Federal Deposit
Insurance Corporation
Office of Inspector General

Semiannual Report to the Congress

April 1, 2026 - September 30, 2026



Integrity
Independence
Objectivity
Transparency
Excellence

Office of Inspector General

250TH ANNIVERSARY OF AMERICA
1776–2026

Under the Inspector General Act of 1978, as amended, the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) has oversight responsibility of the programs and operations of the FDIC.

The FDIC is an independent agency created by the Congress to maintain stability and confidence in the Nation's banking system. The FDIC insures deposits; examines and supervises financial institutions for safety and soundness and consumer protection; makes large, complex financial institutions resolvable; and manages receiverships. Approximately 4,966 individuals carry out the FDIC mission throughout the country.

According to FDIC data (June 30, 2026), the FDIC insured $10.84 trillion in domestic deposits in 4,238 institutions, of which the FDIC supervised 2,661. The Deposit Insurance Fund balance totaled $161.1 billion. Active receiverships totaled 44, with assets in liquidation of about $23.2 billion.



Semiannual Report to the Congress

April 1, 2026 - September 30, 2026

OIG

Office of Inspector General

Federal Deposit Insurance Corporation

Our Mission

To deliver credible results that drive meaningful change, enhance integrity and accountability, and maintain public trust in the FDIC.

Our Vision

To be a leader within the IG community through proactive, agile, and innovative oversight of FDIC programs and operations.

Values

- ★ *Integrity*
- ★ *Objectivity*
- ★ *Independence*
- ★ *Excellence*
- ★ *Transparency*



Inspector General's Statement



I am pleased to submit this *Semiannual Report to the Congress* highlighting the oversight activities of the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) for the period April 1, 2026 – September 30, 2026.

Throughout this time, we implemented our Strategic Plan for 2026-2031. The plan outlines areas of focus office-wide to ensure that while carrying out the OIG's statutory mission of conducting audits and investigations, we strengthen relationships with stakeholders and partners, manage and optimize resources and technology, and remain focused on the value of our people and workplace culture. Our results in this semiannual report are presented within the framework of these Strategic Goals.

Our Office of Audits issued three reports: one was the Failed Bank Review of Metropolitan Capital Bank & Trust, where we determined that the failure occurred primarily due to insufficient Board and management oversight of the bank's high-risk business strategy with extensive levels of risky assets. In a second report on the FDIC's Incident Detection and Response Program, we made four recommendations to improve the FDIC's processes to detect, respond, and actively defend against cyber threats. Issuance of our annual evaluation in accordance with the Federal Information Security Modernization Act (FISMA) was the third report—noting that KPMG found the FDIC's information security program was generally effective and that the FDIC had established several information security program controls and practices that were consistent with FISMA requirements, resulting in a rating of "4" or "managed and measurable." However, the report cited two recommendations from prior FISMA reports that remained open and warranted continued attention. The FDIC responded that it was committed to completing corrective actions to address these outstanding recommendations and further strengthen its information security program. We have since closed those two recommendations.

With regard to investigations, we continued to investigate fraud related to FDIC-regulated and insured banks, achieving outcomes that strengthened integrity and controls at the FDIC and within the financial sector. During the reporting period, our cases resulted in 46 indictments/informations; 46 convictions; 40 arrests; and more than $684 million in fines, restitution ordered, and other monetary recoveries. Importantly, in addition to successful casework, a key initiative for our Office of Investigations during the reporting period was the transition to a new Case Management Tracking System, which we anticipate will substantially enhance accuracy, efficiency, reporting, and decision-making capabilities for our office.

In this report, we present numerous case highlights where individuals pled or were found guilty and sentenced. For example, the former president and Chief Executive Officer of The First National Bank of Lindsay, which failed in October 2024, pled guilty to bank fraud. In another case, a former federal contractor was found guilty for his role in a conspiracy to destroy government databases, password trafficking regarding information from a computer hosting Equal Employment Opportunity Commission data, and possession of a firearm. Additionally, an individual was sentenced to 151 months in prison for leading a $27 million fraud and money laundering scheme targeting about 2,000 elderly victims across the U.S., and the former Chief Financial Officer of Bank of the Valley was sentenced to 36 months in prison for bank fraud. In another significant case, Alibaba Group and AUS Merchant agreed to pay $600 million to resolve Department of Justice allegations.

The increasing number and nature of fraud schemes that threaten consumers and banks continue to cause serious harm. We work to prevent those from happening through investigations, social media postings, pursuit of Hotline inquiries, website notifications, internal and external outreach, and support of other agency efforts. Several of these schemes are highlighted in this report, and we also note outreach activities that we have undertaken to deter such schemes. Chief among those during the reporting period were a video podcast and another video on the dangers of falling for impersonation schemes, both available at https://www.fdicoig.gov/impersonation-scams.

We have continued to engage in productive relationships with stakeholders—those internal to the FDIC at the management and seniormost leadership level, as well as those in the IG community, law enforcement partners, Congress, the Government Accountability Office, media, and the public. Their support is critical to our success.

Additionally, during the reporting period, we have carefully monitored our resource needs to carry out the OIG mission, as conveyed in our Congressional Budget Justification for fiscal year 2027 and in discussions with the Office of Management and Budget and Congressional appropriators. To manage and optimize resources and technology, we continue ensuring the security of the OIG's infrastructure; upgrading dashboards supporting budget, human resources, and procurements; advancing the use and value of data analytics; and exploring the most effective means of leveraging super intelligence.

I also note that Mike McCarthy, former Counsel to the IG, retired after 25 years of Federal service. Mike was an invaluable member of our office, and we will miss his sage advice and positive presence in the OIG. Regina Sandler is taking on the role of Counsel to the IG, and we have also recently promoted Matthew Simber to serve as the Assistant Inspector General for Audits. We welcome both Regina and Matthew to our Executive team.

In closing, I am grateful to work alongside members of the FDIC OIG and pleased that two of our teams received prestigious annual awards from the Council of the Inspectors General on Integrity and Efficiency for their distinguished accomplishments. During the reporting period, we acknowledged America's 250th Anniversary with a look back to the origin and evolution of Inspectors General and are proud to have upheld the history of the IG concept at the FDIC. With the constant support of the FDIC and the Congress, we are committed to continuing to serve the public in the years ahead.

/S/

Jennifer L. Fain
Inspector General
October 2026



Table of Contents

Inspector General's Statement	**i**
Acronyms and Abbreviations	**2**
Introduction and Overall Results	**3**
Audits, Evaluations, and Other Reviews	**4**
Investigations	**13**
Other Goal Areas	**34**
Cumulative Results	**44**
Reporting Requirements	**45**
Appendix 1 Information in Response to Reporting Requirements	**47**
Appendix 2 Information on Failure Review Activity	**60**
Appendix 3 Peer Review Activity	**61**
OIG 250th	**64**
Congratulations	**65**

An electronic copy of this report is available at www.fdicoig.gov.



Acronyms and Abbreviations

BOV	Bank of the Valley
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CFPB	Consumer Financial Protection Bureau
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
DHS	Department of Homeland Security
DIF	Deposit Insurance Fund
DOJ	Department of Justice
ECU	Electronic Crimes Unit
EEOC	Equal Employment Opportunity Commission
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act
FNBL	First National Bank of Lindsay
FRB	Board of Governors of the Federal Reserve System
FSOC	Financial Stability Oversight Council
GAO	Government Accountability Office
GSA	General Services Administration
HSI	Homeland Security Investigations
IG	Inspector General
IRS-CI	Internal Revenue Service-Criminal Investigation
IT	Information Technology
OA	Office of Audits
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
PD	Police Department
PRAC	Pandemic Response Accountability Committee
SBA	Small Business Administration
SI	Super Intelligence
TIGTA	Treasury Inspector General for Tax Administration
USAO	United States Attorney's Office
VA	Department of Veterans Affairs



Introduction and Overall Results

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) is a statutorily created independent office, whose core purpose is to prevent and detect fraud, waste, abuse, and mismanagement in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the FDIC. The OIG provides independent oversight of the FDIC by conducting audits, evaluations, investigations, and other reviews; and keeping the Chairperson and Congress fully and currently informed about problems and deficiencies relating to the administration of FDIC programs and operations. The mandate of the OIG is derived from the Inspector General Act of 1978, as amended.

Our Office conducts its work in line with a set of strategic goals that we have adopted, and the results of our work during the reporting period are presented in this report within the framework of those goals. These goals focus on areas that are critical to our success: Promoting Accountability and Integrity; Strengthening Relations with Partners and Stakeholders; Managing and Optimizing Resources and Technology; and Valuing Our People and Workplace Culture. The OIG's collective efforts will guide our Office as we pursue these goals and carry out the OIG mission. The following table presents overall statistical results from the reporting period.

Overall Results (April 1, 2026 – September 30, 2026)	
Audit, Evaluation, and Other Products Issued	**3**
Recommendations	**4**
Investigations Opened	**44**
Investigations Closed	**2**
Judicial Actions:	
Indictments/Informations	**46**
Convictions	**46**
Arrests	**40**
OIG Investigations Resulted in:	
Special Assessments	**$8,400.00**
Fines	**$176,528.00**
Restitution	**$46,008,968.27**
Asset Forfeitures	**$423,068,810.00**
Criminal Penalty	**$210,000,000.00**
Civil Penalty	**$4,919,631.00**
Administrative Recovery	**$64,692.76**
Total	**$684,247,030.03**
Referrals to the Department of Justice (U.S. Attorney and DOJ Antitrust)	**44**
Investigative Reports Referred to FDIC Management	**6**
Responses to Requests Under the Freedom of Information/Privacy Act	**19**
Subpoenas Issued	**6**



Audits, Evaluations, and Other Reviews

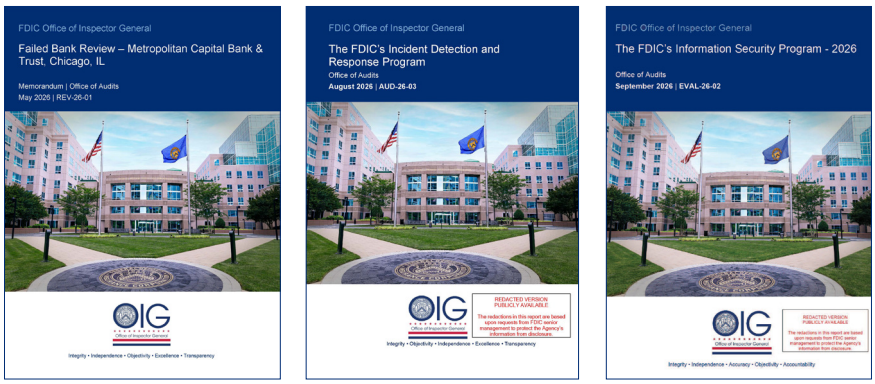
In keeping with our Strategic Goals, **the FDIC OIG conducts audits, evaluations, and reviews to promote accountability and integrity in FDIC programs and operations.** We do so by responsibly and transparently:

- Conducting high-impact audits, evaluations, and other reviews focused on critical risk areas, ensuring relevance, timeliness, and adherence to professional standards.
- Writing clear, concise, and persuasive reports based on reliable evidence and sound analysis, effectively communicating findings and recommendations.
- Making recommendations that effect change, address control weaknesses, and focus on outcome-oriented results, and ensuring effective implementation by the FDIC through enhanced monitoring.

During the reporting period, we issued three reports. One addressed a failed bank, and the other two related to information security issues at the FDIC—one that audited the Incident Detection and Response Program and the other our annual evaluation in accordance with the Federal Information Security Modernization Act.

We note that in addition to planned discretionary work, under the Federal Deposit Insurance (FDI) Act, our Office is statutorily required to review the failures of FDIC-supervised institutions causing material losses to the Deposit Insurance Fund (DIF) if those occur. The materiality threshold is currently set at $50 million.

If the losses to the DIF as a result of a failure are less than the material loss threshold, the FDI Act requires the Inspector General of the appropriate Federal banking agency to determine the grounds upon which the state or Federal banking agency appointed the FDIC as receiver and whether any unusual circumstances exist that might warrant an In-Depth Review of the loss. During the reporting period, we issued a failed bank review, that of Metropolitan Capital Bank & Trust, Chicago IL. This bank failed on January 30, 2026, with losses to the DIF estimated at about $19.7 million at the time.



Audit and Evaluation Reports issued during the reporting period.

