Annual Report of the Council of Inspectors General on Financial Oversight

July 2026

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 Act) was signed into law, establishing the Financial Stability Oversight Council (FSOC or Council) and the Council of Inspectors General on Financial Oversight (CIGFO). Chaired by the Department of the Treasury (herein "Treasury" or "the Department") 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, comprised of eight Inspectors General (IG) with oversight responsibilities for financial-sector agencies and programs, was created to facilitate information sharing, provide a forum for discussing oversight work, and evaluate the effectiveness and internal operations of FSOC.

Over the past year, FSOC issued its *Annual Report*,[1] outlining priority areas and actionable policy recommendations. These include bolstering Treasury's market resilience; addressing cyber risk and navigating an evolving threat landscape; enhancing supervisory and regulatory frameworks for depository institutions; and harnessing artificial intelligence (AI) to promote financial stability. Additionally, FSOC and Treasury's Artificial Intelligence Transformation Office launched the AI Innovation Series, a public private initiative that brings together financial institutions, technology firms, regulators, and subject matter experts to examine high value AI use cases and identify practical approaches for scaling innovation while maintaining safety and soundness. As FSOC continues to monitor new and emerging risks, CIGFO remains diligent in fulfilling its oversight responsibilities.

The Dodd-Frank Act authorizes CIGFO to convene working groups, by a majority vote, to review FSOC's internal operations and effectiveness. Since 2011, CIGFO has established such working groups composed of staff from the member Inspector General offices. In July 2024, CIGFO convened a working group to assess FSOC's 2023 *Guidance on Nonbank Financial Company Determinations*. This review is expected to be completed in the summer of 2026.

CIGFO's monitoring responsibilities also include sharing financial regulatory developments that inform member agencies' ongoing and future work. During quarterly meetings this past year, CIGFO members were briefed on significant legal cases and rulings, as well as legislative activities including the *Taking Account of Institutions with Low Operations Risk Act*, the *CAMELS Rating Modernization Act*, and the *Fiscal Contingency Preparedness Act*, each with potential implications for the financial regulatory system.

In February 2026, the FSOC Chairperson testified before the U.S. House Financial Services Committee, emphasizing that FSOC continues to prioritize economic growth and economic security. The testimony highlighted four key policy areas: Treasury markets, cybersecurity,

[1] Financial Stability Oversight Council 2025 Annual Report (December 11, 2025)

regulatory modernization, and AI. These areas are discussed in greater detail in FSOC's annual report.

The collaborative efforts of the IG community remain essential to promoting transparency, accountability, and resilience across the nation's financial infrastructure. Looking ahead, CIGFO members will continue, both individually and collectively, to strengthen the financial system through rigorous 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:

- The *Taking Account of Institutions with Low Operations Risk Act* would apply to 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), and the Consumer Financial Protection Bureau (CFPB). The Act requires each regulator to "tailor" the regulatory actions applicable to an institution, in regards to the type of institution, in a manner that limits the regulator impact, including cost, human resource allocation, and other burdens, on the institution, as is appropriate for the risk profile and business model involved.

- The *CAMELS Rating Modernization Act* would require the Federal Financial Institutions Examination Council of 1978, to revise the weighting of each CAMELS component[2] and either eliminate the management component of the rating or revise the management component to limit the assessment to objective measure of governance and controls used to manage the risk profile; to ensure the composite ratings are determined based on a transparent methodology limited to objective criteria.

- The *Fiscal Contingency Preparedness Act* would require the Department of the Treasury, in coordination with the Office of Management and Budget, to conduct annual "fiscal stress tests" on the U.S. government's ability to respond to emergencies like an economic recession or depression, a domestic energy crisis, a catastrophic natural disaster, a health crisis, a significant armed conflict or event, a significant cyberattack, or a financial crisis. This Act seeks to improve

[2] Federal banking agencies use the Uniform Financial Institutions Rating System, or "CAMELS," to assign composite and component ratings to financial institutions. An institution's composite CAMELS rating integrates ratings from six component areas – capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk.

transparency for the short- and long-term effects on the Federal Government if such an event occurs.

- Legislative matters of interest, including proposed legislation on various topics including: prohibiting the use of reputation risk by regulators, alternating or extending examination cycles, raising consolidated asset thresholds, and increasing FDIC insurance limits for non-interest-bearing accounts held in certain financial institutions.

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—

- CIGFO, *Audit of the Financial Stability Oversight Council's Controls over Non-public Information* (June 2012)
- CIGFO, *Audit of the Financial Stability Oversight Council's Designation of Financial Market Utilities* (July 2013)
- CIGFO, *Audit of the Financial Stability Oversight Council's Compliance with Its Transparency Policy* (July 2014)
- CIGFO, *Audit of the Financial Stability Oversight Council's Monitoring of Interest Rate Risk to the Financial System* (July 2015)
- CIGFO, *Audit of the Financial Stability Oversight Council's Efforts to Promote Market Discipline* (February 2017)
- CIGFO, *Corrective Action Verification of FSOC's Implementation of CIGFO's Audit Recommendations in the 2013 Audit of FSOC's Financial Market Utility Designation Process* (May 2017)
- CIGFO, *Top Management and Performance Challenges Facing Financial Regulatory Organizations* (September 2018)
- CIGFO, *Audit of the Financial Stability Oversight Council's Monitoring of International Financial Regulatory Proposals and Developments* (May 2019)
- CIGFO, *Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations* (July 2019)
- CIGFO, *Survey of FSOC and its Federal Member Agencies' Efforts to Implement the Cybersecurity Act of 2015* (January 2020)
- CIGFO, *Council of Inspectors General on Financial Oversight Presidential Transition Handbook* (December 2020)
- CIGFO, *Guidance in Preparing for and Managing Crises* (June 2022)
- CIGFO, *Audit of the Financial Stability Oversight Council's Efforts to Address Climate-Related Financial Risk* (August 2023)
- CIGFO, *Council of Inspectors General on Financial Oversight Presidential Transition Handbook (Updated)* (December 2024)

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 of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB) by conducting audits, evaluations, investigations, and other reviews of their programs and operations 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 (Dodd-Frank 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 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.

Completed Work, April 1, 2025–March 31, 2026

Board

Major Management Challenges

While not required by statute, we identify and monitor the major management challenges we believe that, if not addressed, are most likely to hamper the Board's ability to accomplish its strategic objectives. We use these challenges as the basis for our planning activities and seek to conduct audit and evaluation work connected to many of these topics during any work-planning cycle. We identified the Board's major management challenges by assessing key themes from our prior and ongoing audit and evaluation work, our discussions with Board management, and our knowledge of the agency's programs and operations. We generally issue these challenges every other year, in alignment with our biennial planning activities.

The Board's major management challenges are

- 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

The Board Should Enhance Its Ability to Monitor the Efficiency and Timeliness of Its Processing of Certain Banking Applications

Before engaging in certain activities like mergers or acquisitions, banks must apply for approval from Reserve Banks or the Board, which review applications for legal issues and considerations and for safety and soundness principles.

Despite recent measures to increase efficiency, median application processing times increased from 2021 to 2024—by about 11 percent for all application types and by about 40 percent for small community bank mergers and acquisitions. Board officials and staff cited numerous reasons for delays, such as time needed to consult with other regulatory agencies and conduct internal reviews before final action. We could not validate these explanations for the delays, because the Board does not track sufficient information to pinpoint opportunities for improvement.

We made three recommendations to enhance the Board's efforts to increase the efficiency and timeliness of the banking application process.

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

Effective information technology (IT) risk management is critical to the safety and soundness of financial institutions, including more than 600 community banking organizations (CBO) supervised by the Board and Reserve Banks.

However, procedures for IT examinations of CBOs are not up to date and do not reflect the evolving IT and cybersecurity risk environment. In addition, Reserve Banks have varying approaches to training examiners who conduct CBO IT examinations and completing and retaining documents used to scope such examinations.

We made five recommendations to ensure that the approach to IT and cybersecurity supervision addresses evolving risks, that training for examiners is more structured, and that the documentation of examination scopes is more consistent.

Results of Scoping of the Evaluation of the Board's Practices and Controls for Safeguarding Confidential Supervisory Information in OASIS

The Board's OASIS technology platform, which examiners use to document their supervisory activities of the nation's largest financial institutions, contains confidential supervisory information (CSI). The loss or misuse of CSI could result in significant legal, reputational, or financial risk to the Board, Reserve Banks, financial institutions, and individuals.

We identified several concerns regarding CSI access in OASIS, which the Board must address before we conduct further work. For example, users have more access to sensitive information than appears to be warranted based on their specific financial institution examination assignments, which is inconsistent with Board policy and a key information security principle.

We made four recommendations to enhance the Board's practices and controls for safeguarding CSI in OASIS.

The Board Has Generally Effective Processes for Approving and Monitoring the Currency Budget's Multicycle Projects but Can Better Document Those Processes

The Board is the sole issuing authority of the nation's currency, and it pays the Bureau of Engraving and Printing (BEP) for expenses related to producing banknotes. As part of this arrangement, BEP develops a multicycle project budget for its large-scale capital investments (such as production equipment and facilities) that span multiple years.

The Board's processes for approving and monitoring the multicycle project budget are generally effective, providing sufficient resources to the BEP and promoting effective stewardship of funds. However, the Board has not incorporated all of its approval and

monitoring processes into its memorandum of understanding with BEP.

We made one recommendation for the Board to incorporate these processes to ensure both parties agree to and are accountable for their respective responsibilities.

2025 Audit of the Board's Information Security Program

Each year, we audit the Board's information security program as required by FISMA.

The maturity level of the Board's information security program decreased since 2024, leading us to conclude the program is no longer effective. Challenges in cybersecurity governance, coupled with opportunities to strengthen cybersecurity profiles, mobile device security, and information classification for CSI, contributed to the decline.

We made three recommendations to strengthen the Board's information security program. Given the sensitivity of the information in our review, portions of the public version of this report were redacted.

Ongoing Work as of March 31, 2026

Board

Evaluation of the Board's Insider Risk Management Activities

We are assessing 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.

Evaluation of the Board's Processes for Appointing and Approving Federal Reserve Bank Leaders

We are assessing the design and implementation of the Board's processes for appointing, approving, and consulting on the selection of certain Reserve Bank leaders, including processes related to the identification and resolution of potential conflicts of interest.

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

We are assessing the effectiveness of the Board's and the Federal Reserve Banks' practices for following up on supervisory findings that address safety and soundness issues in the large and foreign banking organization portfolio.

2026 Audit of the Board's Information Security Program

To meet FISMA requirements for 2026, we are assessing the effectiveness of the Board's (1)

security controls and techniques for selected information systems and (2) information security policies, procedures, standards, and guidelines.

Security Control Review of the Board's One Agile Supervision Solution

To meet FISMA requirements, we tested selected security controls for OASIS. The system is used by examiners to document their supervisory activities of the nation's largest financial institutions.

Security Control Review of the Board's Banknote Inventory System

To meet FISMA requirements, we tested selected security controls for the Banknote Inventory System. The system is used to track banknotes and other items related to currency development, performance, and production.

Security Control Review of the Board's Research and Statistics Recruiting System

To meet FISMA requirements, we tested selected security controls for the Research and Statistics Recruiting system. The system is used to identify, track, screen, and select individuals for economist and research assistant positions at the Board.

Completed Work, April 1, 2025-March 31, 2026

CFPB

The CFPB Can Improve Its Safeguards for Protecting Confidential Supervisory Information

In 2023, the CFPB declared a major incident breach that affected about 256,000 consumers and 46 institutions after an examiner sent CSI, including personally identifiable information, to a personal email account.

CFPB guidance does not effectively limit access to CSI in its system of record for supervision activities and does not sufficiently limit access to CSI used to prioritize supervisory activities. Additionally, the CFPB's guidance for managing CSI breaches does not include expectations for assessing and documenting the severity of breaches and determining, enforcing, and documenting consequences for responsible employees. Further, the agency does not conduct trend analysis on the causes of breaches to determine the appropriate adjustments to controls based on reoccurring themes. Finally, the CFPB does not have a defined process to notify affected supervised institutions of breaches.

We made seven recommendations to improve the CFPB's safeguards for protecting CSI.

2025 Audit of the CFPB's Information Security Program

Each year, we audit the CFPB's information security program as required by FISMA.

The maturity level of the CFPB's information security program has decreased since 2024, leading us to conclude the program is no longer effective. For example, authorizations to operate for many systems are not maintained, risk acceptance memorandums lack documented analysis of cybersecurity risks, and outdated software remains in use. While the agency was able to maintain or even strengthen information security in some areas, such as transitioning to continuous vetting of employees, those efforts do not mitigate the overall decline.

We made six recommendations to strengthen the CFPB's information security program.

Ongoing Work, as of March 31, 2026

CFPB

Congressional Request: Review of the CFPB's Workforce and Contract Reduction Actions

We are reviewing the CFPB's workforce and contracting actions to determine their high-level effects on mission-related activities and support functions. We are not assessing whether these actions complied with applicable laws, regulations, policies, or procedures because they are the subject of ongoing litigation.

Congressional Request: Review of the CFPB's Adherence to Processes and Procedures in Connection with Certain Policy and Oversight Matters

We are assessing whether the CFPB, under former Director Rohit Chopra, adhered to relevant processes and procedures in its decisions to broaden its definition of "unfair, deceptive, or abusive acts or practices" and its definition of "credit" under the Truth in Lending Act. We will also inquire whether the CFPB has available information that will enable us to assess the time and costs associated with the enforcement actions issued during then Director Chopra's tenure in comparison to those issued during the tenure of prior directors.

Board and CFPB Investigative Work

Our Office of Investigations investigates criminal, civil, and administrative wrongdoing by Board and CFPB employees as well as alleged misconduct or criminal activity that affects the Board's or the CFPB's ability to effectively supervise and regulate the financial community. We operate under statutory law enforcement authority granted by the U.S. attorney general, which vests our special agents with the authority to carry firearms, to seek and execute search and arrest warrants, and to make arrests without a warrant in certain circumstances.

Our investigations are conducted in compliance with Quality Standards for Investigations, issued by CIGIE, and Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority.

