Justice Computer Crimes and Intellectual Property Section, prosecuted this case.

Maryland Resident Sentenced to 24 Months in Mortgage Fraud Scheme

During this reporting period, the subject of a Treasury OIG and Fairfax County Police Department investigation was sentenced to 24 months' incarceration, 36 months of supervised release, $183,000 in restitution, and a $100 special assessment for bank fraud. The subject

devised a scheme to defraud a mortgage lender into agreeing to a short sale, or pre-foreclosure sale, of a residential property in Alexandria, Virginia that was pending foreclosure for non-payment of the mortgage. The subject and the nominee owner received the proceeds of the fraudulent sale which was used to pay off the remaining loan balance and purchase a new property in Ft. Washington, Maryland. The subject also forfeited $276,000 of the proceeds of the offense prior to sentencing. The USAO for the Eastern District of Virginia prosecuted the case.

Allegations of Emergency Rental Assistance Fraud Substantiated

On April 15, 2024, Treasury OIG completed its report of investigation based on receipt of a complaint alleging that one individual submitted three false tenant applications and one fraudulent landlord application to obtain $101,000 in California COVID-19 Rent Relief funds from the ERA program. The investigation revealed the subject filed a fraudulent landlord application and took over the true landlord's ERA account to erroneously obtain ERA funds for himself and three fake tenants totaling $101,000. The investigation was presented to the California Office of the Attorney General and was subsequently declined due to lack of prosecutorial resources and higher priority investigations. This case was presented to the USAO for the Northern District of California, who declined prosecution due to lack of prosecutorial resources and higher priority investigations.

Civil Settlement Obtained for Contractors that Failed to Meet Cybersecurity Requirements Regarding the Emergency Rental Assistance Program

On May 13, 2024, two contractors agreed to pay a total of $11 million in civil settlements for failing to abide by requirements of New York's ERA program. The ERA contract required specific cybersecurity requirements, and the contractors admitted they had failed to properly meet the requirements. The USAO for the Northern District of New York and Department of Justice Civil Division negotiated the settlement.

PRAC Subject Sentenced for Theft of Government Funds After Falsifying Economic Injury and Disaster Loan and Paycheck Protection Program Loan Applications

On April 26, 2024, a subject in a Pandemic Response Accountability Committee (PRAC) Task Force investigation was sentenced to 36 months' probation, with four months' home confinement, and $200,000 in restitution. The subject applied for and received one Economic Injury and Disaster Loan (EIDL), and two Paycheck Protection Program (PPP) loans, while debarred from receiving federal contracts. The subject attested on each PPP and EIDL application that they were not barred from receiving federal contracts. The USAO for the Eastern District of Virginia prosecuted the case.

Coronavirus Relief Fund, Paycheck Protection Program, and Economic Injury and Disaster Loan Fraud Substantiated

On August 29, 2024, Treasury OIG completed its report of investigation for a joint case with the Federal Bureau of Investigation regarding CRF fraud against the Department of Economic Development, Louisville, KY. Specifically, the investigation revealed three subjects conspired to submit fraudulent documentation to obtain CRF funding for businesses they owned during the COVID-19 pandemic. The subjects also received funding from the Small Business Administration's PPP and EIDL program, both totaling over $200,000. This matter was presented and declined by the USAO for the Western District of Kentucky and the USAO for the Eastern District of Kentucky, citing the loss amount being below threshold and venue concerns.

Appendix A:
Council of Inspectors General on Financial Oversight Presidential Transition Handbook (Updated)

Council of Inspectors General on Financial Oversight

Presidential Transition Handbook

December 2024

Council of Inspectors General on Financial Oversight

MISSION

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act)* established the Council of Inspectors General on Financial Oversight (CIGFO) to provide oversight of the Financial Stability Oversight Council's (FSOC) operations and suggest measures to improve financial oversight.

* Public Law 111-203 (July 21, 2010).

Executive Summary

Introduction to CIGFO

In the aftermath of the 2008 financial crisis, Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) "to promote the financial stability of the United States by improving accountability and transparency in the financial system, to end 'too big to fail', to protect the American taxpayer by ending bailouts, to protect consumers from abusive financial services practices, and for other purposes."