Results of the audits, evaluations, and other reviews completed during the reporting period are summarized below. In addition to FDIC OIG reports, we summarize a memorandum issued by a working group of the Council of Inspectors General on Financial Oversight, of which we were a part. We also include a listing of the challenges we highlighted in our Top Management and Performance Challenges report that we issued in March 2026. These challenges are largely driven by our audit and evaluation work throughout the year. Notably, however, the challenge related to identifying and combating fraud and misrepresentation derived principally from our investigations. A listing of ongoing audit and evaluation assignments, prompted in part by our assessment of the Top Management and Performance Challenges Facing the FDIC, is also presented. We give an update on an OIG email security matter. Finally, we present information on recommendations unimplemented for more than one year.

Importantly, with regard to closing recommendations, it is important to note that during the reporting period, we closed the final open recommendations from our report on *The FDIC's Sexual Harassment Prevention Program*. We made 24 recommendations in that report to improve the program and the impact of those will significantly contribute to an improved workplace culture at the FDIC.

Audits, Evaluations, and Other Reviews

Failed Bank Review—Metropolitan Capital Bank & Trust, Chicago, Illinois

On January 30, 2026, the Illinois Department of Financial and Professional Regulation (IDFPR), Division of Banking, took possession and control of Metropolitan Capital Bank & Trust, Chicago, IL, (Metro Capital) and appointed the FDIC as the receiver. Metro Capital was a state-chartered bank that became FDIC-insured on January 25, 2005, and operated from a single leased office in Chicago, IL. Metro Capital was wholly owned by Metropolitan Capital Bancorp, Inc. – a privately held, one bank holding company. Metro Capital focused on relationship banking with high net-worth individuals, with an emphasis on unsecured lending and loans secured by privately held stock or interest in limited liability companies.

We reported that according to the FDIC, the estimated loss to the DIF from this failure was $19,647,000 or 8 percent of the bank's $232,051,439 in total assets.

As referenced above, when the DIF incurs a loss under $50 million, the FDI Act, 12 U.S.C. § 1831o(k)(5), requires the Inspector General of the appropriate Federal banking agency 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 of the loss. An in-depth review is a formal evaluation of the causes of the institution's failure, resulting loss to the DIF, and the FDIC's supervision of the failed institution, including the FDIC's implementation of the Prompt Corrective Action provisions of Section 38 of the FDI Act.

Following a period of supervisory actions by regulators, the IDFPR took possession of Metro Capital because it experienced continued asset quality issues, which ultimately eroded its capital position. In conducting this failed bank review, we assessed key documents related to Metro Capital's failure, including the Division of Risk Management Supervision's Supervisory History, the Division of Resolutions and Receiverships' Failing Bank Case, and specific examination and visitation reports issued from 2018 to 2025.

We determined that Metro Capital's failure occurred primarily due to insufficient Board and management oversight of its high-risk business strategy with extensive levels of risky assets (e.g., unsecured and Private Interest Collateral loans). The bank did not apply appropriate controls and credit risk management practices to measure, monitor, and address the inherent risks associated with these assets. The bank experienced continued deterioration in credit quality, which contributed to significant loan losses and rapid deterioration of its capital.

Our review did not find unusual circumstances that would warrant an in-depth review of the loss.

The FDIC's Incident Detection and Response Program

Under Federal law and regulation, the FDIC is responsible for safeguarding information, data, and assets from loss, theft, or compromise. To accomplish this, the FDIC must maintain the ability to prepare for, respond to, and resolve computer security incidents. We conducted an audit to determine to what extent the FDIC has implemented processes to detect, respond, and actively defend against cyber threats. Of note, in conducting this audit, we leveraged technology by conducting in-house adversary emulation tests using an open-source module and in close coordination with the FDIC's Chief Information Officer Organization and Division of Information Technology. The emulation tests simulated real-world attacks by threat actors in order to uncover risks and security gaps before they impact an organization.

The Cybersecurity and Infrastructure Security Agency has continued to identify cyber threats targeting critical infrastructure, such as the Financial Services Sector. Failure to protect bank, employee, and other sensitive information could cause irreparable financial, reputational, operational, or other harm to the FDIC, individuals, and entities.

Our audit determined that the FDIC has implemented controls and processes in eight security areas to detect, respond, and actively defend against cyber threats. However, we identified improvement opportunities in three security areas covering its incident detection and response program. Specifically, we reported that the FDIC can (1) strengthen its monitoring of endpoint detection and response logs to better detect known adversarial techniques such as running malicious code, maintaining access, and avoiding detection; (2) update its policies for involuntarily separated employees to address the elevated risk present when an employee is involuntarily separated; and (3) better align its incident response capabilities testing to National Institute of Standards and Technology standards while improving coordination between the Office of the Chief Information Security Officer and the Division of Information Technology.

Prompt remediation of the issues we identified will better position the FDIC to monitor, detect, and respond to threat actors in a timely manner to minimize the damage they can cause and reduce the risk to the FDIC's mission to maintain stability and public confidence in the Nation's financial system.

We made four recommendations to improve the FDIC's processes to detect, respond, and actively defend against cyber threats. We recommended that the FDIC assess the current process for maintaining incident detection strategies to identify where gaps in coverage exist; inspect current access permissions on FDIC endpoints and update accordingly; update applicable FDIC directives related to involuntary separations for the timely removal of logical access based on risk-driven timetables; and align current incident response testing procedures to NIST Cybersecurity Framework incident response functions. The FDIC concurred with all four recommendations and plans to complete all corrective actions by July 31, 2027.

Federal Information Security Modernization Act (FISMA) 2026

FISMA requires the head of each agency to implement policies and procedures to cost effectively reduce risks to an acceptable level. Without effective controls for safeguarding its information systems and data, the FDIC would be at an increased risk of a cyberattack that could disrupt critical operations and allow inappropriate access to, and disclosure, modification, or destruction of FDIC information.

During the reporting period, we issued our 2026 report on the FDIC's Information Security Program per statutory FISMA requirements. The objective of this evaluation was to assess the effectiveness of the FDIC's information security program and practices. The OIG contracted with KPMG LLP to perform this work.

Inspectors General assign maturity level ratings to each FISMA metric, as well as an overall rating, using a scale of 1-5, where 5 represents the highest level of maturity. KPMG determined that the FDIC's overall information security program was operating at a Maturity Level 4 (Managed and Measurable).

KPMG found the FDIC's information security program was generally effective and that the FDIC established several information security program controls and practices that were consistent with FISMA requirements. KPMG did not identify any new findings specific to this year's metrics. However, the report references previously identified security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices that the FDIC should continue to improve in order to enhance the agency's security program.

The report cites two recommendations from prior FISMA reports that remain open and warrant continued attention. The FDIC's response indicates that the FDIC is committed to completing corrective actions to address these outstanding recommendations and further strengthen its information security program. (As noted earlier in the IG's Statement in this report, those two recommendations were closed after the end of the reporting period.)

FSOC Working Group Memorandum

Council of Inspectors General on Financial Oversight (CIGFO) Memorandum: CIGFO issued its memorandum titled, *Audit of the Financial Stability Oversight Council's Designation of Nonbank Financial Companies*, on July 30. The memorandum describes the Financial Stability Oversight Council's (FSOC) 2023 *Guidance for Nonbank Financial Company Determinations* process as it existed during the audit period.

The CIGFO team, which included staff from the FDIC OIG's Office of Audits (OA), examined the process and documentation in place during the audit period, including FSOC's development of the 2023 Guidance, its coordination with member agencies, and its Analytic Framework supporting responsibilities under Section 113 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).

Based on the information reviewed during the audit period, the team observed the following:

- The 2023 Interpretive Guidance outlines the process that reflects FSOC's authorities under the Dodd-Frank Act and describes the steps FSOC may take in addressing potential threats to U.S. financial stability.
- FSOC documented engagement with its member agencies in developing the 2023 Interpretive Guidance and Analytic Framework.
- Member agency responses to the team's structured questionnaire demonstrated that the process described in the 2023 Interpretive Guidance supported FSOC's ability to address its responsibilities under Section 113 during the audit period.

Importantly, in March 2026, FSOC issued proposed revisions to its interpretive guidance and released them for public comment. These proposed revisions were outside the scope of the CIGFO review and once finalized are expected to materially change aspects of FSOC's current designation process. As such, the memorandum discusses observations made during the audit period and does not include evaluative judgments regarding the sufficiency or statutory alignment of FSOC's 2023 Guidance.

Top Management and Performance Challenges

During the past year, the Federal government, including the FDIC, felt the impact of significant restructuring and reform. Our annual reporting of the Top Management and Performance Challenges facing the FDIC, issued in March 2026, highlighted areas that we believed warrant the FDIC's continued attention as it carries out its critical mission and briefly assessed 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 was likely to undergo significant changes going forward that may impact these currently identified Top Challenges.

We noted 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 Within Financial Institutions.
- Scams Targeting Unwitting Customers.
- Addressing Misuse of the FDIC Name and Logo.

We are now reviewing the past listing and assessing the current management and performance challenges facing the FDIC. We will issue our next assessment in conjunction with the FDIC's issuance of its Annual Report in February 2027.

Ongoing Work

At the end of the current reporting period, we had a number of ongoing audits, evaluations, and reviews, in large part emanating from our analysis of the Top Management and Performance Challenges and covering significant aspects of the FDIC's programs and activities. These include the following projects formally announced to the FDIC and highlighted below:

- **Valuation Process for Large Regional Bank Resolutions:** The 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 Examinations of Banks' Anti-Money Laundering (AML)/Countering Financing of Terrorism (CFT) and Sanctions Compliance:** The 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's Franchise Marketing Process for Large Regional Bank Resolutions:** The 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.
- **Material Loss Review of Community Bank & Trust - West Georgia:** The objectives are to (1) determine why Community Bank & Trust's problems resulted in a material loss to the DIF and (2) evaluate the FDIC's supervision of Community Bank & Trust, including the FDIC's implementation of the Prompt Corrective Action requirements of Section 38 of the FDI Act, and make recommendations for preventing any such loss in the future.
- **Audit of the FDIC's Off-boarding Process:** The objective is to determine whether the FDIC's controls over the off-boarding process for separating employees and contractors are designed and operating effectively.
- **FDIC Workforce Optimization Initiative:** Staffing Levels and Examination Impacts: The objective is to review the FDIC's 2025 staffing level changes and determine the extent to which those changes have had an impact on the FDIC's ability to complete safety and soundness examinations.

- **Audit of the FDIC's IT Readiness for Large Complex Institutions Resolutions:** The objective is to determine the extent to which the FDIC ensures that its IT capabilities, services, and support are sufficient to achieve divisional goals for the resolutions of large complex financial institutions and that those goals align with FDIC strategic priorities.
- **Failed Bank Review of Tioga-Franklin Savings Bank:** The objectives are to determine (a) the grounds identified by the state banking agency for appointing the FDIC as receiver and (b) if the circumstances surrounding the failure of the bank warrant an in-depth review of the loss.

Update on an Issue Related to OIG Email Security

As reported in our previous semiannual reports, and originating during the course of a prior audit under FISMA, we learned that the FDIC process for emails included manual review by the FDIC (FDIC employees and/or contractors) of messages flagged by automated tools. We pointed out that this process presented security and privacy risks that FDIC employees and/or contractors could be inadvertently exposed to information that they would otherwise not be permitted to review. In addition, this process presented risks that emails relevant to urgent law enforcement matters would not be received by the OIG in a timely manner, thus presenting security and safety concerns.

Since our last reporting period, the OIG continues to monitor the FDIC's progress in modernizing the OIG's email infrastructure and addressing the security and privacy risks previously identified. While the FDIC has implemented interim processes and procedures developed in coordination with the OIG that reduce the risks associated with the former manual review of OIG email, the overall modernization effort remains incomplete.

A critical requirement for full mitigation of these risks is the transition to having OIG email flow directly into the OIG's own email tenant, coupled with the deployment of Data Loss Prevention capabilities that provide full auditing and control over OIG data visibility. Additionally, agreement between the OIG and the Corporation on the appropriate level of auditing visibility is necessary to ensure that sensitive OIG information is properly safeguarded. Until the Corporation completes these steps and the supporting infrastructure is fully implemented, tested, and accepted, the OIG cannot consider the modernization effort complete.

As of the most recent information provided to us, the next phase of work required to support the OIG's independent tenant and Data Loss Prevention implementation, has not yet been funded and remains under internal review by the Corporation. The OIG will continue to request updates and work with the Chief Information Officer to ensure that the identified risks are fully addressed and that appropriate long-term controls are put in place.