The Board is responsible for consolidated supervision of bank holding companies and state-chartered banks that are members of the Federal Reserve System, known as state member banks. Under delegated authority from the Board, the Reserve Banks supervise bank holding companies and state member banks, and the Board's Division of Supervision and Regulation oversees the Reserve Banks' supervisory activities. Our investigations concerning bank holding companies and state member banks typically involve allegations that senior officials falsified financial records, lied to or misled examiners, or obstructed examinations.

The CFPB implements and enforces federal consumer financial law and supervises large banks, thrifts, and credit unions with total assets of more than $10 billion and certain nonbank entities, including mortgage brokers, loan modification providers, payday lenders, consumer reporting agencies, debt collectors, and private education lenders. Our investigations concerning the CFPB's responsibilities typically involve allegations that company directors or officers provided falsified business data and financial records to the CFPB, lied to or misled examiners, or obstructed examinations. Additionally, with certain exceptions, the CFPB's enforcement jurisdiction generally extends to individuals or entities that are engaging or have engaged in conduct that violates federal consumer financial law.

Many of our investigations concern fraud related to the Federal Reserve's pandemic response efforts, including the Main Street Lending Program, which supported lending to small- and medium-sized for-profit and nonprofit organizations in sound financial condition before the COVID-19 pandemic, and the Paycheck Protection Program Lending Facility, which extended credit to eligible financial institutions and took Paycheck Protection Program loans guaranteed by the U.S. Small Business Administration as collateral. In addition, our office also conducted investigations in support of our PRAC membership. Our office is also part of the U.S. Department of Justice's COVID-19 Fraud Enforcement Task Force.

Office of Inspector General
Commodity Futures Trading Commission

The Commodity Futures Trading Commission (CFTC or Commission) Office of Inspector General (OIG) is an independent office within the CFTC 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 recommends 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 and regulations, 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 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.[3] In its most recent report, the OIG identified the following top management and performance challenges related to the financial sector:

- *Pending Legislation: Regulation of Digital Assets*
- *Expiration of Customer Protection Fund Expense Account (Whistleblower Program)*

Pending Legislation: Regulation of Digital Assets

Legislation pending before Congress would delegate varying degrees of regulation of cryptocurrencies and other digital assets to the CFTC. The Digital Asset Market Clarity Act of 2025 (CLARITY Act or CLARITY)[4] proposes a division of digital asset market jurisdiction between the Securities and Exchange Commission (SEC) and CFTC. CLARITY also recognizes decentralized governance systems, which innovates how individuals collectively reach agreement on development and administration of blockchain systems, and impacts banking institutions' treatment of digital assets.

Proposed Title IV under CLARITY sets out a comprehensive regulatory scheme for digital asset markets under CFTC jurisdiction. Under CFTC jurisdiction and responsibility, CLARITY requires (among other things):

[3] 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.

[4] H.R. 3633, 119th Congress. The Senate is considering the bill and has issued a bipartisan discussion draft.

- Futures commission merchants to use qualified digital asset custodians, trading certifications and approvals for digital commodities
- Registration of digital commodity exchanges, brokers and dealers, associated persons, commodity pool operators and commodity trading advisers in digital commodities
- Qualified digital asset custodians to be regulated by a federal, state, or foreign authority and subject to adequate supervision and regulation by a federal, state, or foreign authority and subject to adequate supervision and regulation for digital asset custodial activities, and subject to standards set by the CFTC and – for CFTC registrants – subject to CFTC rules to custody digital assets
- Comprehensive customer fund segregation requirements and commingling restrictions

In addition, CLARITY exempts certain decentralized finance activities related to blockchain networks from CFTC regulation, but not from CFTC's anti-fraud or anti-manipulation enforcement authority; and requires the trading of other types of tradable digital assets (which are not digital commodities) on or through a person registered with the CFTC as though the asset was a digital commodity.

With regard to estimated costs to regulate the digital asset industry within CFTC jurisdiction,[5] CLARITY would authorize CFTC to charge and collect initial and annual filing fees from any entity registered with the CFTC as a digital commodity exchange, a digital commodity broker, or a digital commodity dealer, as authorized in advance through Congressional appropriations.[6] Further, CFTC would be permitted expedited hiring authority to fill positions related to carrying out CLARITY. Both authorities would sunset after four fiscal years. In addition, on November 10, 2025, Chairman John Boozman and Senator Cory Booker released a bipartisan discussion draft of legislation regulating crypto markets in the United States. Like the CLARITY Act, it seeks to concentrate federal oversight over cryptocurrency markets with the CFTC.

Anticipated passage of legislation expanding CFTC jurisdiction and authority related to cryptocurrency and other digital assets may present a significant management challenge. CFTC may be required to implement new registrant categories, complete necessary rulemakings, and implement mandated cooperative regulatory efforts. Challenges include obtaining additional qualified staff, developing institutional knowledge and expertise, launching and maintaining necessary additional data systems and analytics, and management of additional budgetary resources.

[5] The agency's FY 2026 President's Budget request did not appear to estimate or include funds necessary to regulate the digital asset marketplace. See, CFTC, FY 2026 President's Budget (May 2025). https://www.cftc.gov/sites/default/files/CFTC_FY2026_Presidents_Budget.pdf. Congress appropriated CFTC $365 mil. for FY 2026. P.L. 119-75 (2/3/2026).

[6] Last year the Congressional Budget Office estimated that a similar funding mechanism proposed in legislation (H.R. 4763 or FIT21) to regulate digital asset markets would (as appropriated) "roughly offset the costs for the CFTC to implement H.R. 4763." (https://www.cbo.gov/system/files/2024-05/hr4763_house.pdf)

We take this opportunity to note we are also monitoring event contract developments, including recent litigation involving CFTC in multiple jurisdictions.

Expiration of Customer Protection Fund Expense Account (Whistleblower Program)

Section 748 of the Dodd-Frank Wall Street Reform and Consumer Protection Act[7] (Dodd-Frank Act) established the CFTC Whistleblower Program and the CFTC Customer Protection Fund ("CPF" or "Fund"), which is available to pay awards to eligible whistleblowers and to fund customer education initiatives. 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 $390 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.

In accordance with the Dodd-Frank Act, the Commission deposits certain collected monetary sanctions into the Fund whenever the balance of the Fund at the time the monetary sanction is collected is less than $100 million, and this applies even when the deposit of a monetary sanction causes the balance of the Fund to exceed $100 million. The existing mechanism to fund the CPF is not tied to anticipated or potential award payouts and instead is dependent on the timing of penalty collections. If a large penalty is collected when the CPF is below $100 million, the fund can appear to be hoarding large amounts.

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 by statute in 2021 (P.L. 117-25, sec. 1, as amended) expired on September 30, 2025; however, the Consolidated Appropriations Act, 2026 (P.L. 119-75, sec. 5002) extended the deadline to September 30, 2026.

The pending expiration of separate funding for administrative expenses potentially presents significant management challenges for the WBO and OCEO. The administrative funds reverted to the CPF upon expiration, but if the CPF is thereafter depleted through the payment of awards, the OCEO and WB programs will cease operations completely. Delays in processing and receiving awards could damage OCEO and WBO operations and reputations. The time to

[7] Dodd-Frank Wall Street Reform and Consumer Protection Act, P.L. 111-203, 124 Stat. 1376 (July 10, 2010).

reestablish OCEO and WBO operations once funding is available could be substantial. In addition, the possibility of a program shutdown potentially contributes to WBO and OCEO employee turnover. Moreover, if penalties are not available to fund the CPF when whistleblower awards are due and owing, awards will be delayed. A better solution might involve funding the CPF for anticipated need based on pending WBO activity.

Recent, Current or Ongoing Work in Financial Oversight

Audit of the CFTC's FY2025 Annual Financial Report (25-AU-01)

The objective of this Congressionally mandated audit was to render an opinion on the agency financial report (financial statements) in accordance with Generally Accepted Government Auditing Standards (GAGAS). The audit was completed by an independent public accountant (IPA) with CFTC OIG Office of Audits 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 Federal Financial Management Improvement Act;
- No reportable noncompliance with provisions of laws tested or other matters; and
- CFTC received a "clean" opinion with no significant issues noted.

Audit of the CFTC's FY2025 Customer Protection Fund (25-AU-02)

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 Office of Audit oversight. In its audit report, the IPA reported that CFTC received a "clean" opinion with no significant issues noted.

Recent, Current or Ongoing Work in Regulatory Oversight

Audit of the CFTC's Whistleblower Program (26-AU-04)

The objectives of this audit include assessing the effectiveness of the program's governance, internal controls, and processes for administering whistleblower tips, investigations, and award determinations. Additionally, it will assess whether the program operations are consistent with statutory and regulatory requirements and resources are managed effectively. This audit was announced in March 2026 and is ongoing.

Evaluation of CFTC's Division of Clearing and Risk (DCR)'s Policies and Procedures (26-E-01)

On March 31, 2026, the Office of Evaluations announced a review of CFTC's DCR's Policies and Procedures. This assessment will evaluate whether DCR's policies and procedures support mission objectives and can adapt to the evolving nature of the regulatory risk environment. Recent transitions in leadership across the agency as well as the expanding and evolving regulatory environment have left many divisions traversing uncertain territories due to the risk of policies and procedures not adapting in step. Additionally, some divisions may have lost valuable skill sets due to the Deferred Resignation Program option, federal government-wide Reductions-in-Force and other significant human capital factors. Well documented policies and procedures ensure consistent reviews and analysis, reduce risk of non-compliance with laws and regulations, and ensure integrity and reliability of a division's efforts in meeting the agency's mission.

Follow Up on Relevant Prior Year Recommendations

24-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 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. During the reporting period the CFTC implemented corrective actions to close four recommendations.

Office of Inspector General
Federal Deposit Insurance Corporation

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) is responsible under the Inspector General (IG) Act 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. Our mission is to deliver credible results that drive meaningful change, enhance integrity and accountability, and maintain public trust in the FDIC.

Background

The 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; and resolves failed banks.

The FDIC insures $10.82 trillion in domestic deposits at about 4,336 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 2,738 of the insured institutions. The Deposit Insurance Fund (DIF) balance totaled $153.9 billion as of December 31, 2025. Active receiverships as of December 31, 2025, totaled 44, with assets in liquidation of about $24.3 billion.

The FDIC OIG is an independent and objective oversight unit established under the IG Act of 1978, as amended (IG Act). Under the IG Act, our responsibility is to prevent, deter, and detect fraud, waste, abuse, and mismanagement in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the Agency. At the FDIC, our mission is to deliver credible results that drive meaningful change, enhance integrity and accountability, and maintain public trust in the FDIC.

We pursued audits, evaluations, and other reviews throughout the year in carrying out this mission. Of particular interest for this Council of Inspectors General on Financial Oversight (CIGFO) report and implications for the broader financial sector, our audit and evaluation work

covered topics such as the failure of Pulaski Savings Bank, Chicago, Illinois, and a report addressing the Significant Service Provider Examination Program.

Importantly, and in connection with matters affecting the financial sector, in March 2026, 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. Other CIGFO-member agencies may face similar challenges, and our identification of eight challenges may be of interest.

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 through our Electronic Crimes Unit 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 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 202 cases associated with fraud in the CARES Act and ARP programs. 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, 2026, the FDIC OIG issued 11 audit and evaluation-related products, including our Top Management and Performance Challenges report, and made 35 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.

Failure of Pulaski Savings Bank, Chicago, IL

On January 17, 2025, the Illinois Department of Financial and Professional Regulation (IDFPR), Division of Banking, took possession and control of Pulaski Savings Bank and appointed the FDIC as receiver. Pulaski Savings Bank was a state-chartered mutual savings bank that first became FDIC-insured on August 9, 1989. Pulaski Savings Bank was a certified Community Development Financial Institution primarily focused on single family residential loans that

operated from a single branch office location in Chicago, IL. The bank's funding largely came from local, core deposits. According to the FDIC, at the time of failure, the estimated loss to the DIF from Pulaski Savings Bank's failure was $28,449,000 or 62 percent of the bank's $45,919,248 in total assets.

When the DIF incurs a loss under $50 million, the Federal Deposit Insurance (FDI) Act requires the Inspector General of the appropriate Federal banking agency to conduct a review of the failed bank to determine the grounds identified by the state or Federal banking agency for appointing the FDIC as receiver and to determine whether any unusual circumstances exist that might warrant an In-Depth Review (IDR) of the loss.

Our Failed Bank Review found that Pulaski Savings Bank failed due to impaired capital, and we determined that an IDR of the loss was warranted given the high estimated loss rate (62 percent) and unaccounted for deposit liabilities.

We subsequently conducted an IDR to (1) determine the cause(s) of Pulaski Savings Bank's failure and resulting 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 FDI Act.

As noted above, Pulaski Savings Bank's failure occurred primarily due to impaired capital. Specifically, the bank had deposit liabilities of at least $20.7 million not accounted for in its core financial system. Since assets corresponding with these deposits were not identified, the subsequent recording of these previously unrecognized deposits exceeded the bank's equity capital, at which point, the bank became critically undercapitalized.

Consistent with PCA provisions, the FDIC notified Pulaski Savings Bank that it was "critically undercapitalized" and required it to take actions necessary to increase capital. Ultimately, the IDFPR determined that the bank was impaired, took possession, and appointed the FDIC as receiver.

With regard to supervision, the FDIC conducted its examinations in a timely manner and identified weaknesses in the bank's management since 2017. While the FDIC did not formally designate a dominant official at Pulaski Savings Bank, its supervisory actions sought to mitigate weaknesses in the bank's management, including certain key person risks in the most recent examination cycles. For that reason, we did not make a formal recommendation in this report. However, we encouraged the Division of Risk Management Supervision to consistently consider the presence and impact of dominant officials as part of the examination process and designate officials as such when appropriate and in accordance with FDIC procedures and guidance.

Significant Service Provider Examination Program

Under the Bank Service Company Act of 1962, the FDIC, the Board of Governors of the Federal Reserve System, and Office of the Comptroller of the Currency have the statutory authority to examine covered services provided by third parties to their regulated financial institutions. The FDIC conducts service provider examinations to evaluate the overall risk exposure and risk management performance and determine the degree of supervisory attention needed to ensure weaknesses are addressed and risks are properly managed by financial institutions using service providers.

The FDIC performs these examinations using two risk designations: significant service providers (SSP) and regional service providers (RSP). SSPs are large and complex service providers designated as agreed upon by the Federal Banking Agencies (FBA) for special monitoring and collaborative interagency supervision at the national level. In contrast, RSPs are smaller in size, less complex, and provide services to banks within a local region.