The Dodd-Frank Act created both the Financial Stability Oversight Council (FSOC or Council) and the Council of Inspectors General on Financial Oversight (CIGFO). CIGFO comprises eight Inspectors General (IG) responsible for oversight of agencies and programs in the financial sector.[1] CIGFO 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.

The Dodd-Frank Act 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 IG offices to conduct these reviews of FSOC operations.

In addition to CIGFO's oversight activities, it performs monitoring activities and shares financial regulatory information among the member IGs, which enhances each IG's knowledge and insight about specific issues related to current and future work. For example, during its quarterly meetings, CIGFO members discussed recent cyberattacks on financial institutions and turmoil in the banking sector, as well as legislative activities that could impact the financial regulatory system.

Transition Issues Relating to CIGFO

Once leadership of FSOC and its member agencies are appointed, it is important for CIGFO and FSOC's leadership to have regular and candid communications. Regular communications will enable CIGFO to inform FSOC leadership about ongoing work, the results of completed work, and the status of any open recommendations from CIGFO working group reports.

The transition team should review the July 2024, *Annual Report of the Council of Inspectors General on Financial Oversight*, as this document consolidates each IGs concerns and recommendations with a focus on issues that may apply to the broader financial sector.

[1] When CIGFO was created it was originally comprised of nine IGs. However, during the past year, the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) ended its operations as the last remaining investment made by Treasury through the Troubled Asset Relief Program was repaid, thereby ending the program.

Dodd-Frank Act, FSOC, and Role of CIGFO

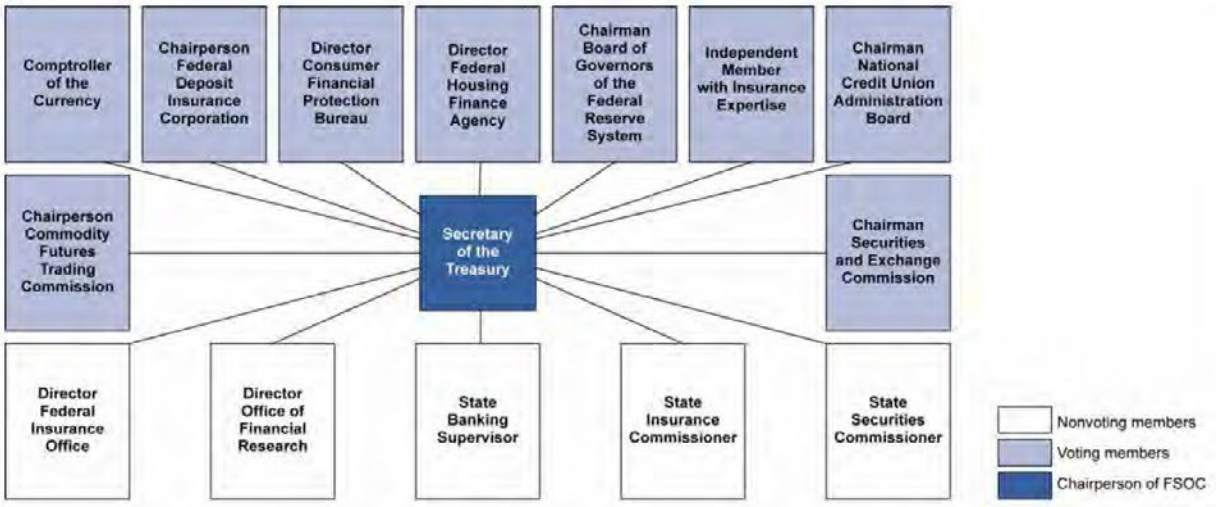
Dodd-Frank Act, FSOC, and Role of CIGFO

Dodd-Frank Act and FSOC

In July 2010, the Dodd-Frank Act was signed into law and created a new regulatory and resolution framework designed to promote the financial stability of the United States. The Dodd-Frank Act is comprehensive in scope, providing for significant changes to the structure of federal financial regulation and substantive requirements that apply to a broad range of market participants, including public companies that are not financial institutions. Among other measures, the Dodd-Frank Act included corporate governance and executive compensation reforms, new registration requirements for hedge fund and private equity fund advisers, heightened regulation of over-the-counter derivatives and asset-backed securities, and new rules for credit rating agencies. The Dodd-Frank Act also mandated significant changes to the authority of the Board of Governors of the Federal Reserve System and the Securities and Exchange Commission as well as enhanced oversight and regulation of banks and non-bank financial institutions. Finally, the Dodd-Frank Act established the Consumer Financial Protection Bureau as a new federal agency to regulate the offering and provision of consumer financial products and services under various consumer financial protection laws.