OIG Recommendations Open Over One Year

As noted in Table 1 in the Appendix of this report, as of the end of the reporting period, there were nine recommendations that the OIG made to management that remained open for more than one year. We routinely coordinate with the FDIC's Office of Risk Management and Internal Controls to determine whether the OIG's recommended and agreed-upon corrective actions have been completed. In reviewing the status of these open recommendations, the OIG believes that four of the nine should have been closed in a timelier manner. We included three of these four in our prior semiannual report. A listing of these reports and associated recommendations follows:

The FDIC's Orderly Liquidation Authority
EVAL-23-004, September 28, 2023

Recommendation 2: We recommend that the Acting Director, Complex Institution Supervision and Resolution, develop and consistently maintain comprehensive Orderly Liquidation Authority policies and procedures for systemically important financial companies, to include: (a) Tier I policies and procedures for framework-level activities (b) Tier II policies and procedures for operational process-level activities (c) Tier III policies and procedures for institution-specific planning activities. (d) Other operational program policies and procedures for Orderly Liquidation Authority resolution planning activities.

FDIC Readiness to Resolve Large Regional Banks
EVAL-25-02, December 10, 2024

Recommendation 1: We recommend that the Deputy to the Chairperson for Financial Stability and Director, Division of Complex Institution Supervision and Resolution, in coordination with the Acting Director, Division of Resolutions and Receiverships, the Deputy to the Chairperson and Chief Operating Officer, and the Deputy to the Chairperson and Chief Financial Officer, establish and implement an agency-wide resource committee to monitor and report on corporate resource needs, including existing recruiting strategies, staffing levels, and information technology resources in order to strengthen resource planning and response capabilities for large regional bank resolutions.

Recommendation 6: We recommend that the Deputy to the Chairperson for Financial Stability and Director, Division of Complex Institution Supervision and Resolution, in coordination with the Acting Director, Division of Resolutions and Receiverships, develop and implement a resolution readiness training program for key personnel responsible for executing the Regional Resolution Framework and related procedures. The training program should address awareness, plan-specific, role-based, and functional training.

Review of FDIC's Ransomware Readiness
REV-24-01, March 20, 2024

Recommendation 4: We recommend that the Chief Information Officer Organization conduct an analysis to identify viable alternatives for testing restoration of Active Directory from backups, or have senior management formally accept the risk of not testing these backups.

The above discussion reflects the status of the recommendations listed as of September 30, 2026. The FDIC may have taken action to implement these recommendations subsequent to that date. Our website presents the most current status of unimplemented recommendations at Unimplemented Recommendations | Federal Deposit Insurance Corporation OIG.



Investigations

As reflected in our Strategic Goal to promote accountability and integrity, a key area of our statutory responsibility is our investigative role. Similar to audit and evaluation work, we conduct **investigative activity in a responsible, transparent manner.** We do so by:

- Leading high-impact investigations of significant matters of wrongdoing and misconduct relating to agency employees, contractors, and institutions, and ensuring adherence to professional standards.
- Building strong relationships with FDIC and law enforcement partners to drive key investigations and ensuring appropriate actions are taken based on investigative findings.
- Enhancing information sharing to proactively identify, assess, and respond to dynamic risks and supporting law enforcement initiatives and cases in the financial sector.

Our investigations are largely based upon referrals from the FDIC; our law enforcement partners, including other OIGs; the Department of Justice (DOJ), including U.S. Attorneys' Offices (USAO) and the Federal Bureau of Investigation (FBI); and referrals from our OIG Hotline. Our Office of Investigations (OI) plays a key role in investigating sophisticated schemes of bank fraud, embezzlement, money laundering, cybercrime, and currency exchange rate manipulation—fraudulent activities affecting FDIC-supervised or insured institutions. Whether it is bank executives who have caused the failures of banks, or criminal organizations stealing from Government-guaranteed loan programs—these cases often involve bank directors and officers, Chief Executive Officers, attorneys, real-estate insiders, financial professionals, crypto-firms and exchanges, Financial Technology (FinTech) companies, and international financiers.

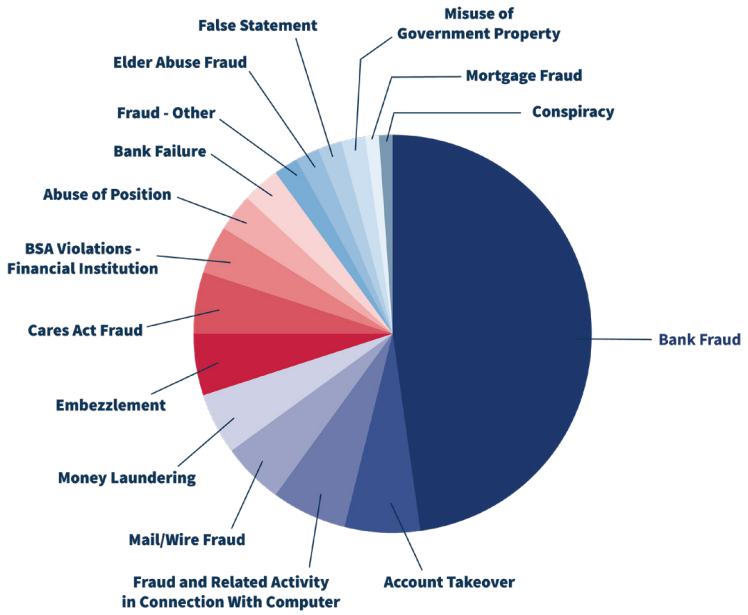
FDIC OIG investigations during the reporting period resulted in 46 indictments/informations, 46 convictions, 40 arrests, and more than $684 million in fines, restitution ordered, and other monetary recoveries. We opened 44 cases and closed 2 during the reporting period. The low number of closed cases this period occurred because we halted closures during the transition to our new Case Management Tracking System. However, during the review of cases, we noted duplicate entries for two cases and closed those from the system. We referred six investigative reports to FDIC management for action.

OIG investigations can develop evidence of criminal misconduct that can support the FDIC's and other regulatory entities' ability to remove individuals from banking and prohibit their future participation. By sharing investigative findings and court outcomes with our partners, the OIG helps establish the factual basis for prohibition actions when statutory requirements are met. These prohibitions help protect depositors, prevent future harm, and preserve public confidence in the banking system. During this reporting period, OI's investigations led to three prohibition/removal orders.

Open Investigations

The FDIC OIG's open investigations cover a wide range of allegations, as shown in the accompanying Figure.

Open Investigations – Allegations



Update: Management Advisory on Risks of Applications Installed on FDIC Mobile Devices

The OIG issued a management advisory memorandum to the FDIC Chairman in February 2026, based on OI forensic analysis. The memorandum advised that user-installed mobile applications pose risk to the FDIC's data and information systems. Such applications may inadvertently expose sensitive information, introduce malware, or facilitate data leakage, particularly if connected to non-FDIC accounts. The intent of the memorandum was to assist the Chairman in his consideration of actions to mitigate potential risks posed by employee-installed applications on FDIC mobile devices. In response, the FDIC implemented certain policy and technology changes intended to address these risks. We can now report that as a result of corporate action to address the risks of applications installed on FDIC mobile devices, the FDIC took four personnel actions, with others underway. The OIG continues to work with the Corporation to remediate other such installations of risky applications.

Electronic Crimes Unit

Our Electronic Crimes Unit (ECU) is an important component within OI. The ECU provides industry-leading digital forensic, eDiscovery, and cryptocurrency tracing support to investigations nationwide, and conducts high-impact, cyber-focused criminal investigations impacting FDIC programs and operations. The ECU lab analyzes voluminous electronic records in support of complex financial fraud investigations that span the U.S. and overseas. The ECU lab also provides a platform for complex data analysis, eDiscovery, forensic data services, undercover work, and investigative technology operations, as well as the analysis of electronically stored information. Since FY 2024, the ECU lab has supported approximately 130 requests for assistance within OI that provided forensic and analytical support for 40 search warrants, over 64 forensic imaging requests, and numerous eDiscovery reviews for Special Agents throughout the country. The ECU has collected over 314 items and imaged over 358 terabytes of data in support of ongoing investigations.

ECU Special Agents are tasked with investigating complex financial cybercrimes that directly and indirectly affect FDIC program and operations. Investigative priorities include intrusions, cryptocurrency, impersonation, ransomware, Darkweb, business email compromises, and account takeovers targeting banks and financial institutions. The ECU continues to focus on early-warning notifications to enable prompt and coordinated law enforcement responses to adversarial cyberattacks. Notably, as well, the ECU is actively engaged in coordinating with the FDIC and assisting with the take-down of fake websites that misrepresent the FDIC and seek to victimize the public.

The ECU is also addressing insider cyber threats involving FDIC financial institutions and FinTech companies, particularly in cases where employees improperly disseminate personally identifiable information via social media and other digital platforms. Through advanced investigative methodologies and collaboration with industry and law enforcement partners, the ECU is committed to identifying insider threats and holding responsible parties accountable.

(Learn more about the FDIC OIG ECU in a video on our website at www.fdicoig.gov/oig-videos.)



ECU Agent (in center) engages in outreach at AGA training and another ECU Agent shares information on the OIG and ECU with middle school students.

Pandemic-Related Financial Crimes

Since many of the programs in the Coronavirus Aid, Relief, and Economic Security (CARES) Act and related legislation were administered through banks and other insured institutions, our OI has been actively involved in investigating pandemic-related financial crimes affecting the banks. In addition, our Office has regularly coordinated with the supervisory and resolutions components within the FDIC to watch for patterns of crimes and other trends in light of the pandemic. Our Special Agents have worked proactively with other OIGs; U.S. Attorney's Offices; and other law enforcement agencies on cases involving frauds targeting the $5 trillion in funds distributed through pandemic relief programs. Through these collaborative efforts, we have been able to identify, develop, and lead cases specific to fraud related to stimulus packages. We have played a significant role within the law enforcement community in combating this fraud, and since inception of the CARES Act, have been involved in 202 such cases. As time goes on, our CARES Act related cases have lessened, but our impact remains to be felt. As one example from the reporting period, Regions Bank, headquartered in Birmingham, Alabama, agreed to pay the U.S. $4.9 million to resolve allegations that Regions received payments it should not have received from the U.S. in connection with Regions approving forgiveness of a customer's Paycheck Protection Program loan, despite the fact that the loan was not eligible for forgiveness.

Overall, during the reporting period, the FDIC OIG's efforts related to the Federal government's COVID-19 pandemic response resulted in six charging actions (indictments, informations, and superseding indictments and informations), three arrests, and eight convictions involving fraud in the CARES Act programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases totaled $23,239,233.

Leveraging Data Analytics

Importantly, our Office continues to develop its data analytics capabilities – to use technology in order to convert large datasets to actionable insights. We are gathering relevant internal and external datasets, developing cloud-based tools and technology in conjunction with the Corporation, and leveraging FDIC OIG data science expertise – in order to marshal our resources and harness voluminous data.

The OIG is also engaged in data analytics outreach and partnerships with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and coordinated a joint session at the 2026 FDIC Data Summit with the Federal Trade Commission on fraudsters impersonating FDIC officials. Our ultimate goal is to proactively identify tips and leads for further investigations and high-impact cases, detect high-risk areas at the FDIC for possible audit or evaluation coverage, and recognize emerging threats to the banking sector.

Our data analytics efforts with respect to our OI also involve collaboration with the Pandemic Response Accountability Committee (PRAC), the FDIC, DOJ, FBI, Federal Trade Commission, and others. These efforts have resulted in expanded access to investigative data tools and capabilities for OIG investigations; identification of potential data sets relevant to OIG efforts; new opportunities for collaboration with external partners; identification of additional data analytics pilot projects; and information sharing agreements to help inform overall strategic planning within the OIG.

BEWARE OF SCAMS!

Our Office is working diligently to address two major scams plaguing the FDIC and the FDIC OIG. The first is **Impersonations.** There has been a sharp increase in impersonation scams where victims receive unsolicited phone calls, text messages, letters, or e-mails claiming to be from the FDIC, the FDIC OIG, other law enforcement organizations, or financial institutions. Scammers purporting to be from the FDIC or FDIC OIG may use the FDIC or FDIC OIG's seal or logo to make their demand for funds appear to look legitimate. The FDIC and FDIC OIG will not send unsolicited correspondence asking for sensitive personal information or demanding payment through gift cards, wire transfers, or digital currency.

In an effort to prevent the public from falling prey to such schemes, the FDIC OIG has produced a video podcast featuring the FDIC OIG's Chief of Staff who interviews one of the OIG's Special Agents in Charge, along with a second video featuring the FDIC OIG's AIGI. These videos are available at https://www.fdicoig.gov/impersonation-scams. We strongly advise the public to "HALT." That is:



A second and sometimes related scam involves fictitious FDIC websites. The FDIC OIG is warning banks and bank customers about **Misrepresentation** schemes targeting consumers using such fake FDIC websites. And this is how it works:

- Fraudsters impersonating the FDIC, FDIC OIG, or the FBI contact consumers stating their financial accounts were compromised and that officials at their financial institution are under investigation.
- Victims are asked to secure their funds and are directed to transfer money to a purported "FDIC-managed" secure account.
- Victims are then sent information through email with a link to a fictitious website that includes an "FDIC case number," a point of contact, and login information.