In December 2023, the OIG issued a memorandum where we found that the FDIC had not established performance goals, metrics, and indicators to measure overall program effectiveness and efficiency for the RSP Examination Program. Accordingly, we recommended that the FDIC conduct a formal assessment of the RSP Examination Program to establish program-level goals, metrics, and indicators and determine whether additional resources and controls were needed to improve the effectiveness of the program.

During this past year, we conducted an audit to determine the effectiveness of the SSP Examination Program in evaluating the risk exposure and risk management performance of SSPs and determining the degree of supervisory attention needed to ensure weaknesses are addressed and risks are properly managed. We determined that the FDIC had not established program-level performance goals and metrics to measure overall SSP Examination Program effectiveness and efficiency.

The service providers included in the SSP portfolio evolve over time based on the FBAs' assessment of risk. The FBAs generally have discretion about which and how many service providers to examine. FDIC officials stated that they used a risk-based approach to attempt to direct examination resources to service providers that pose the greatest risk to banks. The risk factor of greatest concern is the risk of a service provider failure causing a failure at one or more banks, but the FDIC considers other risks such as those related to privacy.

Division of Risk Management Supervision (RMS) officials stated that they consider quantitative factors to determine which service providers pose the greatest risk to banks. These factors include metrics such as the number of banking customers the service provider serves, the value of the assets held by client banks, the volume of payments processed, and other key business line metrics.

RMS also considers qualitative factors in determining prioritization efforts for SSP examinations. For example, RMS considers the mission criticality and substitutability of the services provided and the potential impact that a disruption in the service would have on the client bank. However, RMS officials stated they seek to avoid taking actions that would shape the bank service provider market or create the perception that the FDIC is endorsing certain service providers.

We observed that the vendor selection process in place when we began our review was highly subjective, poorly documented, and would benefit from additional quantitative analysis. In that regard, the FBAs set out to establish a new FBA Inherent Risk Methodology Analysis (IRMA) that was a risk-based methodology for measuring and risk-ranking service providers.

IRMA is designed to (1) prioritize service providers who are currently supervised to determine the appropriate examination frequency and commensurate resourcing, (2) evaluate whether new service providers should be supervised and added to the program, and (3) evaluate whether existing service providers should no longer be supervised and removed from the program.

We reported that these updates should lead to improved decisions about which providers to select for examination since the selection methodology would be more grounded in quantitative analysis; however, the effort was not complete as of May 2025.

We recommended that the Director, RMS, complete efforts to develop and implement program-level goals and metrics for both the Regional and Significant Service Provider Examination Programs. This should include finalizing and implementing IRMA. In its response, the FDIC concurred with our recommendation.

Top Management and Performance Challenges

During the past year, the Federal Government, including the FDIC, underwent significant restructuring and reform that continues to unfold. Our annual reporting of the Top Management and Performance Challenges facing the FDIC highlighted areas that we believe warrant the FDIC's continued attention as it carries out its critical mission and briefly assesses the Agency's progress in addressing those challenges. By statute, the FDIC OIG is required to conduct this assessment for inclusion in the FDIC's Annual Performance and Accountability Report, which was issued on March 26, 2026.

The Top Challenges that we identified were based on the status, makeup, and processes in place at the FDIC as of mid-February 2026. They were based on our independent oversight through audits, evaluations, investigations, and reviews; discussions with FDIC management at all levels; inquiries and trends from our OIG Hotline; and other credible external sources. We acknowledged that the FDIC is likely to undergo significant changes going forward that may impact these currently identified Top Challenges.

We noted this year that overall, the long-term success of the FDIC depends on a sufficient cadre of skilled personnel, a safe and accountable workplace, effective governance and interdivisional coordination, resolution and receivership readiness, effective supervision, adherence to established internal controls, strong information security, and identification of fraud risks within the banking industry. Maintaining public confidence and the FDIC's role in ensuring financial and banking system stability remain essential priorities.

We identified the following eight Top Challenges facing the FDIC, full details of which are posted on our website at TMPC.

1. **Optimizing the FDIC Workforce.**
   - Human Capital Risks and Workforce Challenges.
2. **Maintaining a Safe and Accountable Workplace Culture.**
3. **Strengthening Organizational Governance.**
   - Fostering Agency-Wide Coordination to Work as One-FDIC.
   - Measuring Progress Towards Mission Goals.
4. **Sustaining Readiness to Execute Resolution and Receivership Responsibilities.**
   - Improving Readiness for Large Regional Bank Failures.
   - Procurement of Resolution and Receivership Services.
5. **Ensuring Effective Supervision.**
   - Escalating Supervisory Actions.
   - Supervision of Third-Party Service Providers.
   - Reforming the FDIC's Supervisory Framework.
6. **Improving Contract Management.**
   - Adhering to Contracting Requirements and Internal Controls.
   - Improving Procurement of Services.
7. **Enhancing Cyber and Data Security.**
   - Implementing the Use of Artificial Intelligence.
8. **Identifying and Combating External Fraud and Misrepresentation.**
   - Insider Fraud.
   - Scams Targeting Unwitting Customers.
   - Addressing Misuse of the FDIC Name and Logo.

Ongoing Projects

As of March 31, 2026, we had a number of ongoing audit and evaluation projects that will be of relevance to the broader financial sector when completed, among those:

- **Valuation Process for Large Regional Bank Resolutions:** Our objective is to determine whether the FDIC adhered to established policies and procedures for the valuation function in response to the failures of Silicon Valley Bank, Signature Bank of New York, and First Republic Bank.

- **FDIC's Franchise Marketing Process for Large Regional Bank Resolutions:** Our objective is to determine the extent to which the FDIC adhered to established policies and procedures consistent with FDI Act requirements for the Franchise Marketing function in response to the failures of Silicon Valley Bank, Signature Bank, and First Republic Bank.

- **FDIC Examinations of Banks' Anti-Money Laundering (AML)/Countering Financing of Terrorism (CFT) and Sanctions Compliance:** Our objective is to determine whether (1) the FDIC effectively conducted AML/CFT examination scoping and planning activities, and to what extent planning decisions align with identified risks, and (2) the examiners have the necessary training and skills to evaluate AML/CFT and sanctions compliance.

FDIC OIG Investigations

Our office is committed to partnerships with other OIGs, the Department of Justice, 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 companies, and international financiers.

Our investigative results over the 12 months ending March 31, 2026, included the following: 81 indictments; 97 convictions; 85 arrests; and potential monetary recoveries (fines, restitution, asset forfeitures, settlements, special assessments) of more than $646.7 million.

Among other cases, we continue to investigate PPP 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, 2025, through March 31, 2026, the FDIC OIG's efforts related to the Federal Government's COVID-19 pandemic response resulted in 19 indictments and informations; 15 arrests; and 22 convictions involving fraud in the CARES Act Programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases alone totaled in excess of $41.4 million.

Several examples from the past year illustrate the varied impact of our investigations.

Startup CEO Charlie Javice and Chief Growth Officer Olivier Amar Sentenced

On September 29, 2025, in the Southern District of New York, Charlie Javice was sentenced to 85 months in prison, 3 years of supervised release, and ordered to pay a forfeiture judgment of $22,360,977.48 and restitution in the amount of $287,501,078.00 (joint and

several with a co-defendant). Javice was previously convicted in March 2025 after a 6-week trial for conspiracy to commit wire fraud and bank fraud, wire fraud, bank fraud, and securities fraud. Olivier Amar, the startup's Chief Growth Officer, was also convicted at trial. On November 5, 2025, in the Southern District of New York, Olivier Amar was sentenced to 68 months in prison, 3 years of supervised release, and ordered to pay $168,531,713 in restitution and $5,690,70.31 in forfeiture.

In or about 2017, Javice founded Frank (Frank), a for-profit company that offered an online platform designed to simplify the process of filling out the Free Application for Federal Student Aid. In or about 2021, Javice began to pursue the sale of Frank to a larger financial institution. Two major banks, JPMorgan Chase Bank (JPMC) and Capital One, expressed interest and began acquisition processes with Frank. Javice represented repeatedly to those banks that Frank had 4.25 million customers or "users"; however, Frank had fewer than 300,000 users. In reliance on Javice's fraudulent representations about Frank's users, JPMC agreed to purchase Frank for $175 million. Following the sale, when JPMC sought to verify the number of Frank's users and the amount of data collected about them, Javice fabricated a data set. Unbeknownst to JPMC, at or about the same time that Javice was creating the fabricated data set, Javice and Amar sought to purchase, on the open market, "real" data for over 4.25 million college students to cover up their misrepresentations. As part of the deal, JPMC hired Javice and other Frank employees. Javice received over $21 million for selling her equity stake in Frank and, per the terms of the deal, was to be paid another $20 million as a retention bonus.

> ***Source**: USAO for the Southern District of New York**. Responsible Agencies:** This investigation is being conducted by the FDIC OIG. The case is being prosecuted by the USAO for the Southern District of New York.*

KeyBank Agrees to $7.8 Million Settlement Agreement

On January 7, 2026, it was announced that KeyBank entered into a settlement agreement with the United States resolving allegations that the bank violated the False Claims Act by submitting for forgiveness fraudulent loans from the PPP, which one of Key Bank's branch managers, Tommy Hawkins, had fraudulently conspired to obtain. KeyBank agreed to pay $7,770,595.25 in the settlement agreement.

In 2020 and early 2021, Hawkins worked as the branch manager of the Conshohocken, Pennsylvania, branch of KeyBank. Hawkins worked with co-conspirators to recruit individuals who owned companies with little or no operations to open bank accounts at Hawkins' branch and apply for PPP loans. Hawkins helped the recruited individuals submit PPP loan applications that contained materially false representations about the companies' number of employees and payroll expenses. The applications also included false documentation, including tax forms. Based on these fraudulent applications, Hawkins' bank approved at least 38 PPP loans and disbursed approximately $5 million. Hawkins received incentive compensation through the bank for opening business bank accounts for the companies that received the fraudulent

PPP loans. Hawkins also had an agreement with his co-conspirators to pay him $5,000 for each PPP loan that he helped to secure.

In spring 2021, KeyBank detected suspicious patterns in Hawkins' origination of new business accounts. After an internal investigation, KeyBank disclosed to the Small Business Administration (SBA) its concerns with 18 PPP loans that KeyBank identified as potentially fraudulent. Over the ensuing months, KeyBank's investigations identified approximately a dozen additional PPP loans that were likely fraudulent, and it disclosed those to the SBA. KeyBank did not investigate or otherwise detect fraud in the remaining loans to fraudulent PPP borrowers that Hawkins facilitated during that time. Notwithstanding its concerns with the loans, KeyBank submitted forgiveness applications or guaranty purchase forms to SBA for the fraudulent PPP loans from the Conshohocken branch. Because each individual loan was below $150,000, SBA granted that forgiveness on an expedited basis.

In addition to the civil settlement, 14 individuals were charged in the criminal case, including former KeyBank employee Hawkins. Eleven of the fourteen individuals have already pled guilty.

> ***Source**: USAO for the District of New Jersey. **Responsible Agencies:** This is a joint investigation by the FDIC OIG, FBI, Social Security Administration OIG, SBA OIG, and Department of Labor OIG. The matter is being prosecuted and litigated by the Criminal and Civil Divisions of the USAO for the District of New Jersey, respectively.*

Finally, in addition to the several discrete cases highlighted above, we have undertaken other actions of import to the broader financial sector. Specifically, during the reporting period, we partnered with USAOs in judicial districts in 40 locations in the U.S. to bring to justice individuals who have defrauded the FDIC or financial institutions within the jurisdiction of the FDIC or criminally impeded the FDIC's examination and resolution processes. Our collective efforts have served as a deterrent to others contemplating criminal activity and helped maintain the public's confidence in the Nation's financial system. We have also participated in hundreds of Task Forces and Working Groups nationwide where we collaborate with our colleagues to combat white-collar crime and 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. Finally, we have increased our outreach efforts to inform stakeholders such as banks and the general public about scams that can harm them, including investment scams, relationship scams, impersonation and misrepresentation scams, call spoofing, and ATM jackpotting frauds.

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.

Background

The Housing and Economic Recovery Act of 2008 established FHFA (also known as U.S. Federal Housing) in July 2008. FHFA regulates and supervises Fannie Mae and Freddie Mac (collectively, the Enterprises) and their affiliate, U.S. Financial Technology, LLC (U.S. FinTech), as well as the Federal Home Loan Banks (FHLBanks)[8] and the FHLBanks' fiscal agent, the Office of Finance. FHFA has served as the Enterprises' conservator since September 2008.

FHFA is responsible for ensuring that 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, 2025, the Enterprises collectively reported approximately $7.8 trillion in assets, and the FHLBanks reported more than $1.2 trillion.

OIG's Risk-Based Oversight Strategy

FHFA's dual roles as the regulated entities' supervisor and the Enterprises' conservator put FHFA in a position different from that of other federal financial regulators, and OIG structures its oversight program to examine rigorously the Agency's exercise of both responsibilities. As part of that oversight, OIG focuses its work on the areas of greatest risk

[8] Collectively, the Enterprises, U.S. FinTech, and the FHLBanks are the "regulated entities." 12 U.S.C. § 4502(20).

to FHFA and the regulated entities through our audits, evaluations, and compliance reviews, and investigations.

Management and Performance Challenges

An integral part of OIG's oversight is to identify and assess FHFA's top management and performance challenges, and to align our work accordingly. We annually 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 those challenges for Fiscal Year (FY) 2026 is available on our website.

FHFA's most significant management and performance challenges for FY 2026 are:

- Managing risk in the Enterprises' multifamily lines of business;
- Managing vulnerability within FHFA's information security programs and at the regulated entities;
- Addressing human capital risk at FHFA;
- Overseeing the regulated entities' reliance on counterparties and third parties; and
- Creating and maintaining records justifying key management decisions.

OIG considers these challenges when planning its oversight activities.

Significant Reports

OIG focused much of its oversight activity on identifying vulnerabilities in the areas highlighted above 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, 2025, and March 31, 2026, provides important insights across FHFA's programs and operations, including the regulated entities under the Agency's purview.