The Dodd-Frank Act created FSOC which is comprised of ten voting members and five nonvoting members (see Figure 1). Chaired by the Secretary of the Department of the Treasury (Treasury), FSOC is charged with identifying risks to the financial stability of the United States; promoting market discipline; and responding to emerging threats to the stability of the U.S. financial system.

Figure 1: FSOC Membership



Source: GAO 12-886, Financial Stability – New Council and Research Office Should Strengthen Accountability and Transparency of Decisions, September 2012

Role and Authorities of CIGFO

The Dodd-Frank Act also created CIGFO, which is comprised of the IGs of the major federal government Financial-Sector Regulatory Organizations, 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 the FSOC.

CIGFO is chaired by the IG of Treasury and its members include the IGs of the Federal Deposit Insurance Corporation, the Commodity Futures Trading Commission, the Department of Housing and Urban Development, the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau, the Federal Housing Finance Agency, the National Credit Union Administration, and the Securities and Exchange Commission. CIGFO members oversee one or more Financial-Sector Regulatory Organizations, as shown in Figure 2.

Figure 2: CIGFO Membership & Oversight Responsibilities

CIGFO MEMBERSHIP	OVERSIGHT OF FINANCIAL-SECTOR REGULATORY ORGANIZATIONS
Department of the Treasury (Chair)	Department of the Treasury Office of the Comptroller of the Currency
Federal Deposit Insurance Corporation	Federal Deposit Insurance Corporation
Commodity Futures Trading Commission	Commodity Futures Trading Commission
Department of Housing and Urban Development	Department of Housing and Urban Development
Board of Governors of the Federal Reserve System and Consumer Financial Protection Bureau	• Board of Governors of the Federal Reserve System • Consumer Financial Protection Bureau
Federal Housing Finance Agency	Federal Housing Finance Agency
National Credit Union Administration	National Credit Union Administration
Securities and Exchange Commission	Securities and Exchange Commission

Source: CIGFO's Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations (July 2019).

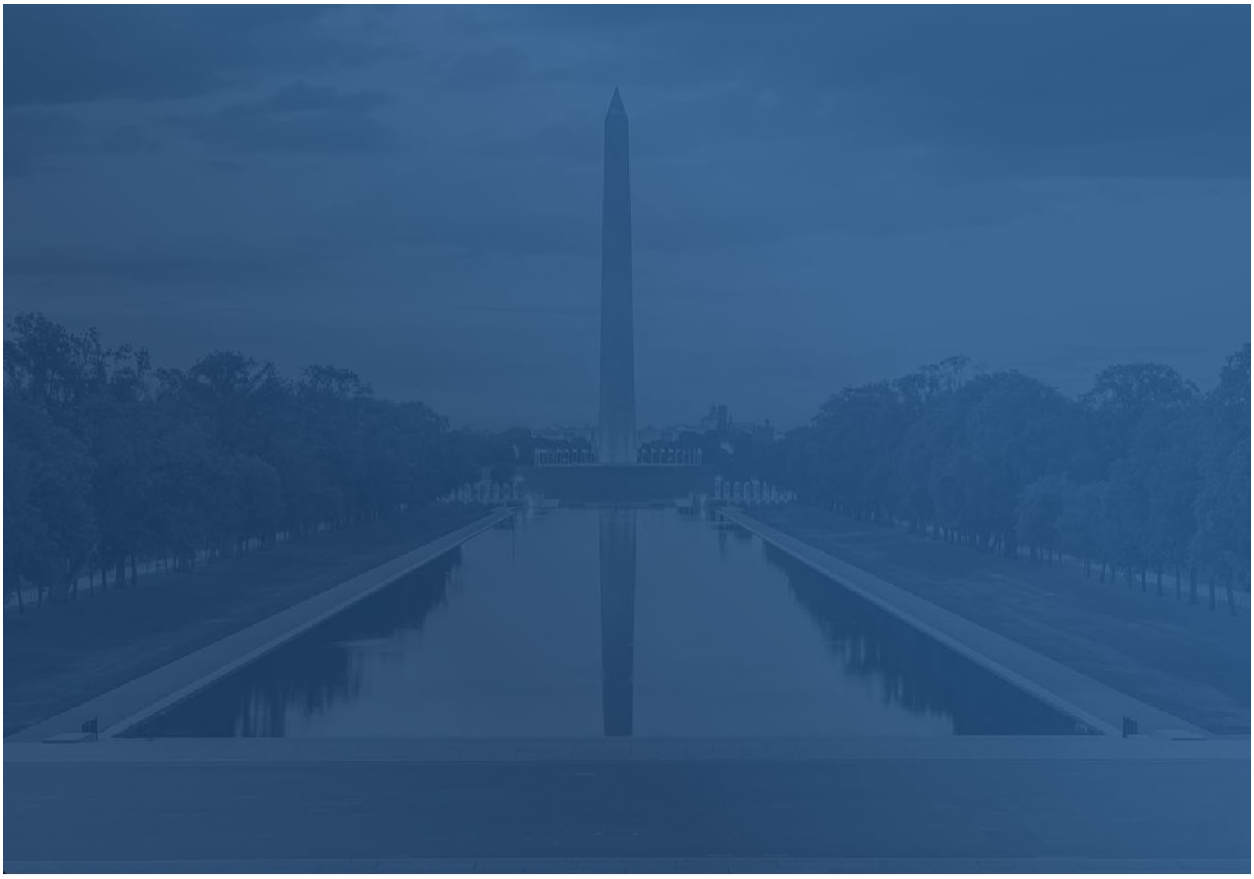
CIGFO provides an opportunity to leverage the expertise and experience of its IG members, who bring unique independent perspectives to the table on both joint projects and individual efforts.