- The fictitious websites have FDIC somewhere in the name and provide the victim with false account information displaying the funds provided.
- Fictitious FDIC websites may appear legitimate, with layouts similar to the official fdic.gov website, with the same color or fonts, but the URLs to these sites will not end in a .gov.

We strongly advise the public:

- Do not agree to make bank transfers or provide funds (cash, gold bars, digital currency) when contacted by an unknown individual.
- If you are unsure about whether or not an unsolicited phone call from an unknown individual claiming to be from the FDIC, FDIC OIG, or the FBI is legitimate, hang up and contact the agency directly using contact information from the official .gov website.
- Do not use any contact information provided by the unknown individual who contacted you (including visiting a website provided or contacting them using a phone number or text message provided by the unknown individual).
- Do not give anyone your bank account credentials or PIN.
- Do not meet unknown individuals in person and never allow an unknown individual to visit your home or meet you at a bank branch.
- Stop communication immediately if an unknown individual asks for assistance with financial transactions.

If you suspect you have been a victim of either of these scams, please contact the FDIC OIG Hotline.



Don't become the victim of a scammer.
View our videos: https://www.fdicoig.gov/impersonation-scams

Case Highlights

The cases discussed below are illustrative of some of the OIG's investigative success during the reporting period. They are the result of efforts by FDIC Special Agents and support staff in Headquarters, Regional Offices, and the OIG's ECU. As noted, these cases reflect the cooperative efforts of OIG investigators, FDIC Divisions and Offices, other OIGs, USAOs, and others in the law enforcement community throughout the country. These working partnerships contribute to ensuring the safety and soundness of the Nation's banks, strengthen our efforts to uncover fraud in the Federal pandemic response, and help promote integrity in the FDIC's programs and activities.

Guilty Plea in Contract Fraud Scheme

On September 2, 2026, in the U.S. District Court for the District of Columbia, Richeline Fung pled guilty to one count of 18 U.S.C. § 287 (False, Fictitious, or Fraudulent Claims). Fung was charged by Criminal Information on July 28, 2026 for her role in a contract fraud scheme involving simultaneous or 'double billing' across several government contracts while working on separate government contracts and/or employed directly by other government agencies, which was contrary to the terms and conditions of the contracts.

Beginning in January 2019, and continuing through at least June 2025, Fung and others carried out a scheme whereby overlapping hours were billed across multiple contracts with government agencies for human resources duties (including the migration of FDIC and FDIC-OIG personnel documents to the eOPF). The group actively sought positions on multiple government contracts despite restrictions in their terms of employment on the ability to work on outside matters while performing the duties of each respective contract. In some instances, Fung and others billed more than 30 hours in a single day across multiple contracts. Additionally, Fung served as a career permanent employee at the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS-CISA) while simultaneously working on six other government contracts. One of Fung's co-conspirators worked as a career permanent GS-15 at DHS-CISA and another worked as a career permanent GS-14 at the agency, while a third worked as a career permanent GS-13 at the Department of Housing and Urban Development during the scheme. All four were paid salaries from their respective agencies while simultaneously billing for the alleged work across the various separate government contracts.

Digital and residential search warrant operations revealed the scheme was carried out, in part, by using external devices to mimic activity on the government laptops issued to Fung and her co-conspirators for their contract work. During one such search warrant operation, multiple laptops for different agencies were observed, open, and signed in simultaneously in the home office of one of the co-conspirators.

Proceeds of the scheme were used to purchase multiple properties in the National Capital Region, fund lavish vacations, and open small human resources businesses that were eventually used to further the scheme by serving as subcontractors on contracts with federal agencies. The loss to the government attributed to Fung was approximately $245,252.

Source: Based on a request for assistance from AmeriCorps OIG's Office of Investigations.
Responsible Agencies: FDIC OIG joint investigation with AmeriCorps OIG, FBI, Defense Criminal Investigative Service, DHS OIG, Health and Human Services OIG, General Services Administration OIG, Treasury Inspector General for Tax Administration (TIGTA), Housing and Urban Development OIG, Energy OIG, and Pension Benefit Guaranty Corporation OIG.
Prosecuted by the USAO, District of Columbia.

Former Federal Contractor Found Guilty

On May 7, 2026, former federal contractor Sohaib Akhter (Sohaib) was found guilty by a jury for his role in a conspiracy to destroy government databases hosted by a Federal government contractor (Company 1). Sohaib was also found guilty of password trafficking regarding information from a computer hosting Equal Employment Opportunity Commission (EEOC) data and possession of a firearm by a prohibited person. Sohaib was indicted on November 13, 2025, for conspiring to delete databases used to store United States (U.S.) government information and password trafficking. On January 5, 2025, a superseding indictment was filed for possession of a firearm by a prohibited person and witness tampering. Sohaib has a sentencing date currently scheduled for December 2026.

In early February 2025, the FDIC OIG began investigating Sohaib and his twin brother Muneeb Akhter (Muneeb) for allegedly accessing FDIC OIG information without obtaining the proper background checks from FDIC's Security Enterprise Programs Section. The FDIC OIG notified the Federal contractor (Company 1), who subsequently elected to terminate Muneeb and Sohaib. On February 1, 2025, Muneeb asked Sohaib for the plaintext password of an individual who submitted a complaint to the EEOC's Public Portal, which was maintained by the Akhters' employer. Sohaib conducted a database query on the EEOC database and then provided the password to Muneeb. This password was subsequently used to access that individual's email account without authorization.

When the company discovered Sohaib's prior felony conviction, it terminated both brothers' employment during an online remote meeting on February 18, 2025. Immediately after being fired during this meeting, the brothers sought to harm their employer and its U.S. government customers by accessing computers without authorization, write-protecting databases, deleting databases, and destroying evidence of their unlawful activities. The compromised information included case management and Freedom of Information Act response processing software. Over the course of several hours, the brothers deleted approximately 96 databases storing U.S. government information hosted by the company.

A search of Sohaib's cellphone revealed that he had obtained firearms as early as January 2025 and, following the execution of an FDIC OIG-led search warrant on March 12, 2025, took steps to sell them. On March 18, 2025, Sohaib drove to a firearms company in Farnham, Virginia, with his domestic partner, who completed paperwork for a transaction to sell the company seven firearms. As a convicted felon, Sohaib could not legally possess firearms.

Source: Based on a referral from the FDIC.
Responsible Agencies: The FDIC OIG ECU conducted this investigation jointly with the DHS OIG and Homeland Security Investigations (HSI). Valuable assistance was provided by Agriculture OIG; Department of Education OIG; Environmental Protection Agency OIG; EEOC OIG; Federal Reserve Board (FRB) OIG; Health and Human Services OIG; DHS Office of the Chief Security Officer; Housing and Urban Development OIG; Interior OIG; International Development Finance Corporation OIG; DOJ OIG; Labor OIG; Nuclear Regulatory Commission OIG; Small Business Administration (SBA) OIG; TIGTA; Veterans Affairs OIG; U.S. Capitol Police; and the Fairfax County Police Department (PD), Virginia.
Prosecuted by the USAO, Eastern District of Virginia and the Computer Crimes and Intellectual Property Section.

Former Bank President and CEO Pleads Guilty

On May 6, 2026, Danny Seibel pled guilty in U.S. District Court for the Western District of Oklahoma to one count of bank fraud related to his actions to defraud The First National Bank of Lindsay (FNBL). A sentencing date has not been set.

Seibel served as the President and Chief Executive Officer of FNBL from February 2007 until his termination in September 2024. Seibel also held other management roles at FNBL, including Chief Financial Officer and Bank Secrecy Act Officer. Seibel issued loans to certain FNBL borrowers that the borrowers never repaid. Some borrowers were unaware Seibel failed to record loans, posted fake loans to accounts, and made false entries on their loans and deposit accounts. Seibel frequently manipulated bank records to make it appear loans were current and deposit accounts were not overdrawn. Often, Seibel disbursed loan proceeds without recording the loans in the bank's software system. As a result, financial records submitted to the Board of Directors and in Call Reports, were often misstated.

Several unnamed borrowers allegedly conspired with Seibel and were aware of Seibel's tactics and the financial benefit they received. On several occasions, they asked Seibel to "fix" or add funds to their overdrawn accounts. Seibel then made manual entries, without recording a loan or receiving a legitimate deposit. During the August 2024 bank examination, Seibel provided the Office of the Comptroller of the Currency with a false and fraudulent Daily Maintenance Report which omitted hundreds of changes Seibel manually made to due dates, maturity dates, and times past due on numerous loans. On October 18, 2024, FNBL was closed by the Office of the Comptroller of the Currency, and the FDIC was appointed receiver. The initial estimate of the loss to the DIF was $42.3 million.

Source: FDIC's Division of Resolutions and Receiverships.
Responsible Agencies: Joint investigation by the FDIC OIG, FBI, Federal Housing Finance Agency OIG, and Internal Revenue Service-Criminal Investigation (IRS-CI).
Prosecuted by the DOJ Money Laundering, Narcotics and Forfeiture Section and the USAO for the Western District of Oklahoma.

Alibaba Group and AUS Merchant Services Agree to Pay $600 Million to Resolve DOJ Allegations

Alibaba Group Holding Limited (Alibaba) and its U.S.-based payment processor, AUS Merchant Services Inc. (AUS, and formerly known as Alipay US), entered a non-prosecution agreement to pay $600 million to resolve the Justice Department's allegations that they violated the Federal Food, Drug, and Cosmetic Act (FDCA) by failing to prevent merchants from selling and importing illegal pharmaceuticals, controlled substances, listed chemicals, and pill presses into the U.S. through the Alibaba.com and AliExpress.com e-commerce platforms and for failing to have an adequate anti-money laundering compliance program.

As part of the non-prosecution agreement, Alibaba and AUS accepted responsibility for the acts of their officers, directors, employees, and agents in connection with their conduct. Alibaba agreed to pay a criminal monetary penalty of $125 million and to forfeit $200 million. AUS agreed to pay a criminal monetary penalty of $85 million and to forfeit $190 million. Alibaba and AUS also agreed to enhance their compliance programs and to continue cooperating with the department in any ongoing or future criminal investigation relating to this conduct.

Alibaba operates e-commerce platform Alibaba.com, one of the world's largest business-to-business (B2B) online marketplaces, and e-commerce platform AliExpress.com, a global business-to-consumer online marketplace. AUS is a subsidiary of Ant Group, which operates Alipay, one of the largest mobile and digital payment platforms in the world.

Alibaba admitted that, between January 2016 and December 2024, it failed to prevent merchants using its Alibaba.com and AliExpress.com platforms from engaging in approximately 80,000 product sales involving imports into the U.S., including List I and II chemicals, pharmaceuticals, and pharmaceutical counterfeiting equipment. These sales violated the FDCA and other federal laws. The combined gross merchandise value of these transactions exceeded $200 million. During the investigation, federal law enforcement conducted over 40 undercover purchases of pharmaceuticals and counterfeiting equipment that were illegal to be imported into the U.S.

Although Alibaba maintained policies restricting the sale of prohibited products on Alibaba.com and AliExpress.com, employees raised concerns that the company's compliance controls were inadequate and failed to prevent the sale and importation of illegal products. Alibaba also provided merchants and buyers with a private, in-platform messaging service that some merchants used to facilitate unlawful transactions. In some instances, merchants used Alibaba's messaging service to direct buyers to third-party encrypted messaging platforms to facilitate those unlawful transactions. Alibaba derived some profit related to those sellers' illegal activities on Alibaba.com by charging membership, marketing, advertising, shipping, and payment-processing fees.

AUS admitted that, between January 2020 and December 2023, it accepted U.S. dollar-denominated payments through credit cards and wire transfers routed through U.S. bank accounts held at Citibank and J.P. Morgan Chase before transferring the funds offshore for settlement on behalf of its customers. When AUS implemented its own transaction-monitoring system for those transactions, it failed to fully incorporate certain wire-transfer data. As a result, its transaction monitoring did not always identify transactions involving payments from high-risk jurisdictions or multiple payors on a single invoice.

Additionally, AUS admitted that its anti-money laundering compliance program failed to prevent some Alibaba merchants from using its payment processing and settlement services to facilitate the sale and importation of prohibited products into the U.S. In certain instances, rather than systematically restricting merchants identified as selling prohibited merchandise, AUS instead reported those merchants to Alibaba. In at least one instance, a merchant subsequently continued selling prohibited products to U.S. buyers after AUS had investigated and reported the merchant.