Regulated Entities

FHFA regulates and supervises its regulated entities primarily through its Division of Enterprise Regulation and Division of Federal Home Loan Bank Regulation (DBR). During the relevant period, we assessed FHFA's oversight of several key areas, including duty to serve obligations, regulatory information sharing, model risk, and multifamily examinations.

The Enterprises must serve very low, low, and moderate income families in three underserved markets: manufactured housing, affordable housing preservation, and rural housing (i.e., Duty to Serve). Annually, FHFA is required to evaluate the Enterprises' compliance with their Duty to Serve obligations, rate their performance for serving each underserved market, and report to Congress. In AUD-2025-005, we determined that the Agency's oversight of the Enterprises' compliance with their Duty to Serve requirements lacked certain procedural safeguards necessary to ensure full effectiveness. While we

found that some oversight functions were generally effective, others were not. That is, the FHFA did not always document accurate and complete evaluations of the Enterprises' performance, and internal guidance was outdated. FHFA agreed with our three recommendations to address these findings.

In EVL-2025-005, we assessed the framework for FHLBank System members' federal and state financial regulators to share relevant supervisory information with FHFA and the FHLBanks. We found that several FHLBanks received incomplete information about their members. We also found lapses in the FHLBanks' receipt of material adverse event notifications, the process by which members notify their FHLBank of negative changes to their financial or operating condition. FHFA agreed with all six of our recommendations to address these findings.

In AUD-2025-009, we determined that DBR needed to improve controls over its risk models and analysis products to ensure their accuracy and reliability for decision-making and analyzing the FHLBanks' market risk model results. That is, DBR had not designed and implemented controls addressing model risk management supervisory expectations for three important areas: model inventory maintenance, independent model validation, and model performance tracking. Furthermore, some control procedures were not up-to-date and lacked certain controls over model risk management. We also found weaknesses in DBR's retrieval of review documentation. FHFA agreed with our three recommendations to address these findings.

The Enterprises provide liquidity to the multifamily mortgage market by purchasing and securitizing multifamily mortgage loans. FHFA monitors the Enterprises' multifamily activities, including seller/servicers, portfolio monitoring, and accounting. In AUD-2026-002, we found that the Agency generally complied with guidance for conducting its multifamily examinations, but the examiners did not fully document their sampling approach for the selection of Fannie Mae loan files tested. FHFA agreed with our two recommendations to address this finding.

Agency Operations

Our body of work encompasses not only FHFA's oversight of the regulated entities but also the Agency's internal operations. In AUD-2025-007, we assessed FHFA's information security controls from January 2025 through July 2025. We determined that FHFA's security controls were not fully effective to protect its network and systems against external threats. For example, we were able to download internal files from one of the Agency's websites, which handles personally identifiable information, without authentication or detection. We also found that FHFA's internal video surveillance system was publicly accessible online, unmonitored, and contained known vulnerabilities dating back to 2019. These vulnerabilities make FHFA's information technology infrastructure, and the non-public information stored on it, more susceptible to unauthorized access and security compromises. FHFA agreed with all 19 of our recommendations to address our findings.

In EVL-2025-003, we assessed whether FHFA adhered to its policies when granting and distributing monetary awards, recruitment bonuses, and retention allowances during fiscal year 2023 (review period). While FHFA followed requirements for monetary awards and retention allowances, documentation of its justification for recruitment bonuses was insufficient. We found that three of the six recruitment bonuses – totaling $95,768 – either did not include the required justification written by the head of the relevant major FHFA organizational unit, or the required justification lacked documentation. As such, we reported $95,768 in unsupported costs incurred during the review period. FHFA agreed with our two recommendations to address these findings.

In EVL-2026-002, we found that FHFA did not consistently comply with policies and procedures for paying employee reimbursements and stipends. In general, we identified instances in which payments were (1) unsupported by required documentation or in violation of policy; (2) made to ineligible employees or those without required, approved agreements; and (3) disbursed without confirmation of accuracy. We also found that FHFA did not consistently comply with records retention and management requirements. As a result, we questioned costs totaling $65,690 that violated the Agency's policies and procedures governing the expenditure of funds. Of this amount, $9,580 were unsupported costs. FHFA agreed with all of our nine recommendations to address our findings.

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 with the potential to affect the Agency and its regulated entities. These investigations are conducted in strict accordance with professional guidelines issued by the Attorney General of the United States and the standards established by the Council of the Inspectors General on Integrity and Efficiency for investigations, which are known as the *Quality Standards for Investigations*.

The Office of Investigations is comprised of highly trained special agents and digital and investigative analysts, supported by attorney advisors in the Office of Counsel. We maximize the impact of our criminal and civil law enforcement efforts by working jointly 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, and, in some instances, cases involving banks that are members of the FHLBanks. During the reporting period, OIG's own investigations and its joint investigations with other law enforcement organizations resulted in orders of criminal restitution, fines, special assessments, and forfeitures of more than $255 million.

Notable Criminal Cases

Conspirators Sentenced in Multimillion-Dollar Bank Fraud Scheme, North Carolina

In the Western District of North Carolina, during this reporting period, four conspirators were sentenced to prison for their roles in a multimillion-dollar bank fraud scheme. The scheme participants and sentences were:

- Scheme leader Kotto Paul - 180 months in prison, five years of supervised release, and ordered to pay more than $10 million in restitution, jointly and severally, and $8 million in forfeiture.

- Latoya Ford - 27 months in prison, three years of supervised release, and ordered to pay more than $8 million in restitution, jointly and severally.

- Bruce Marko - 12 months and one day in prison, two years of supervised release, and ordered to pay more than $1.5 million in restitution, jointly and severally, and $264,500 in forfeiture.

- Love Norman - time served, two years of supervised release including one year of home confinement, and ordered to pay over $2 million in restitution and $430,473 in forfeiture.

According to court records, at least seven conspirators executed this scheme that defrauded no fewer than 17 federally insured financial institutions, including several FHLBank member banks, of more than $17 million in fraudulent loans. Members of the conspiracy closed on at least 42 loans, many of which defaulted.

Paul, the leader and primary beneficiary of the fraud conspiracy, relied on a network of scheme participants to prepare and submit the fraudulent loan applications that included material misrepresentations supported by fabricated documentation such as false income and employment information, financial statements, bank statements, and tax returns. The fraudulent loans included business loans purportedly for the purchase of equipment, land development, and residential mortgages.

The defendants used the loan proceeds to purchase real estate, cover unrelated business expenses, make investments, make payments toward earlier loans, and pay for personal expenditures contrary to the stated purposes of the loans in the applications.

Former Investment Advisor Sentenced in Bank Fraud Scheme, Nebraska

On October 30, 2025, in the District of Nebraska, Jesse Hill was sentenced to 60 months in prison, five years of supervised release, and ordered to pay over $37 million in restitution for his role in a bank fraud scheme that attempted to obtain over $45 million in loans from over

20 different financial institutions, including 15 member banks of the FHLBank system.

According to court records, Hill and his conspirator attempted to obtain more than $45 million in loans from financial institutions, many of which are members of the FHLBank system. Hill was an investment advisor that had organized and controlled multiple investment entities over a nine-year period. Hill's conspirator, who passed away in November 2022, operated a real estate business.

In 2020, Hill began seeking loans from financial institutions in the name of the conspirator or the conspirator's entities. It was represented that these loans were for real estate investments and the alleged collateral for the loans was a fictious investment account that was managed by Hill. Hill and his conspirator would grant a surety with the financial institution, typically in the form of a control agreement, a commercial security agreement, or an assignment of account. Hill would falsely claim that the collaborator or their entity were clients through his investment business and prepare and present fraudulent invoices to the financial institutions. Hill would falsely represent values of alleged funds and that no other financial institution had a security interest in these fictitious accounts. Most of the fraudulently obtained funds went to a failed investment scheme.

A portion of the fraudulent loan proceeds were used to pay off or pay down fraudulent loans obtained earlier in the scheme. Proceeds were also deposited into a Charles Schwab account used to purchase property in Puerto Rico and an ownership interest in a PC-12/47E Pilatus Aircraft.

Fraud Ringleader and Conspirators Sentenced in Loan Fraud Scheme, Maryland

During this reporting period, in the District of Maryland, three conspirators were sentenced for their roles in a scheme intended to obtain more than $35 million in commercial real estate loans from financial institutions, including FHLBank member banks, by providing false documentation in support of Small Business Administration (SBA) loan applications for the purchase of hotels.

- Conspiracy ringleader Mehul Khatiwala was sentenced to 84 months in prison, five years of supervised release, and ordered to pay over $6 million in restitution, jointly and severally, $6 million in forfeiture, and a $100,000 fine.

- Project Coordinator Jennifer Watkins was sentenced to 36 months in prison, three years of supervised release, and ordered to pay more than $6 million in restitution, jointly and severally.

- Settlement Agent Rebecca Cohn was sentenced to time served and two years of supervised release.

Court records revealed the aforementioned participants and others conspired to obtain loans to buy and sell hotels in a hotel flipping scheme by making material misrepresentations and omissions to financial institutions during the loan application process. These misrepresentations included the identity of the sellers, the familial relationships between the parties, and the nature and amount of the equity injected by the borrowers under the SBA's Section 7(a) Program.

Khatiwala's conviction and sentencing in this case represent the second time he has been held accountable for criminal activity as the result of an FHFA-OIG investigation. That investigation led to the indictment and conviction of Khatiwala on charges involving schemes to fraudulently obtain approximately $15 million in bank loans to purchase a multifamily residential property and hotels. His first conviction resulted in a sentence of 63 months in prison, four years supervised release, and ordered to pay over $3.5 million in restitution and forfeiture.

Real Estate Broker Sentenced in Origination Fraud Scheme, Florida

On April 30, 2025, in the Middle District of Florida, Maria Del Carmen Montes was sentenced to 33 months in prison, five years of supervised release, and ordered to pay $103,337 in restitution and $15,636 in forfeiture for her role in a loan origination scheme targeting financial institutions that included loans owned by the Enterprises.

According to court records, Montes referred potential homebuyers to a mortgage company. She then created, or caused to be created, fictitious paystubs, false verifications of employment, falsified income information, and other fabricated documents using the buyers' means of identification to induce the mortgage company to approve loans for unqualified clients. Montes also recruited another to facilitate false verifications of employment.

Montes received real estate commission payments from the deceptive mortgage loan transactions and collected cash payments from buyers.

Former Bank Chief Financial Officer Found Guilty in Bank Fraud Scheme, Nebraska

On March 6, 2026, in the District of Nebraska, after a nine-day trial, a federal jury convicted Aaron Luneke of attempted bank fraud and bank fraud for his role in a scheme that victimized two FHLBank member banks.

According to court records and evidence presented at trial, Luneke was the Chief Financial Officer of Bank of the Valley from 2018 to 2022. He was also the co-owner of Living Waters RE, LLC (Living Waters), a company created to build and operate a carwash. Luneke attempted to use fraudulent and inflated invoices from a general contractor and an electrician to increase the valuation of Living Waters to obtain a $3.5 million loan from Stearns Bank on behalf of Living Waters. He also failed to report outstanding debts to family members in his loan application.

Additionally, Luneke used fraudulent and inflated invoices from a general contractor and an electrician as a basis for additional construction proceedings when applying for interim financing for Living Waters in the form of two loans totaling over $4.3 million from Bank of the Valley.

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 55.6 million single-family loans since its inception in 1934.[9] FHA reported that in fiscal year (FY) 2025, it served a total of 876,502 forward mortgage borrowers.[10] This included 648,764 purchase mortgages with over 83 percent going to first-time home buyers. In FY 2025, FHA endorsed a total of $274.76 billion in forward mortgages, which was a moderate increase from FY 2024. FHA's portfolio also included 3,893 insured residential care facilities and 82 hospitals.[11] As of October 2025, FHA had a combined insurance portfolio valued at $1.64 trillion.[12] 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

[9] https://www.hud.gov/sites/dfiles/Housing/documents/FHAFY2025ANNUALMGMNTRPT.PDF, p. 8
[10] https://www.hud.gov/sites/dfiles/Housing/documents/2025FHAAnnualReportMMIFund.pdf, p. 24
[11] https://www.hud.gov/sites/dfiles/Housing/documents/FHAFY2025ANNUALMGMNTRPT.PDF, pp. 29-30
[12] https://www.hud.gov/sites/dfiles/Housing/documents/2025FHAAnnualReportMMIFund.pdf, p. 60

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 2025, Ginnie Mae issued $526.4 billion in MBSs, pushing the total MBS outstanding to a historic high of $2.8 trillion.[13]

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 which are highlighted in our Top Management Challenges for FY 2026 report. Of note, in the current report, we removed the challenges most related to the financial sector.

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 has four priority open recommendations related to the financial sector:

Report and Recommendation Number	Recommendation	Status
2017-KC-0001 FHA Paid Claims for an Estimated 239,000 Properties That Servicers Did Not Foreclose Upon or Convey on Time Recommendation 1A	Issue a change to regulations at 24 CFR Part 203, which would avoid unnecessary costs to the FHA insurance fund, allowing an estimated $2.23 billion to be put to better use. These changes include (1) a maximum period for filing insurance claims and (2) disallowance of expenses incurred beyond established timeframes.	To fully address this recommendation, HUD must publish the FHA Maximum Claim Rule. Implementation of this rule should result in HUD putting $2.23 billion to better use.