The Dodd-Frank Act assigns CIGFO the following duties:

- Meet not less than once each quarter to facilitate the sharing of information and to discuss the ongoing work of each IG who is a member of CIGFO as it applies to the broader financial sector and ways to improve financial oversight.

- Submit annually to Congress and FSOC a report highlighting the concerns and recommendations of each IG, with a focus on issues that may apply to the broader financial sector, and a summary of general observations of CIGFO, with a focus on measures that should be taken to improve financial oversight.

In addition, the Dodd-Frank Act authorizes CIGFO to convene working groups to evaluate the effectiveness and internal operations of the FSOC and it directs CIGFO to submit reports to FSOC and to Congress on these evaluations.



CIGFO Independence

CIGFO Independence

IGs, and by extension, CIGFO, must perform their audits, investigations, evaluations, and special reviews objectively and independently from the agency.

Several key provisions of the Inspector General Act of 1978, as amended (IG Act),[2] seek to ensure IG independence, in both reality and appearance. For example, according to the IG Act, an agency head may not prevent the IG from initiating, carrying out, or completing any audit or investigation, except for in very limited circumstances.

Moreover, IGs report only to the agency head or in certain instances, the officer next in rank below the agency head. To ensure IG access to relevant information, the IG Act requires IGs to report to their agency heads "without delay" the circumstances of any unreasonable refusal of their information requests. In regards to FSOC, CIGFO reports to its chair, the Treasury Secretary and its members.

[2] 5 U.S.C. Chapter 4

CIGFO Reports and Process

CIGFO Reports and Process

CIGFO Working Group Projects

Since 2011, CIGFO has established numerous working groups, comprised of staff from the CIGFO member IG offices, to conduct reviews of FSOC operations. CIGFO relies on these working groups to fulfill its mission as outlined in the Dodd-Frank Act. To learn more about CIGFO and to review each of the reports mentioned below and others, visit our website: Council of Inspectors General on Financial Oversight.

In Progress Working Group Project – *FSOC's Designation of Nonbank Financial Companies*

Section 113 of the Dodd-Frank Act gives FSOC the authority to designate a nonbank financial company for heightened supervision by the Board of Governors of the Federal Reserve System if it determines that the company could pose a threat to the financial stability of the United States. In November 2023, FSOC issued new interpretive guidance with an effective date of January 16, 2024, that details FSOC's process to make such designations. This working group project will assess (1) the sufficiency of the new guidance to effectively respond to financial stability threats as authorized under Section 113 of the Dodd-Frank Act; (2) the extent that the FSOC members were engaged in the development of the new guidance considering such factors as lessons learned and any identified barriers from earlier guidance; and (3) the impact on the nonbank designation process as a result of the new guidance compared to prior guidance and processes. This report is expected to be issued in the fall of 2025.