Source: The Food and Drug Administration (FDA) Office of Criminal Investigation's Rhode Island Task Force.
Responsible Agencies: FDIC OIG joint investigation with the FDA Office of Criminal Investigation's Rhode Island Task Force, IRS-CI's Global Illicit Financial Team, the Homeland Security Task Force New York-Financial, and the U.S. Postal Inspection Service.
Prosecuted by the USAO for the District of Rhode Island, the Civil Division's Enforcement and Affirmative Litigation Branch, DOJ's Money Laundering, Narcotics and Forfeiture Section, and the FDA's Office of the Chief Counsel.

Guilty Plea in Account Takeover and Check Fraud Scheme

On September 4, 2026, Ariana De Los Angeles Rodriguez Faria pled guilty in the Southern District of Florida to one count of 18 U.S.C. § 1349 (Conspiracy to Commit Mail and Wire Fraud). Rodriguez Faria was previously indicted on July 7, 2026. This investigation involves account takeover and check fraud schemes totaling approximately $9 million with victims throughout the U.S. and Mexico. Six defendants have been charged in conjunction with this investigation.

From approximately May 2024 through January 15, 2025, Rodriguez Faria, along with other co-conspirators, participated in an organized account takeover scheme. During this period, the co-conspirators unlawfully obtained access to multiple victims' bank accounts. After gaining unauthorized access, the co-conspirators requested and caused new checkbooks associated with the victims' accounts to be issued and mailed to addresses under their control. Upon obtaining the fraudulently issued checkbooks, the co-conspirators deposited checks drawn on the victims' accounts into bank accounts they controlled for their personal financial gain and to further the scheme. Faria's involvement resulted in an estimated loss of at least $786,000 across eight compromised victim accounts.

Source: HSI Miami – El Dorado Task Force.
Responsible Agencies: FDIC OIG joint investigation with HSI, IRS-CI, TIGTA, and U.S. Postal Inspection Service.
Prosecuted by the USAO, Southern District of Florida.

Sentencing in Fraud and Money Laundering Scheme Targeting Elderly Victims

On May 8, 2026, Zhao Wang, a/k/a "Oscar," was sentenced in the Southern District of California to 151 months in prison for leading a $27 million fraud and money laundering scheme targeting approximately 2,000 elderly victims across the U.S. Wang, a Chinese national, is the lead defendant charged in a five-defendant indictment unsealed in 2024. Previously, Wang pled guilty to Conspiracy to Commit Mail and Wire Fraud (18 U.S.C. 1349), as well as Conspiracy to Launder Monetary Instruments (18 U.S.C. 1956(a)(1)(A)(i), 1956(a)(1)(B)(i) and 1956(h)).

Members of the conspiracy operated a series of bank and government impersonation, technical support, and refund scams targeting elderly victims (including impersonating the FDIC). Victims received unsolicited phone calls, emails, and pop-up ads directing victims to call a phone number. Unbeknownst to the victims, those phone numbers belonged to India-based scam call centers. Once a victim called the call center, members of the conspiracy used social engineering techniques to build trust with the victim. In many instances, the conspirators had victims download commercially available remote desktop software, which the conspirators used to access victims' computers and to carry on the scams.

One of the most frequent scams was a refund scam. In the refund scams, victims were told they were entitled to a small refund, for example, from a retailer for an alleged unauthorized charge. While pretending to process the refund, the victim would be accidentally "over-refunded" money. The conspirators would then instruct the victim to send the alleged over-refunded money through wire transfers or in cash via express mail to members of the conspiracy. In reality, the victims had not been refunded any money and victims were scammed into sending their own money.

After building trust with a victim, the conspirators would induce victims to send money to members of the conspiracy in the U.S., in locations throughout Southern California, Nevada, and elsewhere. The money was sent to members of the conspiracy, including Wang, either by wire transfers or most often as bulk cash via express mail packages. When a victim was duped into sending bulk cash in the mail, defendant Wang would provide his India-based co-conspirators a fictitious name plus an address of a retail location that could accept express mail packages. Those names and addresses would then be relayed to the victims, who were instructed to express mail the bulk cash. Then, once a victim had sent the cash in the mail, Wang and his co-conspirators would use fake IDs to get the packages of cash sent by the elderly victims.

Wang also admitted that after receiving the fraud proceeds, he and his co-conspirators laundered the money using cryptocurrency back to their foreign-based counterparts. Wang took upwards of 18 percent of the fraud proceeds and transferred the rest via cryptocurrency to his co-conspirators. Further, Wang admitted that he laundered the proceeds to promote the fraud scheme by using fraud proceeds to pay co-conspirators and to purchase the fake IDs used in the scheme.

Wang and his four co-defendants were charged by indictment in June 2024. In August 2024, Federal agents conducted a nationwide takedown operation, which led to Wang's arrest in Las Vegas, Nevada.

Source: FBI.
Responsible Agencies: FDIC OIG, FBI, HSI, San Diego County District Attorney, San Diego Sheriff Department, San Diego PD, San Diego Elder Justice Task Force, Chino PD, Coronado PD, Escondido PD, Glendora PD, Long Beach PD, Orange County Sheriff Department.
Prosecuted by the USAO, Southern District of California.

Former CFO Sentenced to 36 Months in Prison for Bank Fraud Scheme

On July 13, 2026, Aaron Luneke, former Chief Financial Officer of Bank of the Valley (BOV), was sentenced to 36 months in prison and 60 months of supervised release for his role in a bank fraud scheme. On March 6, 2026, Luneke was found guilty on two counts of bank fraud after a two-week trial in the District of Nebraska. Luneke was previously indicted by a federal grand jury on July 15, 2024.

From approximately August 2018 to May 2022, Luneke served as the Chief Financial Officer of BOV, headquartered in Bellwood, Nebraska. During his time as CFO of BOV, Luneke and his business partner(s), through the business entity, Living Waters RE, LLC, constructed a drive-thru carwash in Columbus, NE, which was financed by BOV. In approximately February 2021, Luneke sought an SBA loan from Stearns Bank, St. Cloud, MN, which would have refinanced the carwash from BOV to Stearns Bank, along with an SBA guarantee, through financing of approximately $3.5 million.

During the underwriting period of the loan with Stearns Bank, Luneke obtained and attempted to utilize fraudulent and inflated invoices, from a contractor and an electrician who worked on the carwash project, to increase the valuation of Living Waters RE, LLC to meet requisite loan-to-value thresholds. Additionally, Luneke failed to report outstanding debts to family members in his loan application and communications with Stearns Bank. Stearns Bank ultimately did not make the SBA loan to refinance the BOV loan.

From approximately April 2021 to June 2021, Luneke sought financing from BOV which included additional funds for the project. Luneke further utilized the fraudulent invoices from the contractor and electrician when securing financing at BOV and the fraudulent invoices were used as a basis for additional construction proceeds. BOV funded the request in the form of two loans totaling $4.3 million.

Source: FDIC Division of Risk Management Supervision.
Responsible Agencies: Joint FDIC OIG investigation with the Federal Housing Finance Agency OIG, FRB OIG, and the FBI.
Prosecuted by the USAO for the District of Nebraska.

Sentencing for Conspiracy to Launder Drug Proceeds

On April 29, 2026, Georgina Banuelos was sentenced in the Northern District of Illinois to 20 months in prison for conspiring to launder drug proceeds for an international drug trafficking organization, in violation of 18 USC 1956(h). Additionally, Banuelos was ordered to forfeit $5,000 in funds traceable to the offense.

Banuelos was employed as a teller at The Fountain Trust Company in Northwest Indiana. Beginning no later than 2018, Banuelos conspired with fellow Fountain Trust Company teller Ilenis Zapata, as well as flight attendant Glenis Zapata, to launder drug proceeds for the Espinosa Drug Trafficking Organization. Specifically, Banuelos and Ilenis Zapata used their positions as bank insiders to convert small denomination bills from drug proceeds into large denomination bills through the vault at The Fountain Trust Company. Converting the small denomination bills into large denomination bills allowed flight attendant Glenis Zapata to transport higher amounts of currency in her carry-on baggage to the southern border of Texas. Banuelos charged a fee of $150 for each $10,000 converted and agreed in her plea agreement to converting at least $1.6 million between 2018 and March 2022.

Source: IRS-CI.
Responsible Agencies: Joint FDIC OIG investigation with the Drug Enforcement Agency and IRS-CI.
Prosecuted by the USAO for the Northern District of Illinois.

Former AT&T Employee Sentenced for Role in SIM Swap Scheme

On September 8, 2026, Kenneth Carter, a former AT&T store employee, was sentenced to 16 months in federal prison and was ordered to pay $99,528 in restitution. On March 24, 2026, Carter pled guilty to one count of conspiracy to commit wire fraud and bank fraud, in violation of 18 U.S.C. § 1349. He had previously been indicted and arrested for his role in transferring victim phone numbers to other devices to bypass two-factor authentication as part of an elaborate bank fraud and wire fraud scheme.

Beginning in 2018 and continuing through 2020, multiple victims' cellular phone accounts were deactivated and re-activated to different phones, a process called "SIM swapping," in furtherance of fraudulent bank account transfers. "SIM swapping" is a technique in which a criminal fraudulently induces a mobile carrier to reassign a cell phone number from the legitimate subscriber's Subscriber Identity Module (SIM) card to a SIM card controlled by another without the legitimate subscriber's authorization or knowledge. This process allows a criminal to intercept two-factor authentication codes sent to the victim via phone call or text message, and to gain access to the victim's various accounts.

Carter, while working as an AT&T employee, was recruited to facilitate these SIM swaps on AT&T customer accounts, using his AT&T employee access to customer records. While those victims' phones were switched, co-conspirators attempted to make large wire transfers from those victims' bank accounts. PayPal records reflect multiple payments from a known Russian leader and co-conspirator in the scheme, to Carter and other co-conspirators who facilitated the SIM swaps.

Multiple customers of JPMorgan Chase Bank, Regions Bank, Bank of America, and PNC Bank are victims of this scheme, estimated to involve over $2 million in fraudulent transactions. This case represents a serious threat to financial institutions that utilize online banking and two-factor authentication for their customers.

Source: FBI.
Responsible Agencies: FDIC OIG joint investigation with the FBI, IRS-CI, and HSI.
Prosecuted by the USAO, Central District of California.

Payment Processor Sentenced for $14 Million Wire Fraud Scheme

On July 20, 2026, Jeremy Todd Briley, a payment processing broker who facilitated stealing money from businesses' bank accounts, was sentenced to 3 years in prison. In April 2026, he pled guilty to one count of wire fraud. Through his scheme, sham merchants stole and attempted to steal $14 million from victims' bank accounts.

Briley, of Happy Valley, Oregon, worked as a payment processing broker. Acting on behalf of clients (merchants), he identified payment processors in the U.S. for his clients to use in processing charges. His two largest clients were sham companies that falsely represented that they provided online marketing services to businesses. Instead, they stole from victims by fraudulently debiting their bank accounts, causing over $14 million in unauthorized debits and attempted debits.

From February 2017 to December 2023, Briley obtained and maintained payment processing relationships for those sham companies so that they could process fraudulent debits, knowing that the sham companies were fraudulently debiting bank accounts. Despite repeatedly receiving information that the debits processed on behalf of the sham companies were not authorized by the victims, Briley concealed the fraudulent activities of the sham companies in various ways, and he arranged for a payment processor to deceive banks by manipulating return rates on the fraudulent debits.

In addition to the prison sentence, Briley was also sentenced to 3 years of supervised release and ordered to forfeit $460,000 in proceeds of the fraud.

Source: Department of Justice Consumer Protection Branch.
Responsible Agencies: FDIC OIG joint investigation with the U.S. Postal Inspection Service.
Prosecuted by the DOJ Consumer Protection Branch.

Fraud Promoter Pleads Guilty to Bank Fraud

On May 7, 2026, Shamarri Tache Brooks, a/k/a Juney Knotzz of Atlanta, Georgia pled guilty to Federal bank fraud and aggravated identity theft charges in connection with a scheme arising from the widespread theft of checks from the mail.

According to the indictment and other information presented in court, from at least January 2022 through November 2025, Brooks committed bank fraud by negotiating checks stolen from the mail. As part of the scheme, he used social media to recruit individuals with existing bank accounts to use as depository accounts for stolen checks. Brooks altered the stolen checks to list the cooperating accountholders as the intended recipients or payees of the checks. Brooks deposited altered checks at ATMs throughout the Atlanta area, often wearing balaclava-style masks with a logo stating "No Free Sauce." Brooks also promoted and sold tutorials for committing various forms of financial fraud, including check fraud. He sold a collection of these tutorials under the name "Sauce Book" or "SB." Brooks also sold images of stolen checks, referred to as "slips," as a part of his fraud business.