[13] https://www.ginniemae.gov/about_us/what_we_do/Annual_Reports/annual_report25.pdf, p. 16

2018-KC-0001 FHA Insured $1.9 Billion in Loans to Borrowers Barred by Federal Requirements Recommendation 1A	Develop a method for using the Do Not Pay portal during the underwriting process to identify delinquent child support and delinquent Federal debt to prevent future FHA loans to ineligible borrowers to put $1.9 billion to better use.	To fully address this recommendation, HUD must provide evidence that it has implemented applicant screening against the Do Not Pay portal to identify delinquent child support and delinquent federal debt to prevent future FHA loans from going to ineligible borrowers. Implementation of this rule should result in HUD putting $1.9 billion to better use.
2018-LA-0007 HUD Paid an Estimated $413 Million for Unnecessary Preforeclosure Claim Interest and Other Costs Due to Lender Servicing Delays Recommendation 1A	Implement a change to regulations at 24 CFR Part 203 to require curtailment of preforeclosure interest and other costs that are caused by lender servicing delays, resulting in $413,513,975 in funds to be put to better use. This should include updating or seeking statutory authority to update HUD's regulations as necessary and coordinating with HUD's Office of Finance and Budget, well before any changes go through departmental clearance, to ensure that planned curtailment requirements can be consistently enforced through the claims process.	To fully address this recommendation, HUD must provide evidence that it has published and adopted the rule. Implementation of this rule should result in HUD putting $413 million to better use.
2019-KC-0003 FHA Insured at Least $13 Billion in Loans to Ineligible Borrowers With Delinquent Federal Tax Debt Recommendation 1A	Require lenders to obtain the borrowers' consent to verify the existence of delinquent Federal taxes with the Internal Revenue Service during loan origination and deny any applicant with delinquent Federal tax debt and no payment plan or a noncompliant payment plan or an applicant refusing to provide consent from receiving FHA insurance to put at least $6.1 billion to better use by avoiding potential future costs to the FHA insurance fund.	To fully address this recommendation, HUD will need to provide evidence that it established a method of borrower consent to verify the existence of delinquent federal taxes including, but not limited to one of the options OIG provided, which were (1) lenders obtaining the borrowers' consent to obtain their tax records directly from the IRS or (2) borrowers accessing their own tax information and submitting it to the lenders. Implementation of this rule should result in HUD putting $6.1 billion to better use.

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

HUD OIG Oversight Related to the Financial Sector

For the period April 1, 2025, through March 31, 2026, HUD OIG completed the following key oversight reports related to the financial sector.

HUD's Office of Single Family Housing Did Not Consistently Monitor Its Field Service Management Contractors' Property Preservation and Protection Services

HUD OIG conducted an audit to assess how HUD monitors its Field Service Management (FSM) contractors' property preservation and protection services. The audit found that HUD's Office of Single Family Housing did not consistently monitor its FSM contractors' property preservation and protection services. Specifically, HUD provided inconsistent monitoring for 34 of the 79 statistically sampled records reviewed, and these involved discrepancies between HUD's assessment, the support, and the performance work statement. HUD did not develop and apply a clear and uniform review framework to ensure that its process and procedures provided for effective FSM contract monitoring. As a result, HUD (1) could not ensure its REO inventory was being maintained in an adequate condition and (2) was not aware of whether contracting actions were needed to address deficient performance. HUD OIG made three recommendations to assist HUD in enhancing its FSM monitoring process. **(HUD OIG Report, 2025-KC-0002, Single Family Housing)**

Potential Fraud Risks and Schemes for HUD's Single Family Housing Program

Beginning in 2021, HUD OIG conducted several audits to assess HUD's anti-fraud efforts and to develop inventories of fraud risks for several of its programs. This previous work found that HUD's fraud risk management program was in its early stages of development and HUD OIG recommended that HUD perform program-specific fraud risk assessments and incorporate these assessments into an agency-wide plan to further advance its program. To continue assisting HUD in improving its anti-fraud efforts, HUD OIG conducted this work to identify potential fraud risks and schemes that could negatively impact HUD's Single Family Housing program. The objective was to assist HUD by developing an inventory of fraud risks for its Single Family Housing program. As part of a larger effort by the HUD Office of Housing Operational Risk Division that included developing fraud risk inventories for all components of the Office of Housing, HUD created a fraud risk inventory for the Single Family Housing program that identified 28 fraud risks or schemes and covered many aspects of the program including appraisal, application, origination, servicing, invoices, and claims. HUD OIG identified five overall fraud risk factors that increase the chance of fraud occurring in the program by increasing the incentive, opportunity, and likelihood for an individual considering committing fraud. HUD OIG used these fraud risk factors, along with the results of brainstorming sessions, interviews, and reviews of audit reports, investigations, and press releases from HUD OIG and other agencies, to develop an inventory of 64 potential fraud schemes that HUD had not previously identified. These schemes could be used to defraud the Single Family Housing program and undermine its integrity, resulting in an increased risk to the FHA insurance fund, borrowers, and lenders. HUD OIG made three recommendations to assist HUD in enhancing

its program specific fraud inventory and oversight of the Single Family Housing program and progressing its anti-fraud maturity. **(HUD OIG Report, 2026-KC-0001, Single Family Housing)**

Ginnie Mae Did Not Formally Assess Rising Nonbank Concentration Risk

HUD OIG conducted an audit of Ginnie Mae's management of its portfolio of federally guaranteed MBS. HUD OIG initiated this audit because of its internal monitoring of the Ginnie Mae portfolio as well as the issuance of a Financial Stability Oversight Council report in 2024 on the rising risks presented by nonbank mortgage companies. The audit objective was to assess Ginnie Mae's evaluation of nonbank issuer concentration risk. The audit found that Ginnie Mae's portfolio experienced a rise in nonbank concentration risk. Specifically, a few nonbank mortgage companies hold a large percentage of Ginnie Mae's portfolio of guaranteed MBS. However, Ginnie Mae does not formally assess whether the risk impacts its operations, existing internal controls, or its ability to meet its agency goals. If this continues, it could complicate Ginnie Mae's ability to effectively monitor or respond to any failures of the largest nonbank mortgage companies. HUD OIG recommended that the President of Ginnie Mae perform an assessment of concentration risk and take appropriate action based on the results. **(HUD OIG Report, 2026-KC-0002, Government National Mortgage Association)**

Audit of Government National Mortgage Association's Fiscal Years 2025 and 2024 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, 2025 and 2024, 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, 2025 and 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 2025 in internal control over financial reporting, based on limited procedures performed; and no reportable noncompliance for fiscal year 2025 with provisions of applicable laws, regulations, contracts, and grant agreements or other matters. **(HUD OIG Report, 2026-FO-0001, Government National Mortgage Association)**

Audit of FHA's Fiscal Year 2025 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 year ending September 30, 2025, 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, 2025, were presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles; one material weakness for fiscal year 2025 in internal control over financial reporting, based on limited procedures performed; and no reportable noncompliance for fiscal

year 2025 with provisions of applicable laws, regulations, contracts, and grant agreements or other matters. **(HUD OIG Report, 2026-FO-0003, 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, 2025, through March 31, 2026, HUD OIG Office of Investigation completed 23 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 $16 million (criminal, civil, and administrative recoveries). During this reporting period, HUD OIG also coordinated with the HUD Departmental Enforcement Center (DEC), resulting in five suspensions and five debarments for single-family investigations. These efforts strengthen the resilience of the housing finance system and support the broader objectives of the Financial Stability Oversight Council by promoting the safety, soundness, and stability of the U.S. financial system and reduce risks that could threaten system integrity. The following are significant investigative cases involving financial fraud:

Hampton Woman Pleads Guilty to $161 Million Mortgage Fraud Scheme

On April 11, 2025, an elementary school secretary and assistant bookkeeper was sentenced in U.S. District Court for the Northern District of Georgia for conspiracy. From August 2019 to January 2023, the defendant, in coordination with others, fabricated and submitted false financial documents—including bank statements, pay stubs, and IRS Forms W-2—to mortgage lenders for loan approval. The defendant produced fabricated documents for approximately 452 mortgage loans, including approximately 180 FHA-insured mortgages. Many of the FHA-insured loans remain in default, with partial claims paid by HUD totaling $1,748,066 million. The elementary school secretary and assistant bookkeeper was sentenced to 26 months in prison and ordered to pay restitution of $1,833,828.23 million with $1,748,000 million due to the FHA.

Real Estate Investor, His Company, and an Employee Sentenced for Defrauding Financially Distressed Homeowners and Financial Institutions

On June 9, 2025, a real estate investment firm, the company's owner, and an employee of the real estate investment firm were sentenced in U.S. District Court for the District of Rhode Island for defrauding financial institutions, the FHA, and homeowners. The defendants used a variety of short sale fraud schemes resulting in losses exceeding $1 million, of which $850,000 were losses to the FHA. The defendants were collectively sentenced to 12 months and 1 day in prison, 6 years of supervised release, 1 year of probation, and ordered to pay restitution of $102,692.

Kissimmee Real Estate Broker Sentenced For Bank Fraud

On April 30, 2025, a realtor was sentenced in U.S. District Court for the Middle District of Florida for bank fraud. The defendant created fictitious pay stubs for companies as proof of employment verification, using the buyers' identification to deceive the mortgage company into approving fraudulent loans. Some of the paystubs the defendant created falsely represented that the borrower was employed by a company that her husband controlled. To further the scheme, the defendant's husband submitted false verification of employment documents in the names of buyers under the pretense that they worked for his business, although they did not. As a result, 20 FHA-insured mortgages were affected by this scheme, as well as 2 additional properties that were insured by another financial institution. The realtor was sentenced to 33 months in prison, 60 months supervised release and ordered to pay a $10,000 fine and $103,337.87 in restitution. The overall investigation led to three defendants being cumulatively sentenced to 33 months in prison, 100 hours of community service, 60 months of probation, 96 months of supervised release, and ordered to pay $30,000 in fines and $103,337.87 in restitution.

Ringleader sentenced in multimillion-dollar fraud operation which saddled victims with crushing debt

The CEO of a fraudulent credit card company was sentenced to 121 months in prison for leading a nationwide mortgage and loan fraud scheme that saddled victims with significant debt. The scheme relied on falsified loan applications, shell companies, straw buyers, and fraudulent pandemic relief claims, resulting in millions of dollars in losses. During this reporting period, seven defendants were sentenced to a combined total of nearly 23 years in prison and ordered to pay $1.8 million in restitution. Of the 17 individuals charged, 16 have been convicted and collectively sentenced to nearly 29 years in prison, with more than $3 million in total restitution ordered.

Additional Investigative Cases Related to the Financial Sector

- Clermont Man Pleads Guilty To Conspiracy To Commit Bank Fraud | Office of Inspector General, Department of Housing and Urban Development (May 9, 2025)
- Suburban Houston woman charged with wire fraud, assaulting officer and threatening to kill a witness (October 20, 2025)

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 Inspector General Act of 1978, as amended (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 an in-depth review.

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
- Implementation of Artificial Intelligence
- Agency Restructuring

We issued audit reports that could relate to the broader financial sector, including an audit of whether the NCUA effectively used cyber threat information for the supervision of credit unions and implemented effective processes to share cyber threat information to support credit union and financial system resiliency. Our audit determined that the NCUA needed to mature its processes for cyber threat information sharing to support supervision of credit unions more effectively during a cybersecurity event or incident that could increase risk to the National Credit Union Share Insurance Fund and financial services sector stability. We also determined that the NCUA should improve its ability to acquire, analyze, and use cyber threat information for internal analysis and external response.

A second audit that could relate to the broader financial sector was our audit of the NCUA's information technology (IT) asset sanitization process. Our audit determined that the NCUA adequately sanitized its IT assets before disposal or reuse. However, we determined that the NCUA should make improvements to its IT asset accountability process because the process did not include a clear chain of custody and other controls.

In addition, we participated in the Council of Inspectors General for Financial Oversight working group that conducted an audit of the Financial Stability Oversight Council's designation of nonbank financial companies.

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

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

Background

The SEC's mission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. The SEC strives to promote capital markets that inspire public confidence and provide a diverse array of financial opportunities to retail and institutional investors, entrepreneurs, public companies, and other market participants.

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 Act), 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 25 functional offices.[14] The Agency's headquarters are in Washington, DC, and it has 10 regional offices located throughout the country. As of March 31, 2026, the SEC employed 3,950 full-time equivalent employees.

[14] Including the Office of Inspector General.

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, evaluations, and other reviews of the SEC's programs and operations at its headquarters and 10 regional offices. These engagements 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 is a federal law enforcement component responsible for investigating significant matters of criminal, civil, and administrative wrongdoing and misconduct relating to SEC employees, contractors, programs, and operations, including SEC-regulated markets. 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 the Dodd-Frank Act 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.

During this reporting period, the SEC OIG launched a Cash Awards Program to encourage all SEC employees to help identify potential fraud, waste, or mismanagement within the agency. Under **5 U.S.C. § 4512**, employees may receive **up to $10,000** when information they provide results in significant cost savings for the agency.

SEC OIG Work Related to the Broader Financial Sector

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

Completed Work, April 1, 2025-March 31, 2026

Audit of the Division of Corporation Finance's Disclosure Operations

Companies that offer securities, such as stocks or bonds for public sale, must truthfully disclose information about those securities and associated risks. To protect investors and facilitate capital formation, the Disclosure Review Program (DRP) in the SEC Division of Corporation Finance selectively reviews the disclosures—typically the annual reports—of more than 7,400 companies required to regularly file financial reports with the SEC. The DRP reviews each company's annual report at least once every three years or more often based on risk factors. The DRP also selects transactional filings for review. We conducted this audit to assess whether the DRP (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.

Although the DRP has a risk-based process for selecting and reviewing filings and met its statutory requirement for reviewing filers' financial statements during the period we reviewed, documentation of and guidance on the annual report selection and scoping processes were lacking. Documenting how and why the DRP selects and scopes its reviews is important for investor protection because it ensures that the DRP appropriately considers and incorporates risk into its decision-making by providing transparency that would contribute to effective oversight. Federal internal control standards also support the need for and value of documentation. Yet, in fiscal years 2023 and 2024, it was often unclear why DRP staff selected companies for elective annual report reviews and how staff decided to scope both required and elective reviews. Staff documented information inconsistently due to a lack of comprehensive guidance in selecting annual reports for elective review and documenting the scope for both required and elective reviews. Additionally, internal guidance (in draft form since May 2017) did not address five of the six risk factors the SEC must consider when selecting companies to review. The guidance includes the DRP's interpretation of the minimum review period, which should also be finalized.

Changes in the DRP workforce may lead to a loss of institutional knowledge, and potential new rules related to crypto assets and other issues may create additional disclosure requirements warranting the DRP's attention. Further, the current regulatory environment may increase new issuer transactional filings. Improved documentation and guidance related to key DRP selection and scoping decisions can help management face these challenges and ensure the DRP uses a risk-based process to make the best use of its limited resources. Accordingly, we recommended that DRP management:

- Require that important information about how annual reports are selected for elective review and scoped, including any relevant risk factors, be documented, among other actions.
- Coordinate with the SEC's Office of the General Counsel to finalize Sarbanes-Oxley Act of 2002 section 408 guidance, including a description of all six factors to be considered and an interpretation of the minimum review period mandate.
- Consider developing a plan that prioritizes DRP goals and requirements in the event of significant staffing decreases and/or significant workload increases.