Recent Working Group Projects

CIGFO Guidance in Preparing for and Managing Crises *(CIGFO-2022-01; June 2022)*

CIGFO convened a working group to compile forward-looking guidance for FSOC and its members to consider in preparing for and managing a crisis. The guidance is a compilation of lessons learned drawn from the experiences of federal agencies during prior crises and any learned during the COVID-19 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. The guidance did not assess the degree to which the FSOC member agencies employ any of the actions or activities discussed. Rather, the purpose of this guidance is to compile information and activities that agencies and CIGFO Offices of Inspector General (OIG) 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. The working group did not make any recommendations to FSOC.

CIGFO Audit of the FSOC's Efforts to Address Climate-Related Financial Risk *(CIGFO-2023-001; August 2023)*

CIGFO convened a working group to perform an audit to assess FSOC's response to Executive Order (EO) 14030, *Climate-Related Financial Risk*. CIGFO concluded that FSOC's actions were consistent with the policy, objectives, and directives set forth in EO 14030. Additionally, FSOC engaged with the member agencies to assess climate-related financial risk and implemented an effective process to develop its *Report on Climate-Related Financial Risk*. CIGFO determined that the FSOC Report satisfactorily met the requirements set forth in EO 14030. Finally, FSOC established a means to facilitate ongoing coordination and information sharing among its member agencies on climate-related financial risk. While we made no recommendations in this report, we encouraged FSOC, through the newly established Climate-Related Financial Risk Committee, to consider member agency suggestions and feedback to enhance the assessment and sharing of climate-related financial risk data and information.

CIGFO Annual Reports

The Dodd-Frank Act mandates that CIGFO submit to FSOC and Congress an annual report that summarizes the general observations of CIGFO based on the views expressed by each IG with a focus on measures that should be taken to improve financial oversight. Each IG who is a member of CIGFO has a section within the annual report with exclusive editorial control to highlight the concerns and recommendations from ongoing and completed work of their office. Additionally, CIGFO provides a section within the annual report on all CIGFO issued working group reports. In July 2024, CIGFO was proud to issue its fourteenth annual report to FSOC and Congress and noted that to date, the corrective actions described by FSOC, with respect to the issued CIGFO working group reports, have met the intent of CIGFO's recommendations.

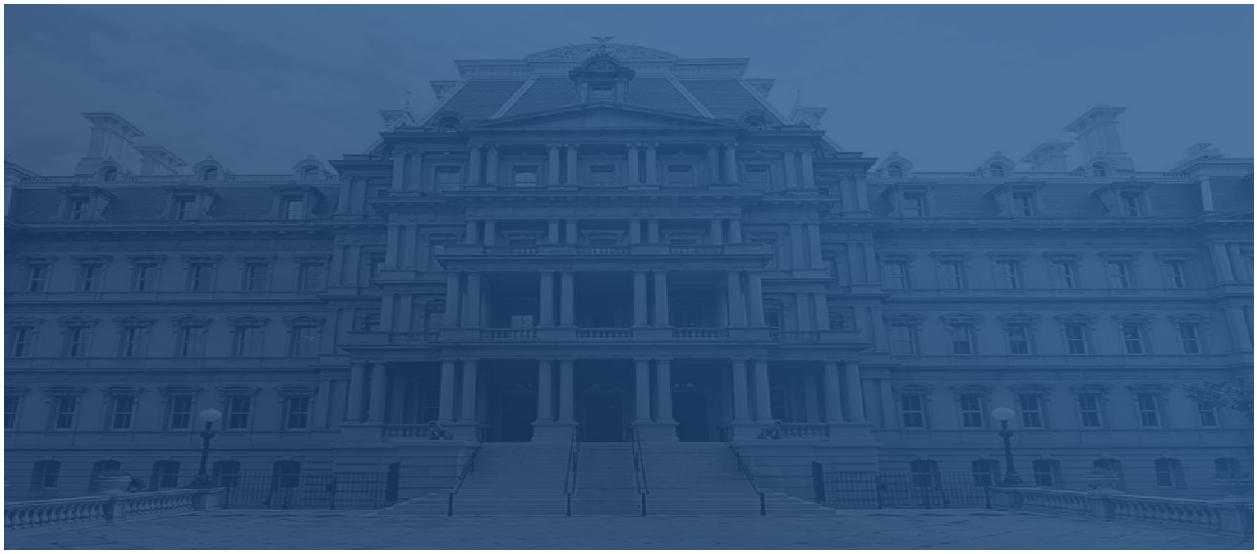
CIGFO and Council of the Inspectors General on Integrity and Efficiency (CIGIE) Coordination