When law enforcement arrested Brooks earlier this year, they recovered over 600 stolen checks from his residence.

Source: Dunwoody, Georgia, PD.
Responsible Agencies: FDIC OIG joint investigation with the FBI, Postal Service OIG, and U.S. Secret Service.
Prosecuted by the USAO, Northern District of Georgia.

Special Feature

Money Mules Fraud Alert

The FDIC OIG is warning the public about criminals utilizing "money mules" to commit and facilitate fraud and other illicit activity through the U.S. financial system. Money mules can be criminally prosecuted and held financially accountable for victims' losses. Avoid becoming a Money Mule!

What is a Money Mule?

Criminal organizations routinely use "money mules" to move proceeds of fraud, scams, and other illicit activity through the U.S. financial system. A money mule is any person who transfers or receives funds at the direction of another, knowing—or being unaware—that the money is tied to criminal activity. This includes individuals moving funds electronically as well as couriers sent to pick up cash, precious metals, or other assets directly from victims of fraud schemes, a tactic increasingly used in scams targeting the elderly.

Money mule networks enable billions of dollars in losses each year across the U.S.[1] The victims whose funds flow through mule accounts are frequently older adults targeted through romance scams, "pig butchering" cryptocurrency schemes, tech support fraud, and government or bank employee impersonation schemes, including FDIC and FDIC OIG impersonation schemes.[2]

How it Works:

Fraudsters typically utilize money mules in multiple ways:

- **Victim to Mule Transfers:** Criminals convince victims—often elderly, college students, or financially vulnerable individuals—to send money under false pretenses. The funds are directed to mule accounts rather than directly to the criminals to obscure identities. In some schemes, criminals dispatch couriers to physically retrieve cash, gold, or other valuables from victims, sometimes posing as law enforcement or bank officials.
- **Recruitment of Mules:** Criminals recruit money mules intentionally (witting) or through deception (unwitting). Recruitment commonly targets job seekers by offering convenient remote work opportunities, often as a rebates or payments processor.[3] Criminals often target students, those looking for work, those on dating websites, the elderly, and individuals experiencing financial hardship, but anyone can be approached to be a money mule.[4]

Once a mule receives the funds – or collects physical assets – the individual is instructed to withdraw cash, buy cryptocurrency, purchase gift cards, transfer funds through additional accounts, or send money overseas. These layering transactions conceal the illicit origin of the funds.

Special Feature (continued)

Red Flags

Common indicators of money mule activity—both for potential scam victims and for people being recruited—include:

- Being asked to use a personal bank account to receive or move money for someone you have never met in person.
- Job postings involving "payment processing" or "funds transfer" work, especially if they require using your own bank account or opening a bank account specifically for the funds transfer processing.
- Unsolicited messages from strangers – potential romantic partners, investment advisers, or purported government officials – directing you to handle funds.
- Pressure to act quickly, secrecy about the reason for the transaction, or inconsistent explanations.
- Funds arriving from multiple unrelated individuals (often older adults), followed by rapid outgoing transfers.
- Requests to convert funds to cryptocurrency, gift cards, wire transfers, or cash withdrawals.
- Being told to hand over cash, gold, or other valuables to a courier sent to your home, especially when the caller claims to be a government or bank employee.

What Happens if You Participate as a Money Mule

- Prosecution for participating in illegal money movement activity.
- Personal liability for repaying victims' losses.
- Exposure of personal information that criminals may later misuse.
- Inaccessible bank accounts and potential long term credit impacts.

Protect Yourself

Individuals can reduce their risk of becoming victims or unwitting participants in a money mule scheme by taking the following steps:

- Never use your personal bank account to receive funds for someone you do not know and trust. Legitimate employers do not require this type of activity.
- Be cautious of unsolicited job offers or online opportunities promising easy money, especially those requiring minimal skills or personal information.
- Verify the identity of anyone requesting financial help or investment activity. Scammers frequently impersonate government agencies, bank employees, and law enforcement.
- Talk to family members – especially older relatives – about romance scams, cryptocurrency investment fraud, and government impersonation schemes.

- Review the available free and online FDIC "Money Smart" resources to learn how to avoid and report identity theft, frauds, and scams.
- Report suspicious activity immediately to your bank and to law enforcement. Early reporting helps limit financial loss and may prevent the use of your account in further criminal activity.
- If you believe you have been recruited as a money mule, stop all transactions at once. Do not send or return funds. Contact your bank and report the incident to the FBI's Internet Crime Complaint Center (IC3.gov), the FTC (reportfraud.ftc.gov), and the FDIC OIG Hotline (fdicoig.gov/oig-hotline).

Additional Resources

- FTC Money Mule Consumer Alert: https://consumer.ftc.gov/consumer-alerts/2020/03/whats-money-mule-scam
- FDIC Money Smart: https://www.fdic.gov/consumer-resource-center/2024-12/december-2024-money-smart-newsletter
- U.S. Computer Emergency Readiness Team: https://www.us-cert.gov/sites/default/files/publications/money_mules.pdf
- FBI Money Mule Public Service Announcement: https://www.ic3.gov/PSA/2021/PSA211203

Red Flags for Financial Institutions:

- Unexpected changes in customer account behavior, including large deposits followed by rapid transfers or withdrawal of funds, including out of state or international transactions.
- Use of synthetic, stolen or fictitious identities to open bank accounts, followed by the deposit and immediate funds withdrawal of large checks, which are returned as fraudulent or non-sufficient funds.
- Deposits from multiple seemingly unrelated parties into an individual's account followed by the rapid conversion of funds to cryptocurrency or prepaid cards.

[1] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

[2] https://www.fdicoig.gov/sites/default/files/document/2022-08/oigimpersonationscamflyer.pdf

[3] https://www.ic3.gov/PSA/2010/WorkAtHome.pdf

[4] https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules

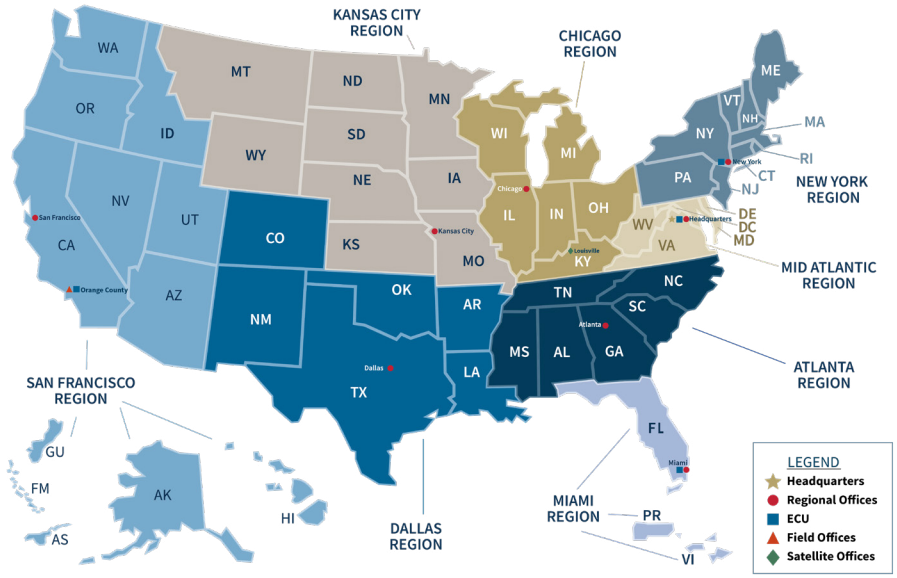
Strong Partnerships with Law Enforcement Colleagues

The OIG has partnered with various USAOs throughout the country in bringing to justice individuals who have defrauded consumers, the FDIC, or financial institutions within the jurisdiction of the FDIC, or criminally impeded the FDIC's examination and resolution processes. The alliances with the USAOs have yielded positive results. Our strong partnership has evolved from years of hard work in pursuing offenders through parallel criminal and civil remedies resulting in major successes, with harsh sanctions for the offenders. 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.

During the reporting period, we partnered with USAOs in judicial districts in 52 locations in the U.S.

Alabama	Kentucky	New York
California	Louisiana	North Carolina
Colorado	Maryland	Pennsylvania
District of Columbia	Michigan	Rhode Island
Florida	Minnesota	South Carolina
Georgia	Mississippi	Tennessee
Idaho	Missouri	Texas
Illinois	Montana	Virginia
Indiana	Nevada	West Virginia
Iowa	New Hampshire	Wisconsin
Kansas	New Jersey	Wyoming

We also worked closely with DOJ, including the Criminal Division, Main Justice; the FBI; other OIGs; other Federal, state, and local law enforcement agencies; and FDIC Divisions and Offices as we conducted our work throughout the U.S during the reporting period.



OIG Regional Map

Keeping Current with Criminal Activities Nationwide

The FDIC OIG participates in the following bank fraud, mortgage fraud, cyber fraud, and other working groups and task forces throughout the country. We benefit from the perspectives, experience, and expertise of all parties involved in combating criminal activity and fraudulent schemes nationwide.