We also inquired about automating aspects of the DRP. While we did not make formal recommendations related to this topic, we encouraged management to continue considering opportunities and to leverage available resources to implement automation where feasible and advisable. Finally, we identified a potential opportunity to consolidate the SEC's disclosure review information technology systems. Because the matter was outside the scope and objectives of this audit, we reported it separately.

We issued our final report addressing these topics on August 26, 2025. Management concurred with our three recommendations. The report is available on our website at https://www.sec.gov/files/sec-oig-aud-report-586.pdf.

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

The SEC regulates the securities markets and, like other federal agencies, must generally notify the public of its proposed rules, assess the economic implications of its rulemaking, and consider comments received. In October 2022, we reported an overall increase in SEC rulemaking activities, and we identified associated risks and challenges.

We conducted this audit to assess aspects of the SEC's rulemaking process and related internal controls. Specifically, we reviewed 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 efficiency, competition, and capital formation. We also reviewed SEC actions to ensure staff with sufficient and appropriate skills, experience, and expertise are involved in formulating and reviewing proposed rules.

We reviewed SEC rulemaking activities from January 2018 through December 2022, assessed a sample of 24 rules proposed and/or finalized during that time, and surveyed 647 knowledgeable managers and staff and found that, overall, the SEC defined processes for (1) giving interested persons an opportunity to participate in rulemaking; (2) assessing and documenting the impact(s) of proposed rules on efficiency, competition, and capital formation; and (3) ensuring that staff with sufficient and appropriate skills, experience, and expertise are involved in formulating and reviewing proposed rules. Nonetheless, information we gathered warranted management's attention as the SEC assessed newly issued federal directives and their impact on the rulemaking of historically independent regulatory agencies, such as the SEC.

Specifically, we determined that the SEC provided a comment period ranging from 30 to 92 days for rules issued during the period we reviewed. And, in accordance with SEC internal guidance, SEC rulemaking divisions consistently collaborated with the Division of Economic and Risk Analysis and the Office of the General Counsel. However, other SEC divisions and offices were not always involved in rulemakings within their subject matter expertise.

Additionally, for each of the 24 rules in our sample, the SEC assessed the impact(s) on efficiency, competition, and capital formation. Nonetheless, some SEC staff expressed concerns about limited data and time to perform economic analyses.

Finally, before December 2024, the SEC had not performed an agencywide assessment of the knowledge, skills, and competencies of its rulemaking staff. In addition, non-federal personnel who worked at the SEC under Intergovernmental Personnel Act (IPA) agreements, and who were involved in rulemaking, performed unauthorized supervisory functions. During our audit, the SEC finalized a rulemaking competency study and corresponding dashboard and, as of March 2025, the SEC no longer had IPA personnel onboard.

We also reviewed two matters that were not directly related to our audit objectives but that we discussed with agency officials. These matters involved technological errors that impacted the SEC's receipt of public comments, and SEC personnel releasing embargoed rulemaking information without authorization from the Commission.

The SEC took actions during our audit that addressed some of our concerns. More changes may come from the newly issued federal directives discussed in our final report. Although we did not make formal recommendations, we encouraged management to consider whether additional actions are required to address our observations.

We issued our final report addressing these topics on September 29, 2025. The report is available on our website at https://www.sec.gov/files/sec-oig-aud-report-588.pdf.

Ongoing Work as of March 31, 2026

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 May 2026.

Evaluation of the Division of Enforcement's Collection and Distribution of Disgorgements and Penalties

We have initiated an evaluation to determine whether the Division of Enforcement has processes and procedures that ensure timely, efficient, and effective collections of delinquent disgorgements and penalties and disbursements of funds to harmed investors. The evaluation scope will include a review of collections and distributions data covering fiscal year 2021 through fiscal year 2025.

We expect a report will be issued before the end of FY 2026.

Evaluation of the Office of the Ombuds' Handling and Reporting of Investor Concerns

We have initiated an evaluation to determine whether the Office of the Ombuds appropriately handles and accurately reports matters submitted by investors, market participants, and other stakeholders. We will also evaluate actions taken in response to a management letter we issued in 2021. The evaluation scope will include a review of matters reported to the Office of the Ombuds between October 1, 2023, and September 30, 2025.

We expect a report will be issued before the end of FY 2026.

Evaluation of the EDGAR Business Office's Review Processes

We have initiated an evaluation to determine whether the EDGAR Business Office has effective processes for (1) reviewing requests to submit filings electronically in EDGAR, and (2) promoting the reliability and integrity of filers' submissions. The evaluation will include EDGAR Business Office activities from October 2023 through May 2025.

We expect a report will be issued before the end of FY 2026.

Audit of the Office of the Chief Accountant's Accounting Consultations Process

We have initiated an audit of the Office of the Chief Accountant's accounting consultations process. We will assess whether the process ensures comprehensive reviews (including consideration of past consultations), transparency, and coordination with relevant SEC divisions and offices and external parties, as appropriate. We will also determine whether the Accounting Group performs consultations in a timely manner, in accordance with its policies and procedures, and complies with ethics and information security requirements. The audit will include Accounting Group consultations and activities from fiscal year 2023 through the third quarter of fiscal year 2025.

We expect a report will be issued before the end of FY 2026.

Investigative Accomplishments

The SEC OIG Office of Investigations, OIG's law enforcement component, investigates significant matters of criminal, civil, and administrative wrongdoing and misconduct relating to SEC employees, contractors, programs, and operations, including SEC-regulated markets. 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 and mission integrity; involving public corruption related to the SEC; or implicating major fraud associated

with SEC programs, operations, and personnel. We work closely with other Council of Inspectors General for Financial Oversight (CIGFO) investigative offices and law enforcement counterparts outside CIGFO to hold bad actors accountable or exonerate those falsely accused of wrongdoing. Recently three of our special agents entered into Joint Duty Assignments with the Federal Bureau of Investigation's headquarters-based Economic Crimes Unit.

Select Recent Financial Sector and Related Investigative Results

California immigration lawyer was sentenced to 30 months in prison for large-scale visa fraud and obstruction of an SEC investigation

In January 2026, a California woman who was previously extradited from the Kyrgyz Republic to the United States, was sentenced to 30 months in prison, 2 years of supervised release, and a $20,000 fine based on charges 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.

Hong Kong Businessman Indicted for Role in Filing False SEC Investment Adviser Forms on behalf of Sham Entities Used in Ramp-and-Dump Scheme

On November 14, 2025, A federal grand jury in the District of Columbia returned an indictment charging a Hong Kong man for his role in a conspiracy to file false and deceptive investment adviser forms with the SEC for at least 10 shell business entities that he and co-conspirators created. The false forms gave the impression that the entities were legitimate financial advisers, though they were sham entities. At least two of these false entities were then used to induce retail investors through social media and WhatsApp chats to purchase the stock of Chinese companies listed on Nasdaq.

South Carolina man sentenced to 13 years for $13M Ponzi scheme and cyber stalking

In August 2025, a South Carolina man was sentenced to 13 years in federal prison for operating a multimillion-dollar Ponzi scheme and for stalking two social media content creators. He was also ordered to pay more than $14 million in restitution.

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 (herein "Treasury" or "the Department") 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 1,010 financial institutions.

Background

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. 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 730 national banks, 231 federal savings associations, and 49 federal branches and agencies of foreign banks. The total assets under OCC's supervision are $16.7 trillion.[15] Treasury OIG also oversees four offices created by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) which are (1) the Office of Financial Research, (2) the Federal Insurance Office, (3) the Office of Minority and Women Inclusion within Treasury's Departmental Offices, and (4) the Office of Minority and Women Inclusion within OCC.

Treasury OIG is also responsible for audit and investigative oversight of Treasury programs providing financial assistance to address the economic impacts of the Coronavirus Disease 2019 (COVID-19). Since March 2020, more than $650 billion of financial assistance, overseen by

[15] OCC, *2025 Annual Report* (Jan. 2026), p. 13

Treasury OIG, has been authorized by Congress. Treasury established the Office of Recovery Programs, 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. As Treasury's pandemic-related programs near completion, Treasury OIG's oversight and coordination efforts will correspondingly decline during fiscal year (FY) 2026.

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

In accordance with the Reports Consolidation Act of 2000, the Treasury Inspector General annually provides the Secretary of the Treasury with his perspective on the most serious management and performance challenges facing the Department. In a memorandum to the Treasury Secretary dated December 4, 2025, the Deputy Inspector General reported five management and performance challenges that were directed towards financial regulation and economic recovery.[16] Those challenges are discussed below and include: (1) Resource Optimization; (2) Cyber Threats; (3) Artificial Intelligence (AI) Adoption; (4) Anti-Money Laundering/Terrorist Financing and Bank Secrecy Act Enforcement; and (5) Crypto and Digital Assets Growth. The memorandum also reported concerns about streamlining access to Do Not Pay (DNP) data sources and the ongoing management of the COVID-19 pandemic relief programs.[17]

Challenge 1: Resource Optimization

In assessing the Department's most pressing challenges, it is essential to consider both external factors and future uncertainties that may significantly impact operations. These include, but are not limited to, staff reductions, funding cuts, challenges related to recruiting and retaining qualified personnel, and the ability to meet the Administration's priorities.

Staff and funding cuts have the potential to streamline processes and generate cost savings but may also undermine the Department's operational resilience. The recent retirements and deferred resignations of many experienced personnel across Treasury bureaus and offices have created a significant human capital gap, including the loss of institutional knowledge and continuity, which threatens the Department's ability to fulfill its mission. Budget constraints continue to restrict hiring and recruitment. While exemptions remain for certain critical positions in law enforcement and national security, the Department must still operate under

[16] Treasury OIG, *Management and Performance Challenges Facing the Department of the Treasury,* OIG-CA-26-005 (December 4, 2025)

[17] The Treasury Deputy Inspector General's memorandum included two other concerns not directly related to financial regulation and economic recovery: United States Mint gold acquisitions and Bureau of Engraving and Printing's construction of a new facility.

reduced staffing levels, which may increase workloads, delay implementation of critical initiatives, and reduce Treasury's agility in addressing emerging issues.

The Department also continues to face significant difficulties in attracting and retaining skilled personnel, particularly in specialized areas such as financial analysis, information technology, cybersecurity, regulatory compliance, manufacturing trades and crafts, and police officers (for the Bureau of Engraving and Printing (BEP) and the United States Mint). Contributing factors include competitive labor market conditions, federal compensation limitations, and constrained advancement opportunities. The lack of specialized expertise increases the risk of operational inefficiencies, security vulnerabilities, and non-compliance with laws and regulations. If these challenges are not addressed, the Department will continue to struggle with talent shortages that could hinder its ability to meet increasingly complex operational demands, adapt to evolving policy priorities, and maintain secure and efficient systems.

In the face of these challenges, the Department remains committed to advancing the Administration's goals and is focusing on efforts to improve the efficiency and effectiveness of operations, as it reshapes and optimizes the Treasury workforce by improving processes and enterprise decision-making, and streamlining human capital management through centralization and standardization. To this end, Treasury OIG will evaluate the Department's efforts to create operational efficiencies and generate cost savings while balancing limited resources, reduced staff, and competing mission demands as it executes the Administration's priorities.

Challenge 2: Cyber Threats

Cybersecurity remains a long-standing and serious challenge facing the Nation and continues to be reported by the Government Accountability Office (GAO) as a government-wide issue in its 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 are an ever-present 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 these 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 be nimble and reinforce and/or redirect cybersecurity efforts to address unforeseen events when they arise, such as when serious flaws are discovered in software or systems that place Treasury's information and systems at risk of compromise.

Threat actors frequently probe trusted connections for weaknesses to exploit vulnerable networks or systems and gain access to government systems, leveraging vulnerabilities and varying their methods to disguise their attacks and make detection and prevention difficult.

[18] GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness,* GAO-25-107743 (February 25, 2025)

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 establish a foothold to enable future actions against the Department or those connected to the Department. Through information sharing, federal agencies are better prepared to thwart potential attacks on the cyber infrastructure of the Federal Government and the financial sector.

As the tools used to perpetrate cyber-attacks continue to become easier to use and more widespread, the technological knowledge and resources needed to launch attacks decrease and the chances of successful attacks increase. AI is increasingly used to support and create more realistic social engineering attacks (phishing emails, deepfake voices and videos) and programs that find and/or exploit vulnerabilities with minimal effort on the attacker's part. In addition, supply chain security remains a concern for both software and hardware.

Efforts to address these cybersecurity concerns at the federal level include Executive Order (EO) 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 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 9, 2025, this EO was extended for 1 year.[19] Further, EO 14028, *Improving the Nation's Cybersecurity*, calls for federal agencies to, among other things, update existing plans to prioritize resources for adoption and use of cloud technology and to adopt a zero-trust architecture.[20] EO 14144, *Strengthening and Promoting Innovation in the Nation's Cybersecurity*, mandates software providers selling to the U.S. Government prove they are using secure development practices. These EOs were amended and enhanced by EO 14306, *Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144*. To achieve the goals outlined in EO 14028, the Office of Management and Budget (OMB) issued M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* to provide the strategy for achieving a zero-trust architecture, and require agencies to meet specific cybersecurity standards and objectives by the end of FY 2024. OMB also issued M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* requiring agencies to only use software that complies with secure software development standards. The Department must not only stay on top of developments in cybersecurity, but also with federal requirements as those in turn adapt to the ever-shifting cybersecurity threat environment.

[19] *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain* (May 9, 2025)

[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.

Furthermore, as part of prudent policy and as a cornerstone of implementing zero-trust architecture, Department 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 are also risks to Treasury's networks and systems, due to necessary interconnections to conduct business with service providers and federal, state, and local agencies. Management must continue to monitor the overall threat environment, exercise due care evaluating and authorizing 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 must also ensure that critical data and information maintained by third-party service providers are properly protected.