CIGFO and Council of the Inspectors General on Integrity and Efficiency (CIGIE) Coordination

All eight IGs comprising CIGFO are also members of the Council of the Inspectors General on Integrity and Efficiency (CIGIE). Several of them are currently serving, or have served, on various CIGIE committees and working groups such as:

- CIGIE's Integrity Committee which receives, reviews, and refers for investigation allegations of wrongdoing made against: an Inspector General; designated staff members of an OIG; the Special Counsel, U.S. Office of Special Counsel (OSC); and the Principal Deputy Special Counsel, OSC, and ensures the fair, consistent, timely, and impartial disposition of the allegations.
- CIGIE's Professional Development Committee which provides educational opportunities for members of the IG community and ensures the development of competent personnel.
- CIGIE's Pandemic Response Accountability Committee (PRAC) was established under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act),[3] to promote transparency and ensure coordinated oversight of the government's spending and coronavirus response. Many of the CIGFO IGs are currently serving, or have served, on this important committee and provided their expertise in leading the PRAC's Financial Institutions Oversight Issue Group.

CIGFO working group efforts generally adhere to the Government Auditing Standards, also known as the Yellow Book, and when applicable, conform to the quality standards developed by CIGIE.[4]



[3] Public Law 116-136 (March 27, 2020).
[4] To learn more about CIGIE, visit www.ignet.gov/content/about-igs.

Transition Issues Relating to CIGFO

Transition Issues Relating to CIGFO

Historically, because of their nonpartisan, independent status, IGs have remained in office when Presidential Administrations change. As a result, the CIGFO member IGs will carry forward the knowledge and experience that is crucial to FSOC, CIGFO, and each IG's respective office.

Role of CIGFO in the Transition to a New Administration

Just as individual CIGFO member IGs can perform a valuable role during Presidential transitions at their respective agencies, CIGFO, as a collective body, can provide an equally valuable role in a transition. Based on its experience and unique perspective, CIGFO can be a valuable source of information about the key financial oversight issues that will confront the new Administration's management team.

In the past, the transition teams for many agencies have met separately with the IG of the respective agency for a briefing on the IG's ongoing and recently completed work, as well as the IG's view of the important issues within the agency that will confront the new Administration. It is useful for the transition teams to meet with the IG of that agency early in the transition process. Reflecting the IGs' independence and unique perspective on their agency, transition teams should meet with the IGs separate from their meetings with other management officials within the agency.

A critical document for the transition team to review is the CIGFO Annual Report. This report summarizes the general observations of CIGFO based on the views expressed by each IG with a focus on measures that should be taken to improve financial oversight. The report also consolidates each IGs concerns and recommendations with a focus on issues at their respective agencies and those that may apply to the broader financial sector. This report can provide a useful overview for the transition team and new Administration appointees in understanding the scope of the issues they will confront not only at each member agency, but in the broader financial sector. We suggest the transition teams review the CIGFO Annual Report and discuss with each respective IG their assessment of these issues.

New Administration Officials' Interaction with CIGFO

Once the new Administration takes office and after leadership of FSOC and their member agencies are appointed, it is important that they establish regular communications with CIGFO and the IGs of their respective agency.

Regular communications will enable CIGFO to inform FSOC leadership about ongoing work, the results of completed work, and the status of open recommendations from working group reports and other working group projects.

CIGFO will also be able to answer questions about the processes and procedures it uses in its work and can raise any impediments to its work or any areas that it believes need management attention for corrective action. CIGFO often invites FSOC leadership to speak at CIGFO's quarterly meetings. This ongoing engagement will allow FSOC members to discuss their priorities and views on future CIGFO reviews that could be valuable for agency programs. On these and other issues, ongoing and regular communication between FSOC and CIGFO is important to establish an effective and candid relationship that fulfills the purposes of the Dodd-Frank Act.

Council of Inspectors General on Financial Oversight