New York Region	Newark Suspicious Activity Report (SAR) Review Task Force; El Dorado Task Force - New York/New Jersey High Intensity Drug Trafficking Area; South Jersey Bankers Association; New York External Fraud Group; Eastern District of Pennsylvania Money Laundering Working Group; New Jersey Security Association; Long Island Fraud and Forgery Association; Connecticut USAO Bank Secrecy Act Working Group; Connecticut Digital Assets Working Group; South Jersey SAR Task Force; Pennsylvania Electronic Crimes Task Force; NJ COVID-19 Fraud Task Force; Newark IRS-CI Financial Fraud Working Group; Western District of New York Payment Protection Program Working Group; District of New Hampshire USAO SAR Review Team; Financial Fraud Investigation Partnership with Southern District of NY; NY Cyber Confidence Fraud Schemes Working Group; Maryland Association for Bank Security; Virginia Crime Analysis Network; Florida Crime and Intelligence Analyst Association.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force; Northern District of Georgia Mortgage Fraud Task Force; Eastern District of North Carolina Bank Fraud Task Force; Northern District of Alabama Financial Fraud Working Group; Northern District of Georgia SAR Review Team; Middle District of Georgia SAR Review Team; South Carolina Financial Fraud Task Force; Eastern District of North Carolina Financial Crimes Task Force; Western District of North Carolina Financial Crimes Task Force; Middle District of North Carolina Financial Crimes Task Force.
Miami Region	COVID Working Groups-Southern District of Florida, Middle District of Florida, Northern District of Florida; SAR Review Groups-Miami, Palm Beach, Treasure Coast Financial Crimes Review Team, Key West/Monroe County; DOJ-COVID-19 Fraud Strike Force- Miami.
Kansas City Region	Kansas City SAR Review Team; USAO for the District of Montana's "Guardians Project;" St. Louis SAR Review Team; Minnesota Inspector General Council; Minnesota Financial Crimes Task Force; Nebraska SAR Review Team; Southern District of Iowa SAR Review Team; Iowa Agricultural Task Force in USAO-Northern District Iowa and USAO-Southern District Iowa (joint collaboration with U.S. Department of Agriculture OIG, FBI, FRB OIG, and FDIC OIG).
Chicago Region	Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Central District of Illinois Financial Fraud Working Group; Northern District of Illinois SAR Review Team; Cook County Region Organized Crime Organization; FBI Milwaukee Area Financial Crimes Task Force; FBI Northwest Indiana Public Corruption Task Force; Eastern District of Wisconsin SAR Review Team; Western District of Wisconsin SAR Review Team; Western District of Wisconsin Bankruptcy Fraud Working Group; Indiana Bank Fraud Working Group; Northern District of Indiana SAR Review Team; FBI Louisville Financial Crime Task Force; Western District of Kentucky SAR Review Team; Eastern District of Kentucky SAR Review Team; Southern District of Ohio SAR Review Team; Michiana Loss Prevention Working Group; AML Financial Institution/LE Networking Group; FBI Chicago Financial Crimes Task Force; Western District of Michigan SAR Review Team; Northern District of Ohio SAR Review Team; Southern District of Indiana SAR Review Team; Financial Crimes Investigators Madison; Financial Crimes Investigators Northeast Wisconsin; Financial Crimes Investigators Northwest Wisconsin; WDKY Bankruptcy Fraud Working Group; Midwest Interagency Supervision Working Group; SEC Interagency Securities Council; OIG Illinois Fraud Working Group; FBI Northwest Indiana Public Corruption Task Force.
San Francisco Region	Fresno Mortgage Fraud Working Group for the Eastern District of California; Sacramento Mortgage Fraud Working Group for the Eastern District of California; Sacramento SAR Working Group; Orange County Financial Crimes Task Force-Central District of California; Orange County SAR Review Team; Northern District of California Money Laundering SAR Review Task Force; San Diego Financial Investigations and Border Crimes Task Force; Northern Nevada Financial Crimes Task Force; Financial Services Roundtable coordinated by the USAO of the Northern District of California; Los Angeles Complex Financial Crimes Task Force – Central District of California; Los Angeles Real Estate Fraud Task Force – Central District of California; Homeland Security San Diego Costa Pacifica Money Laundering Task Force; DOJ National Unemployment Insurance Fraud Task Force; California Unemployment Insurance Benefits Task Force; Nevada Fight Fraud Task Force; Las Vegas SAR Review Team; COVID Benefit Fraud Working Group, USAO District of Oregon; Hawaii Financial Intelligence Task Force.
Dallas Region	Oklahoma City Financial Crimes SAR Review Working Group; Austin SAR Review Working Group; Houston High Intensity Drug Trafficking Area SAR Team; Western District of Oklahoma Economic Crimes Working Group and Fraud/SAR Review Team; Eastern District of Oklahoma White Collar Working Group/SAR Review Team; Northern District of Texas COVID Task Force; District of Colorado COVID Task Force; Southern District of Texas SAR Review Team.
Mid-Atlantic Region	Virginia Crime Analysts Network; Northern Virginia Financial Initiative SAR Review Team; Pandemic Response Accountability Committee (PRAC) Fraud Task Force; PRAC Law Enforcement Coordination Subcommittee; PRAC Data Analytics Subcommittee; CIGIE COVID-19 Working Group; DOJ Stimulus Funds Fraud Working Group; District of Maryland SAR Review Task Force; Western District of Virginia SAR Review Task Force, Roanoke, Virginia; Western District of Virginia SAR Review Task Force, Abingdon, Virginia; Eastern District of Virginia SAR Review Task Force; Central Eastern District of Virginia SAR Review Task Force; Northern Virginia Eastern District of Virginia SAR Review Task Force; DOJ Foreign Corrupt Practices Act SAR Initiative; District of Columbia SAR Review Task Force; Southern District of West Virginia SAR Review Task Force; Northern District of West Virginia SAR Review Task Force; Delaware SAR Review Task Force; Maryland Financial Intelligence Team; Global SAR Task Force via the IRS-CI Global Illicit Financial Team (GIFT); Bank Fraud Working Group, National Capital Region; FBI Maryland Financial Crimes Task Force.
Electronic Crimes Unit	Washington Metro Electronic Crimes Task Force; High Technology Crime Investigation Association; FBI Northern Virginia Cyber Task Force; DOJ Civil Cyber-Fraud Task Force; CIGIE Information Technology Committee; CIGIE Forensic Accountant Networking Group; CIGIE Financial Cyber Working Group; National Cyber Investigative Joint Task Force; FBI Headquarters Money Laundering, Forfeiture & Bank Fraud Unit; FBI Washington Field Office Cyber Task Force; FBI Las Vegas Cyber Task Force; FBI Los Angeles' Orange County Cyber Task Force; Secret Service Cyber Task Force, Newark, New Jersey; Secret Service Miami Cyber Fraud Task Force; Council of Federal Forensic Laboratory Directors; International Organized Crime Intelligence and Operations Center; USSS WFO Task Force; National Cyber Forensics and Training Alliance; HSI Cyber Task Force-San Diego CA, Newark NJ, Charlotte NC.



Other Goal Areas

In addition to the audits, evaluations, investigations, and other reviews conducted during the reporting period, our Office has undertaken other activities in areas that complement and support our audit and investigative efforts. Specifically, our Strategic Goals include three important areas: **strengthening relations with partners and stakeholders; managing and optimizing resources and technology;** and **valuing our people and workplace culture.** A brief listing of some of our key strategies and initiatives in these areas follows.

Strengthening Relations with Partners and Stakeholders.

- Communicated with the FDIC Chairman, other FDIC Board Members, Chief Operating Officer/Chief Financial Officer, and other senior FDIC officials through regularly scheduled meetings with them and through other forums. Attended FDIC Board Meetings and certain other senior-level management meetings to monitor or discuss emerging risks at the Corporation and tailor OIG work accordingly.
- Coordinated with the FDIC Chief of Staff, who now Chairs the Audit Committee, to provide status briefings and present the results of completed audits, evaluations, and related matters for the Audit Committee Chairman's and other Committee members' consideration. Presented the results of OIG audits, evaluations, and other publications, including the OIG's assessment of the Top Management and Performance Challenges at scheduled Audit Committee meetings. Apprised other Board Members accordingly.
- Held meetings with FDIC Division Directors and other senior officials to keep them informed of ongoing OIG reviews, results, and planned work. Also began outreach to Divisions and Offices to hear views on the management and performance challenges facing the FDIC and efforts to address those.
- Continued to enhance and update our external website and other social media presence to provide stakeholders better opportunities to learn about the work of the OIG, the findings and recommendations our auditors and evaluators have made to improve FDIC programs and operations, the results of our investigations into financial fraud, and helpful information to guard against ever-evolving scams.
- Chaired the IG community's Forensics Subcommittee to explore forensics best practices, ensure relevant training, promote collaboration and support among the forensics community, and better define General Schedule forensics career levels.

- Finalized the OIG's video podcast on Impersonation Scams. The intent is to warn members of the public not to become victims of unscrupulous individuals seeking to trick them into giving up personally identifiable information, including bank and credit card account information. Also issued a new Scam Alert on a technique called "ramp and dump." In such a scheme, Chinese or other micro/small-cap non-U.S. companies, typically valued at $15 million or less, with an individual share price of $4-6 at the Initial Public Offering (IPO) will obtain a listing on the NASDAQ and go public, while the bad actors are allocated millions of pre-IPO shares at little to no cost to themselves. Leading up to an IPO event, bad actors will solicit investors through WhatsApp group chats by making false claims about the value and instructing the victims to purchase shares on the day of an IPO at a specific time. The bad actors will then sell the shares they possessed pre-IPO at an inflated value. These "match trades" allow bad actors to sell the shares they were allocated at pre-IPO, resulting in 100 percent profit. Also issued an alert on Money Mules—that is, criminal organizations routinely use "money mules" to move proceeds of fraud, scams, and other illicit activity through the U.S. financial system. A money mule is any person who transfers or receives funds at the direction of another, knowing—or being unaware—that the money is tied to criminal activity. This includes individuals moving funds electronically as well as couriers sent to pick up cash, precious metals, or other assets directly from victims of fraud schemes, a tactic increasingly used in scams targeting the elderly. (See earlier Special Feature on Money Mules.)

- Updated website information on the OIG, OA, and OI by revising and updating information fact sheets for stakeholders on the OIG as a whole and the specific nature, focus, and results and impact of Office of Audits' and Office of Investigations' efforts. Made these fact sheets available for staff distribution when engaging in outreach efforts on behalf of our office.

- Supported efforts of two detailees from OA on an as-needed, part-time basis to work with the Federal Communications Commission OIG's Investigative Support Services. They provided investigative support services for criminal and civil investigations requiring complex bank records review, scheduling, and analysis in close collaboration with the Federal Communications Commission OIG's OI until the end of August 2026. Also provided one of the OIG's Special Agents to assist the Federal Communications Commission OIG by leading criminal investigations in support of that office, a detail that has now concluded.

- Coordinated with DOJ and USAOs throughout the country in the issuance of press releases announcing results of cases with FDIC OIG involvement and informed FDIC senior leadership and other members of FDIC management of case actions, as appropriate.

- Updated our Congressional Protocols to reflect our interactions with the Congress. The purpose is to continue efforts to foster open communications with the Congress and FDIC management and maintain effective working relationships based on professionalism and mutual respect. The document covers our Statutory Authorities and Responsibilities, Mandate for Congressional Communications, Forms of Congressional Communications, and Our Commitments to the FDIC. We shared the protocols with the Chairman and the Office of Legislative Affairs and posted them on our website.

- Maintained congressional working relationships by communicating with various Committee staff on issues of interest to them; providing them our *Semiannual Report to the Congress*; notifying interested Congressional parties regarding the OIG's completed audit and evaluation work; providing staff briefings and responses to inquiries as requested. We briefed Senate Banking Committee Minority staff on workforce optimization and responded to Senators Warren and Van Hollen on that matter. Also briefed Senate Banking Majority staff about the mission and work of the FDIC OIG. We briefed House Financial Services Appropriations staff on budget and debanking issues. We also extended outreach to the Joint Economic Committee of the Congress on the Global Scam Economy. We monitored FDIC-related hearings on issues of concern to various oversight committees and coordinated with the FDIC's Office of Legislative Affairs on Congressional matters pertaining to the OIG, including providing that office a copy of our updated Congressional Protocols, as noted above.

- Maintained the OIG Hotline to field complaints and allegations of fraud, waste, abuse, and mismanagement affecting FDIC programs and operations from the public and other stakeholders. The OIG's Whistleblower Protection Coordinator also helped educate FDIC employees who had made or were contemplating making a protected disclosure as to their rights and remedies against retaliation for such protected disclosures. Our web-based hotline portal at https://www.fdicoig.gov/oig-hotline enhances the efficiency and effectiveness of OIG Hotline operations. It also increases transparency and reporting capabilities that support our efforts to engage and inform internal and external stakeholders. During the reporting period, we handled 1,163 Hotline inquiries, 16 of which led to our opening investigations. Our online form, email, telephone, and regular mail were the most common vehicles for inquiries. An increasing number of such inquiries related to impersonation scams.

- Supported the broader IG community by attending monthly CIGIE meetings and other meetings, such as those of the Integrity Committee, Legislation Committee, Audit Committee (chaired by the FDIC IG), Inspection and Evaluation Committee, Technology Committee, Investigations Committee, Professional Development Committee, Assistant IGs for Investigations, and Council of Counsels to the IGs; responding to requests for information on IG community issues of common concern; and supporting various legislative matters through the CIGIE's Legislation Committee.

- Represented the FDIC OIG as a key member of CIGIE: the FDIC IG serves as Chair of the Audit Committee and is also a member of the CIGIE Strategic Hiring Committee, established in accordance with the Office of Personnel Management's guidance implementing Executive Order 14356. As Chair of the Audit Committee, the IG participates as a member of CIGIE's Executive Council. Our Chief Data and Analytics Officer presented an introduction to Super Intelligence (SI) Governance at CIGIE's Quarterly Audit Committee meeting.

- Participated as a member of the Advisory Board for the Pandemic Response Accountability Committee (PRAC) and supported efforts of the PRAC through active participation in its meetings, forums, and work groups and by playing a key role in collaboration with law enforcement partners in investigations of fraud in pandemic-relief programs.

- Participated as a member of the Council of Inspectors General on Financial Oversight (CIGFO), as established by the Dodd-Frank Wall Street Reform and Consumer Protection Act and coordinated with the IGs on that Council. This Council facilitates sharing of information among its member Inspectors General and discusses ongoing work of each member IG as it relates to the broader financial sector and ways to improve financial oversight. Participated on CIGFO's Working Group related to the Financial Stability Oversight Council's Designation of Non-Bank Financial Companies. (See earlier write-up in Audits, Evaluations, and Other Reviews section.) Also provided the FDIC OIG's input on work related to the broader financial sector to CIGFO for its Annual Report issued in July 2026.

- Communicated and coordinated with the Government Accountability Office (GAO) on ongoing efforts related to our respective oversight roles, risk areas at the FDIC, and issues and assignments of mutual interest. Coordinated with the GAO specifically related to its Congressional request to review the status of IG community senior level staffing shortages and assess the impact over the past 5 years, as well as future operations. The IG made opening remarks at the GAO/CIGIE Financial Statement Conference and joined GAO in issuing updates to volumes of the Financial Audit Manual and revisions to the Federal Information System Controls Audit Manual.

- Coordinated with the Office of Management and Budget (OMB) to address matters of interest related to our FY 2027 budget, and proposed budget for FY 2028.

- Worked closely with representatives of the DOJ, including Main Justice, FBI, and USAOs, along with other law enforcement partners, to coordinate our criminal investigative work and pursue matters of mutual concern. Joined law enforcement partners in numerous financial, mortgage, suspicious activity report review, cyber fraud, and PRAC-related working groups nationwide. (See earlier listings in the Investigations section of this report.) Coordinated with DOJ's National Fraud Enforcement Division. Facilitated and presented at DOJ's Money Laundering, Narcotics and Forfeiture Section event and participated as a panelist with the IRS for the Treasury Executive Office for Asset Forfeiture Symposium.