The financial sector and its institutions look to Treasury for effective leadership in the fight against cyber threats. As such, effective public-private coordination is essential to the Nation's financial infrastructure 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's critical infrastructure and reduce operational risks including those 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.[21] In 2018, GAO reported[22] that the extent of adoption of the NIST framework by critical infrastructure sectors was unknown and 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. According to GAO, as of April 2025, Treasury's Financial Services Sector Risk Management Plan includes a line of effort aimed at promoting adoption of financial services sector-specific goals, which may correlate with aspects of the NIST cybersecurity framework; however, GAO noted Treasury did not identify steps it has taken in collaboration with sector partners to develop methods for determining adoption of NIST's cybersecurity framework or sector-specific goals that relate to the framework. Treasury's response to GAO stated that there are limitations on Treasury's ability to implement GAO's recommendation, as Treasury cannot compel entities to share cybersecurity framework adoption data and participation is voluntary.

In addition, quantum computing potentially permits hostile actors to attack the public-key cryptography used as the basis of financial services sector and Treasury signature, identity verification, and data encryption. NIST has released new Federal Information Processing

[21] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, February 12, 2014; superseded by Version 1.1; April 16, 2018)

[22] GAO, *Critical Infatuation Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (February 15, 2018)

Standards for Post-Quantum Cryptography.[23] In coordination with the Office of Cyber Security and Critical Infrastructure Protection, the Department acknowledges that all elements of the financial services sector should be urged to transition to these new standards, preferably completing transition by FY 2035.

In response to our 2024 letter, Treasury noted progress towards its cybersecurity and compliance goals, such as encrypting data at rest for nearly all High Value Assets,[24] and all data in transit for Department-wide network traffic. The Department also reported advancements towards zero trust architecture, by expanding its enterprise-wide authentication platform and phishing-resistant multi- factor authentication. The Department plans to overhaul the cyber compliance program to streamline activities, reduce paperwork, and centrally manage risk.

In addressing increases in cyber threats, Treasury will need to continue to balance cybersecurity demands while maintaining and modernizing information technology systems.

Challenge 3: Artificial Intelligence Adoption

AI is rapidly changing how organizations across government and the private sector operate. For the Department, AI represents both an opportunity and a risk. While it offers the potential to improve efficiency, refine analysis, and strengthen oversight, the technology remains an emerging and imperfect tool, with results that depend heavily on the quality of the data it uses. Results derived from AI can sometimes be biased, incomplete, or potentially fabricated. Risks related to information security and privacy increase as agencies adopt and scale AI infrastructure and usage. In addition, AI technology is evolving at a pace that can create challenges for existing policies and oversight structures. These realities make responsible and effective use of AI a significant management challenge for the Department.

Federal leaders have made clear that AI is a national priority. *America's AI Action Plan*[25] calls for innovation that reflects American values, while EO 14179, *Removing Barriers to American Leadership in Artificial Intelligence*, requires agencies to accelerate AI adoption by removing barriers and establishing consistent standards. Earlier guidance, such as EO 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, introduced principles of trustworthy AI, emphasizing accuracy, reliability, and transparency. More recent directives,

[23] The Federal Information Processing Standards are as follows: 203 entitled *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, 204 entitled *Module-Lattice-Based Digital Signature Standard*, and 205 entitled *Stateless Hash-Based Digital Signature Standard.*

[24] High Value Assets are assets, information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the U.S. national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety.

[25] The White House, *Winning the Race: America's AI Action Plan* (July 2025) https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

including EOs on AI education,[26] workforce readiness,[27] unbiased AI principles,[28] and protection of American innovation abroad,[29] reflect how broad and fast-moving the government's priorities in this area have become. Together, these actions underscore that AI is a core responsibility that demands sustained attention.

For Treasury, meeting this responsibility poses unique challenges. The Department must ensure that AI is introduced carefully and used in ways that strengthen, rather than compromise, its mission. That requires clear governance structures, careful oversight of contractors and vendors, and continuous monitoring to ensure AI systems remain accurate and reliable over time. It also means recognizing the limitations of AI and resisting the temptation to treat it as a replacement for human judgment in areas where accountability, fairness, and transparency are essential. Balancing these demands while AI technology continues to evolve will be an ongoing test for the Department.

Without a coordinated and cautious approach, Treasury risks relying on AI systems that produce unreliable results that can undermine public confidence. By following the direction set in *America's AI Action Plan*, related EOs, and OMB guidance,[30,31] the Department has an opportunity to shape AI adoption in a way that improves efficiency while maintaining accountability and trust. Moving forward, Treasury will need to remain vigilant, strengthen its governance capacity, and adapt continuously to the rapid pace of technological change to ensure AI serves the public interest effectively and responsibly.

Challenge 4: 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 national security through intelligence analysis, sanctions, and international private-sector cooperation. As previously reported, identifying, disrupting, and dismantling these networks continues to be challenging as criminals and other bad actors develop increasingly sophisticated money laundering methods to avoid detection.

TFI's authorities are key tools in implementing U.S. policy to pressure foreign countries and regimes, such as Russia and Iran, as well as rogue actors, such as terrorists, narcotics

[26] EO 14277, "Advancing Artificial Intelligence Education for American Youth" (April 23, 2025)
[27] EO 14278, "Preparing Americans for High-Paying Skilled Trade Jobs of the Future" (April 23, 2025)
[28] EO 14319, "Preventing Woke AI in the Federal Government" (July 23, 2025)
[29] EO 14320, "Promoting the Export of the American AI Technology Stack" (July 23, 2025)
[30] OMB M-25-21, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust" (April 3, 2025) www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through- Innovation-Governance-and-Public-Trust.pdf
[31] OMB M-25-22, "Driving Efficient Acquisition of Artificial Intelligence in Government" (April 3, 2025) www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial- Intelligence-in-Government.pdf

traffickers, and malicious cyber groups, by using a variety of targeted financial measures including economic sanctions. Over the past few years, TFI has significantly increased sanctions against Russia related to its actions against Ukraine and its other specified harmful foreign activities. TFI authorities, including its Bank Secrecy Act (BSA)[32] authorities, have supported Administration priorities, including countering narcotics trafficking and ensuring border security. TFI's counter-terrorism designations disrupt the financial networks that support terrorist organizations. Other TFI tools, such as 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, as well as with 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. Treasury officials stated that TFI continues to strengthen its collaborative approach to achieve its mission to effectively implement U.S. policy and disrupt these financial networks. 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 information in the past. 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.

The Office of Intelligence and Analysis (OIA), as a member of the Intelligence Community, is required to take steps to adopt AI to improve intelligence collection and analysis.[33] 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 resources, as well as necessary updates to the information technology infrastructure, have negatively affected OIA's ability to take further steps to adopt AI.[34]

TFI and its components have a wide range of responsibilities in combatting terrorists, criminals,

[32] P.L. 91-508, Bank Secrecy Act of 1970 (October 26, 1970)
[33] P.L. 117-263, James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (December 23, 2022)
[34] Treasury OIG, *OIA Does Not Have Artificial Intelligence Capabilities and Faces Barriers to its Accelerated Adoption*, OIG-25-025 (April 2, 2025)

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.

Challenge 5: Crypto and Digital Assets Growth

Interest in, and use of, digital assets including cryptocurrencies and stablecoins has increased rapidly over the past year. In January 2025, EO 14178, *Strengthening American Leadership in Digital Financial Technology*, established the President's Working Group on Digital Asset Markets to develop a federal regulatory framework for digital assets and prohibited federal agencies from undertaking any action to establish, issue, or promote central bank digital currencies,[35] except to the extent required by law. On July 14, 2025, OCC, the Federal Deposit Insurance Corporation (FDIC), and the Board of Governors of the Federal Reserve System (the Board) issued a joint statement discussing general risk management considerations for engaging in fiduciary and non-fiduciary crypto-asset safekeeping activities.[36] Clarifying risk management considerations for crypto custody, stablecoin transactions, and blockchain networks facilitates institutional adoption and deeper financial integration with digital assets.

On July 18, 2025, the *Guiding and Establishing National Innovation for U.S. Stablecoins Act* (GENIUS Act)[37] was signed into law, marking the United States' first major legislative step towards federally regulating stablecoins. The GENIUS Act expands Treasury's authority and responsibilities related to cryptocurrencies and digital assets, including strengthening national security through enhanced sanctions and anti-money laundering enforcement, and requires the Secretary of the Treasury to issue regulations regarding illicit digital asset activity. With the Secretary chairing on the Stablecoin Certification Review Committee, Treasury will play a key role in certifying state stablecoin frameworks.

On July 30, 2025, the President's Working Group on Digital Asset Markets released a report containing recommendations to strengthen American leadership in digital financial technology.[38] The Working Group report requires regulators to coordinate on actions to modernize bank regulation for digital assets, and made a number of recommendations for rulemaking; however, the full impact of this report's findings depends on additional legislative action[39] and regulators' implementation of the recommendations.

[35] A central bank digital currency or CBDC is generally defined as a digital liability of a central bank that is widely available to the 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.

[36] OCC, FDIC, and the Board. *Crypto-Asset Safekeeping by Banking Organizations* (July 14, 2025) Crypto-Asset Safekeeping by Banking Organizations

[37] P.L. 119-27, GENIUS Act (July 18, 2025)

[38] https://www.whitehouse.gov/crypto/

[39] H.R. 3633, the Digital Asset Market Clarity Act, passed the House of Representatives on July 17, 2025, and has been sent to the Senate for consideration. The bill seeks to clarify regulatory roles and provide consumer protections within the digital asset market.

While Treasury supports responsible innovation and the potential benefits of digital assets, the Financial Stability Oversight Council (FSOC)[40] reported that many crypto-asset firms may be acting outside of, or not in 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.[41] Insufficient oversight or regulatory safeguards could create opportunities for illicit actors, such as cyber actors, ransomware cybercriminals, drug traffickers, human traffickers, sanctions evaders, and fraudsters who may be using cryptocurrencies and digital assets to transfer and launder illicit monies. The U.S. financial system's strength, size, and reliability make it a notable target, and misuse by illicit actors affects matters of national security.[42] The borderless nature of digital asset markets, combined with a lack of consensus, standards, and practices among crypto industry participants with respect to regulations seeking to counter money laundering and terrorist financing exacerbate these issues.

Volatility in the crypto-asset market also poses risks to the traditional financial system. As of August 2025, the crypto-asset market reached a combined market capitalization of $3.9 trillion, up from approximately $2 trillion in September 2024.[43] Financial institutions that develop concentrations in, or build their business models around partnering with or providing traditional banking products and services to a single industry, including the crypto-asset market, may be adversely impacted by disruptions in that industry. This volatility was demonstrated in the spring of 2023, when 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).[44]

Given recent legislative changes and continued growth and interest in digital assets including cryptocurrencies, the Department must determine how to exploit the opportunities these technologies provide while also taking appropriate steps to mitigate risks to the safety and soundness of the U.S. financial system.

[40] FSOC was established by the Dodd-Frank 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.

[41] FSOC, *2024 Annual Report* pp. 45-49

[42] President's Working Group on Digital Asset Markets, *Strengthening American Leadership in Digital Financial Technology* (July 30, 2025) Strengthening American Leadership in Digital Financial Technology – The White House, p. 100

[43] Cryptocurrency Prices, Charts, and Crypto Market Cap (accessed August 21, 2025)

[44] A crypto winter refers to a period when stocks and currencies in the crypto world lose popularity and value, becoming stagnant. The 2022 crypto winter was triggered, in part, by high inflation rates in the U.S., leading to aggressive interest rate increases by the Board.

Other Matters of Concern

Although Treasury OIG is not reporting these as management and performance challenges, we are highlighting two areas of concern: (1) streamlining access to DNP data sources, and (2) ongoing management of COVID-19 pandemic relief programs.

Streamlining Access to DNP Data Sources

Reducing improper payments remains a government-wide priority and a persistent challenge for Treasury. EO 14249, *Protecting America's Bank Account Against Fraud, Waste, and Abuse*, requires executive branch agencies, in collaboration with Treasury, "to take action to defend against financial fraud and prevent improper payments." Such payments often result from incomplete or inaccurate data, insufficient eligibility verification, or weaknesses in program controls. The Payment Integrity Information Act of 2019[45] further requires agencies to prevent, detect, and recover improper payments. Treasury supports agency compliance with the Payment Integrity Information Act through the DNP portal, a central resource for screening benefit recipients, vendors, and other payees against authoritative databases. The DNP portal has significantly expanded over time, incorporating critical data sources, such as the Social Security Administration's Death Master File (DMF) to strengthen its ability to prevent improper payments. Treasury has also enhanced the portal with advanced analytics and system integration capabilities.

Despite these advancements, Treasury continues to face challenges. Agencies currently have access to the complete DMF, but that authority will expire on December 27, 2026,[46] without legislative action to make access permanent. Privacy, legal, and technical constraints also continue to slow integration of new federal and state data sources, limiting Treasury's ability to provide agencies with the full range of information needed to prevent improper payments. In addition, agencies vary in how effectively and consistently they use DNP tools, which reduces the overall government-wide impact of the system. To address these challenges and implement EO 14249, OMB issued M-25-32, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*. The guidance directs agencies to expand their use of DNP while ensuring strong privacy protections and provides new flexibility for sharing data with Treasury. In response, Treasury is developing a streamlined process for accessing additional data sources. Striking the right balance between modernization, data expansion, and privacy safeguards—while avoiding delays that could hinder agencies' ability to fully leverage DNP—remains a significant management challenge.

To strengthen the DNP portal and address challenges in expanding data access, Treasury should secure permanent legislative authority for the DMF, accelerate federal and state data-

[45] P.L. 116-117, Payment Integrity Information Act of 2019 (March 2, 2020)

[46] On December 27, 2020, Congress passed the Consolidated Appropriations Act of 2021, amending the Social Security Act to authorize the Social Security Administration to share its complete death data with the Do Not Pay program for a three-year period beginning no later than December 27, 2023.

sharing agreements, and ensure robust privacy protections in coordination with OMB and oversight bodies. Simultaneously, Treasury should continue modernizing the DNP system through scalable technology and advanced data analytics, improving agency outreach and training to promote consistent use, and establishing performance measures to track impact on improper payments. Streamlining internal governance for onboarding new data sources will further reduce delays, enabling Treasury to maximize the DNP portal's effectiveness, protect privacy, enhance program integrity, and advance government-wide efforts to reduce fraud, waste, and abuse.

Ongoing Management of COVID-19 Pandemic Relief Programs

In response to legislation passed to address the COVID-19 pandemic,[47] Treasury was tasked with disbursing over $650 billion in aid to more than 30,000 recipients to support transportation industry workers; small businesses; renters and homeowners; and state, District of Columbia, local, territorial, and tribal government entities. The Department established OCA[48] to implement and manage most of Treasury's COVID-19 pandemic programs. Treasury's pandemic programs provided needed support to many people and businesses but were subject to losses from fraud and other improper payments. Treasury OIG has performed audits, reviews,[49] and investigations into many of the more than 10,000 complaints and recipient-reported cases received. For the Coronavirus Relief Fund and the first Emergency Rental Assistance program, Congress assigned the Treasury OIG the statutory authority to recoup funds if the Inspector General determined that a recipient failed to comply with the requirements related to the use of those funds. OCA is responsible for recouping ineligible payments and misuses of funds from other pandemic programs.

The Coronavirus State and Local Fiscal Recovery Fund (SLFRF) program is one of several programs for which OCA is responsible for recoupment. Under the SLFRF program, recipients were required to obligate all award funds by December 31, 2024, and must expend funds by December 31, 2026, with the exception of Surface Transportation projects and Title I projects that have an expenditure deadline of September 30, 2026.[50,51] In a recent report, GAO highlighted the compliance procedures and guidance for the SLFRF program.[52] GAO noted that since 2022, Treasury has required SLFRF recipients to submit project and expenditure reports

47 P.L. 116-136, Coronavirus Aid, Relief, and Economic Security Act (March 27, 2020); P.L. 116-260, Consolidated Appropriations Act, 2021 (December 27, 2020); P.L. 117-2, American Rescue Plan Act of 2021 (March 11, 2021); and P.L. 117-328, Consolidated Appropriations Act, 2023 (December 29, 2022)

48 Formerly known as the Office of Recovery Programs.

49 As of September 2025, Treasury OIG has identified approximately $4 billion in monetary impact ($4.2 million in recoupment and $4 billion in questioned costs) for pandemic programs under Treasury's purview.

50 Surface Transportation projects are funding projects eligible under specific Department of Transportation programs.

51 Title I projects are funding projects eligible under Title I of the Housing and Community Development Act of 1974.

52 GAO, *COVID-19 Relief: Treasury Could Improve Compliance Procedures and Guidance for State and Local Fiscal Recovery Funds*, GAO-25-107909 (July 22, 2025)

to provide information on how recipients used their awards, including obligations and spending amounts. In each year from 2022 to 2024, thousands of SLFRF recipients did not meet the reporting deadline for project and expenditure reports. GAO recommended that Treasury develop and document, in its internal procedures and guidance for recipients, the timing and circumstances under which Treasury will initiate recoupment of awards for recipients that have not met SLFRF reporting requirements. To enhance accountability in the program, OCA needs to develop the procedures and guidance recommended in GAO's report.

As many of the pandemic programs under Treasury's purview wind down, OCA needs to ensure recipients continue to use funds responsibly. OCA also must continue to resolve audit findings of grantees and their subrecipients, including those with questioned costs, that are reported through required audits under the *Single Audit Act* (Single Audit).[53] Treasury OIG reported in our memorandum last year that while progress has been made, OCA was not timely in issuing management decisions for Single Audit findings and that remains the case. Prompt actions are needed because, as GAO stated in a recent letter to Treasury, "as more time passes, it is less likely overpayments will be recovered."[54]

Completed and In-Progress Work on Financial Oversight

OCC's Supervision of Federal Branches of Foreign Banks

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

During our audit, we observed that the International Banking Supervision examinations of selected foreign banking organizations were conducted in accordance with existing OCC and *Federal Financial Institutions Examination Council* guidance in effect during the scope period. We also noted that examination work papers did not include documented evidence of supervisory review as required by OCC policy in effect at the time the examinations were conducted. However, due to the passage of time and substantial changes in OCC and *Federal Financial Institutions Examination Council guidance*, and OCC policies, we determined that continuing our audit would not significantly enhance the International Banking Supervision's supervision of foreign banking organizations. Accordingly, we terminated this audit. (OIG-CA-25-043)

[53] P.L. 104-156, Single Audit Act Amendments of 1996 (July 5, 1996)

[54] GAO, *Priority Open Recommendations: Department of the Treasury,* GAO-25-108067 (August 12, 2025). GAO recommended that Treasury needs to develop processes, such as post-payment reviews or recovery audits, to strengthen its oversight of Emergency Rental Assistance funds. GAO also noted that implementing this priority recommendation could help Treasury more consistently identify and recover overpayments—including those resulting from potential fraud—for ineligible households.

Treasury's Implementation of the Coronavirus Economic Relief for Transportations Services Program; Treasury's Implementation of the Coronavirus SLFRF; Treasury's Implementation of the Coronavirus Capital Projects Fund; and Treasury's Implementation of the Local Assistance and Tribal Consistency Fund

Between March 2020 and July 2022, we initiated audits on each of these pandemic programs. The overall objective of these audits was to assess Treasury's implementation activities to establish the pandemic programs, to include policies, procedures, and relevant terms and conditions for providing assistance under the programs.

We found that Treasury established all four pandemic programs and generally met the statutory deadlines for distributing funds. Treasury also developed program-related policies and procedures, but they were not always sufficient and complete. For example, while Treasury developed compliance monitoring procedures, those procedures were incomplete throughout most of the programs' periods of performance. In addition, we identified concerns with the processes for evaluating application submissions to provide awards or distributions of funds for the Coronavirus Economic Relief for Transportations Services program.

During audit fieldwork, we communicated our concerns and preliminary observations with appropriate Treasury personnel. We also noted concerns related to the pandemic programs in our annual management and performance challenges letters issued to Treasury.

We terminated these audits because Treasury's pandemic programs have reached or are approaching the end of their periods of performance. We have also experienced resource constraints that prevent us from continuing this work.

Although we terminated these four implementation audits, the concerns identified in this memorandum and previously communicated to Treasury are noteworthy and should be considered when establishing programs in the future. (OIG-CA-26-006)

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

Review of FinCEN's Beneficial Ownership Information (BOI) 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 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 Closing and Funding Process for Emergency Capital Investment Program Participants (In Progress)

We initiated an audit to assess Treasury's closing and funding process for ensuring the accuracy of Emergency Capital Investment Program investments in compliance with applicable laws, regulations, and policies and procedures.

Failed Bank Reviews

In 1991, Congress enacted the Federal Deposit Insurance Corporation Improvement Act amending the Federal Deposit Insurance Act. 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 (DIF) is "material." The Federal Deposit Insurance Act, as amended by the Dodd-Frank Act, defines the loss threshold amount to the DIF 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 Dodd-Frank 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 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.[55] As appropriate, OIG auditors also make recommendations for preventing any such loss in the future.

From 2007 through March 2026, FDIC and other banking regulators closed 556 banks and federal savings associations. One hundred and forty-six (146) of these were Treasury-regulated financial institutions. Of the 146 failures, 58 resulted in a material loss to the DIF, 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 Santa Anna National Bank which was closed on June 27, 2025. Additionally, we initiated two in-depth reviews on the failures of the First National Bank of Lindsay and Santa Anna National Bank based on the work performed during non-material loss reviews.

Completed and In Progress work on Failed Bank Reviews

Non-Material Loss Review of Santa Anna National Bank, Santa Anna, Texas

We initiated a non-material loss review of the recent failure of Santa Anna National Bank. The objectives of our review were to (1) ascertain the grounds identified by the OCC for appointing the FDIC as receiver and (2) determine whether any unusual circumstances exist that might warrant a more in-depth review of the loss.

During our review, we determined that an in-depth review of Santa Anna National Bank's failure is warranted given that fraud was a significant contributing factor to Santa Anna National Bank's failure. Performing an in-depth review will provide an opportunity to further evaluate the cause of failure and OCC's supervision of Santa Anna National Bank to determine whether there are any lessons to be learned from this failure. (OIG-26-023)

In-Depth Review of First National Bank of Lindsay, Lindsay, Oklahoma (In Progress)

We completed a non-material loss review of the failure of the First National Bank of Lindsay on March 27, 2025. Accordingly, we initiated an in-depth review of the First National Bank of Lindsay's failure, given that fraud was a significant contributing factor to its failure and there was an extraordinarily high estimated loss rate to assets percentage. The objectives of our in-depth review are consistent with the objectives of a mandated material loss review. Specifically, our objectives are to (1) ascertain the causes of the First National Bank of Lindsay's failure and

[55] 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.

associated impact to the DIF, (2) review the OCC's supervision of the First National Bank of Lindsay, and (3) make recommendations for preventing any such loss in the future.

In-Depth Review of Santa Anna National Bank, Santa Anna, Texas (In Progress)

We completed a review of the failure of Santa Anna National Bank on March 11, 2026. Accordingly, we initiated an in-depth review of Santa Anna National Bank's failure, given that fraud was a significant contributing factor to its failure. The objectives of our in-depth review are consistent with the objectives of a mandated material loss review. Specifically, our objectives are to (1) ascertain the causes of Santa Anna National Bank's failure and associated impact to the DIF, (2) review the OCC's supervision of Santa Anna National Bank, and (3) make recommendations for preventing any such loss in the future.

OIG Investigative Accomplishments

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

Significant Investigations

Indiana Non-Profit Director Convicted and Sentenced in Indiana Emergency Rental Assistance Program Fraud Scheme

On June 9, 2025, Treasury OIG completed its report of investigation into an allegation that an Indiana non-profit Director submitted 26 applications to the City of Fort Wayne, Indiana, Emergency Rental Assistance Program. These applications contained fraudulent tax documents and numerous stolen identities to create potential Emergency Rental Assistance recipients. On May 20, 2024, the Director was indicted on 18 counts of wire fraud, and subsequently sentenced by U.S. District Court, Northern District of Indiana, to 50 months confinement to the Bureau of Prisons, two years of supervised release, and restitution of $166,292.

Oregon Residents Convicted and Sentenced for Oregon Coronavirus Relief Fund Program Fraud

On September 25, 2025, Treasury OIG completed its investigation into two individuals who fraudulently obtained business grants from the Oregon Cares Fund, which received its funding from the Coronavirus Relief Fund. In addition, both individuals fraudulently obtained Pandemic Unemployment Assistance. Both defendants pled guilty and were sentenced collectively to 12 months of home detention, 8 years of probation and restitution, criminal fines, and special

assessments totaling $221,897. The Treasury OIG and Department of Labor OIG conducted the investigation.

Joint Investigation Resulting in Multiple Convictions for Emergency Rental Assistance Theft

On December 4, 2025, Treasury OIG completed its investigation for a joint Treasury OIG and United States Secret Service matter, regarding multiple subjects who conspired to defraud the Emergency Rental Assistance and Payroll Protection programs of approximately $690,000. Three subjects were ultimately indicted and sentenced to a total of two years of incarceration, four years of probation, and $621,050 in restitution – including $151,780 in criminal forfeiture. The U.S. Attorney's Office for the Northern District of Indiana prosecuted the case.

Aviation Company Defrauds Payroll Support Program, Agrees to Repay Debt

On December 4, 2025, Treasury OIG completed its investigation regarding Payroll Support Program fraud involving an aviation company located in Honolulu, Hawaii. The company received $1,697,129.40 in Payroll Support Program funds. A compliance review identified the company potentially used $866,910.93 of the allocated funds for unauthorized expenses to include terminating employees after receiving the Payroll Support Program funds in violation of the Payroll Support Program agreement. An agreement to repay the funds was reached by Treasury and the company resulting in the company repaying the entire allocation of $1,697,129.40.

Fraudulently Obtained Treasury Check Investigation Leads to 43 Convictions

On December 19, 2025, Treasury OIG completed its investigation into a stolen identity refund fraud scheme. The investigation resulted in 43 convictions of individuals involved in obtaining and cashing fraudulently obtained Treasury checks. The defendants included employees of money services businesses and the U.S. Postal Service. The charges resulted in 43 convictions, who were sentenced to a combined 1,300 months in prison, 1,752 months of probation, and ordered to pay $27.5 million in restitution to the U.S. Treasury. Defendants were also ordered to forfeit $2.24 million and pay $8,500 in special assessments. In total, court-ordered financial actions totaled $29.83 million. The Department of Justice in the District of Columbia, the District of Maryland, Greenbelt Office, and the Department of Justice Tax Division prosecuted the case.

Joint Investigation Resulting in American Rescue Plan Fraud Convictions

On January 20, 2026, Treasury OIG completed its investigation for a joint Treasury OIG, Federal Bureau of Investigation, and Housing and Urban Development OIG regarding allegations of fraud against the Treasury funded COVID-19 Relief programs under the American Rescue Plan Act. The investigation resulted in a guilty plea of fraud against the American Rescue Plan Act program and a sentencing of two subjects. The primary subject was

sentenced to 30 months imprisonment and the secondary subject received 3 years of probation; restitution of $749,940 was also ordered. The United States Attorney's Office for the District of Delaware prosecuted the case.

Suspected Money Laundering Through the Mutilated Currency Division

On January 30, 2026, Treasury OIG completed its portion of a joint Federal Bureau of Investigation and U.S. Customs and Border Patrol investigation into an individual suspected of laundering currency through BEP's Mutilated Currency Division. The joint investigation revealed that the subject submitted more than $250,000 of mutilated currency, from multiple international transfers from identified terrorist/high crime locations before submission to the Mutilated Currency Division. Subject alleged they ultimately wanted to deposit a combined check of the funds into a personal account in Canada despite the subject having no known ties to the U.S. The U.S. District of Montana accepted prosecution but due to other prosecutorial priorities, ultimately decided to not proceed with prosecution. However, this investigation revealed Mutilated Currency Division vulnerabilities resulting in the OIG issuing an OIG Systemic Observation report to BEP.

Homeowners Assistance Fraud Investigation Resulted in $2.7 Million in Civil Forfeiture

On March 5, 2026, Treasury OIG completed its investigation regarding Homeowners Assistance Fund fraud under the American Rescue Plan Act. The investigation revealed that an unknown third party impersonated a vendor doing business with the North Carolina Housing Finance Agency and defrauded $2,767,919.94 from the agency's Homeowners Assistance Fund program. The U.S. Attorney's Office for the Eastern District of North Carolina obtained a Civil Judicial Order and Default Judgement of Forfeiture for the entire $2,767,919.94. These funds were returned to the Homeowners Assistance Fund program.