- Represented the OIG in a wide range of internal and external engagements to strengthen understanding of the OIG's overall mission and efforts to combat fraud, waste, abuse, and promote economy, efficiency, and effectiveness. Among those, joined the FDIC Chairman in issuing a global email regarding National Whistleblower Appreciation Day; presented multiple sessions at the 2026 FDIC, DOJ, Federal Financial Institutions Examination Council's (FFIEC) Financial Crimes Conference; presented to San Francisco Regional Office staff; formed a panel for the FDIC's annual Accounting and Auditing Conference; and taught several FFIEC training sessions. External outreach included to the Federal Reserve Bank of Kansas City's AML Conference; Financial & International Business Association's Regulators Roundtable; Michiana (Michigan and Indiana) Loss Prevention Group; ISACA; American Bankers Association; DHS's Annual Certified Fraud Examiner Seminar; George Mason University, Louisiana Bankers Association School; Mizuho USA; Chicago Title Insurance Corporation, Dallas; and CIGIE's IG Forum on Combatting Fraud.

- Hosted several key stakeholder meetings, including a Senate Banking Committee staff visit and tour of the OIG's ECU, a CIGFO Investigations Working Group Meeting, a meeting of the Bank Fraud Working Group for the National Capital Region, and a meeting with the management team for the FRB/Consumer Financial Protection Bureau OIG to coordinate on 2027 audit and evaluation plans.

- Promoted transparency to keep the American public informed through multiple means: the FDIC OIG website to include, for example, full reports or summaries of completed audit and evaluation work; videos or podcasts; listings of ongoing work; information on unimplemented recommendations; X, formerly known as Twitter, communications to immediately disseminate news of report and press release issuances and other news of note; content on our LinkedIn page; and presence on the IG community's Oversight.gov website, which enables users to access, sort, and search thousands of previously issued IG reports and other oversight areas of interest.

- Ensured transparency of our work for stakeholders on Oversight.gov by posting press releases related to investigative cases and related actions, in addition to posting our audits and evaluations, and updated on an ongoing basis the status of FDIC OIG recommendations remaining unimplemented, those recommendations that have been closed, and those recommendations that we consider to be priority recommendations.

Managing and Optimizing Resources and Technology.

- Monitored spending based on our Congressional Budget Justification for FY 2027 in which we requested a total budget of $42.2 million – a $6.3 million reduction from the FY 2026 enacted level of $48.5 million—or a 13 percent reduction. The President's budget supports $39.2 million for personnel salaries and benefits for 97 full-time equivalents and $3 million for non-personnel expenses.

- Submitted Quarterly Reports on Obligations to OMB, as required by the Consolidated Appropriations Act, 2026, presenting the OIG's budget by object class for various quarters and the percentages obligated as of a certain date.

- Developed a new Case Management Tracking System for OI and trained all Special Agents and other key OIG personnel on the new system, for launch on October 1. Training included the Dashboard, Complaint Creation, Initial Case Actions, Case Spinoffs and Investigations, Judicial Activity, Administrative Activity, Searching and Reporting, and Views. Following the explanations of these features, participants performed user training exercises to drive home the points made earlier. After months of careful planning, analysis, coordination, and training, the new platform meets immediate operational needs, strengthens case tracking, enhances data security, and improves efficiency, reliability, and scalability.

- Announced numerous training opportunities and kept OIG staff apprised of mandatory training requirements in such areas as Ethics, Professional Conduct, Insider Threat and Counterintelligence, Cybersecurity and Privacy Awareness, Records and Information Management, and Workplace Security, and monitored progress of such training. Arranged a Training Day so that staff could complete required training.
- Implemented our Strategic Plan and goals for 2026-2031. The plan establishes areas of focus office-wide to ensure that in carrying out the OIG's statutory mission involving audits and investigations, we strengthen relationships with stakeholders and partners, optimize our administration of resources and technology, and remain focused on the value of our people and workplace culture.
- Made key OIG human resources decisions, including promoting individuals from within the office: promoting two Special Agents to Senior Special Agents, and an Audit Manager to Assistant Inspector General for Audits to lead the Office of Audits.
- Provided our OIG Staffing Plan information to Office of Personnel Management and OMB, as required by Executive Order 14356, "Ensuring Continued Accountability in Federal Hiring" and related Office of Personnel Management and OMB guidance. Coordinated with the FDIC in submitting information jointly.
- Held monthly meetings with Office of Management leadership and staff to keep informed and ensure prudent stewardship and effectiveness of budget, human resources, records management, training, procurement, IT, data analytics, and other administrative operations. Shared updates on such matters with other OIG managers.
- Updated OIG policies in such areas as the OIG Staffing and Hiring Process and Procurement.
- Supported several OIG staff in their pursuit of professional development: the OIG human resources staff member who studied for and passed the Delegated Examining Certification Exam to the benefit of the FDIC OIG's human resources operations; three auditors who achieved the Certified Fraud Examiner certification; and another auditor who became a Certified Cryptocurrency Auditor.
- Leveraged technology in an OA assignment involving incident detection and response as noted earlier by conducting in-house adversary emulation tests using an open-source module and in close coordination with the FDIC's Chief Information Officer Organization and Division of Information Technology. The tests simulated real-world attacks by threat actors in order to uncover risks and security gaps before they impact an organization.
- Updated the OIG's intranet site to inform staff of administrative, facilities, and operational services of importance to OIG staff.

- Continued to expand the use of data and SI to improve the efficiency and effectiveness of operations. Ensured adherence to SI governance policies to improve security, protect the integrity of our oversight capacity, incorporate new innovations into our efforts, and meet the requirements of OMB Memorandum M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*. Also formalized the process for approving and mitigating risks from high-impact SI as designated in the memorandum. Partnered with the FDIC to provision for the expanded use of cloud-based SI tools. Actively used SI tools for data management, natural language processing, machine learning, and data visualization on several audit and investigation pilots. These new features have been used to automate data entry for audits, batch summarize investigative materials for investigations, and assist numerous tasks associated with other OIG functions. Piloted and tested a separate tool that will allow OIG employees to use generative SI on certain sensitive matters as appropriate. The first version of this tool will launch for all OIG employees at the start of FY 2027, with additional functionality upgrades planned throughout the following year.

- Held an office-wide session on CoPilot Chat to explain the new tool for the OIG. This tool is intended to improve productivity and help with collaboration. Explained the tool, reiterated the OIG's policy on SI and certain restrictions on its use; stressed the importance of labeling documents; gave tips on prompts, and went over the requirements for training.

- Carried out a number of information technology (IT) initiatives, including the following: Delivered integrated SI/Machine Learning solutions for the ECU Forensics team to enable more effective and timely analysis during investigative activities; enhanced the FDIC OIG website's search functionality; reviewed data hygiene and security in preparation for the deployment of Copilot Chat, to enable a secure and successful first implementation of agency-wide SI capabilities; provided technical platform support for OI in the migration of sensitive data from the outgoing investigative case management system to the new platform and additional support to OI for implementing the new system; introduced automation to internal OIG business workflows to streamline request processing and improve operational efficiency; completed the first iteration of the OIG Budget Dashboard, with visibility into budget execution, burn rates, and actual spending; enhanced leadership's ability to compare planned vs. actual spending and identify variances; expanded the OIG Human Resources' Key Performance Indicator dashboard with additional workforce metrics to provide greater visibility into staffing levels, workforce trends, retirements, and organizational capacity; refined and standardized off-boarding processes to ensure device information is preserved when required for legal matters and safely redeployed or reused when no longer needed.

- Leveraged the OIG ECU's forensic laboratory. The laboratory allows our field Agents to remotely access a server-based lab environment that allows for the storage and processing of digital evidence into forensic reviewable data. This capability greatly increases the efficiency and effectiveness of the investigative process by allowing for much quicker actuation of data into e-discovery platforms. Our aim is to use industry standard and robust e-discovery platforms to triage and review electronic evidence and robust tools to review mobile technology. We are also exploring the best means to support and partner with other external law enforcement parties.

- Continued to pursue OIG data management strategies and solutions. OIG auditors, criminal investigators, and IT professionals are seeking to ensure that we are leveraging the power of data analytics to inform organizational decision making and ensure we are conducting the most impactful audits, evaluations, reviews and investigations. The OIG continues to migrate mission critical datasets into the data lake, supporting both audits and investigations. Currently, all OIG employees can access cloud-based data management software and machine learning analytical tools. The OIG is piloting AI tools in several audit and investigatory tools to determine the return on investment. The OIG will continuously work to integrate additional data and analytical tools each quarter as resources permit.
- Apprised OIG staff of important IT matters pertaining to their mission-critical work and to ensure the security of information used in conducting their work.
- Met monthly with our Data Analytics and Innovation Working Group members to educate staff on SI and Machine Learning tools currently deployed in the OIG. Coordinated with the FDIC's Chief Artificial Intelligence Officer and Legal Division representatives with regard to use of these tools.
- Coordinated with the FDIC who hosts our external website and made improvements to our site, including an enhanced search function and updated additional items of importance to stakeholders.
- Advanced the OIG's data analytics capabilities related to Payment Protection Program fraud through collaboration with the PRAC, FDIC, Federal Trade Commission, DOJ, FBI, and private-sector entities. Additionally, the OIG is continuing to expand our access to data related to commercial real estate and agriculture to detect bank fraud and threats to the integrity of the banking system.
- Relied on the OIG's General Counsel's Office to ensure the office complied with legal and ethical standards, rules, principles, and guidelines; provide legal advice and counsel to teams conducting audits, evaluations and other reviews; and support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.
- Continued to disseminate information on OIG internal policies related to audit, evaluation, investigation, operations, and administrative processes of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the Office. Also ensured adherence to Executive Orders as they pertain to operations of the OIG.
- Oversaw contracts to qualified firms to provide audit, evaluation, IT, and other services to the OIG to provide support and enhance the quality of our work and the breadth of our expertise as we conduct audits, evaluations, and investigations, and to complement other OIG functions, and closely monitored contractor performance.
- Implemented a new Procurement Request portal to facilitate requests and ensure appropriate controls when procuring needed items and services for the OIG.

Valuing our People and Workplace Culture.

- Planned an All-OIG meeting for the new fiscal year to set the OIG's tone and agenda for the year and to give all component office Executives, Managers, and staff an opportunity to look back to their teams' accomplishments and look forward to new initiatives and priorities going forward.
- Acknowledged OIG staff during Public Service Recognition Week in appreciation for the service they provide to the FDIC and the banking system as members of the FDIC OIG. We were proud to join our colleagues to celebrate the millions of Federal, state, county, and local government employees who serve communities nationwide. Also honored Special Agents on Peace Officers Memorial Day during National Police Week.
- Acknowledged OIG staff for accomplishments and contributions: Federal Maritime Commission IG appreciated the support of one of our Special Agents; another Special Agent was recognized by the USAO in the Central District of California; another Special Agent received a prestigious award at the USAO Annual Awards Ceremony at U.S. District Court in Baltimore, Md; and an investigative financial analyst who was a member of the PRAC Investigative Services Analyst Team was honored by the Association of Certified Fraud Examiners DC Chapter with the 2026 Fraud Fighter of the Year Award.
- Held regular OIG senior leadership coordination meetings to affirm the OIG's unified commitment to the FDIC OIG mission and to strengthen working relationships and collaboration among all FDIC OIG offices.
- Held individual component office meetings in OA, OI, and Office of Management, during which staff had opportunities to exchange information, collaborate on ongoing work projects, develop plans and priorities for the future, and build a sense of camaraderie in pursuit of the OIG's common goals.
- Supported efforts of the OIG's Workforce Council. The mission of this Council is to foster and support a workplace that engages employees, builds trust, and identifies improvements and best practices for the OIG. The Council continued past initiatives, such as its Health and Wellness Challenge, and met several times to further pursue its mission. Also responded to Workforce Council questions raised regarding our financial and human resources as presented in our Congressional Budget Justification for FY 2027.
- Kept OIG staff engaged and informed of office priorities and key activities through regular meetings among staff and management; updates from senior management and IG community meetings; issuance of bi-weekly "End Notes" communications from the IG, and other communications.
- Enrolled OIG staff in several different FDIC, CIGIE, and other Leadership Development Programs to enhance their leadership capabilities.
- Supported OIG staff pursuing professional training and certifications to enhance their expertise and knowledge.
- Came together as an office to participate in an "OIG 250" giving initiative by collecting and delivering school supplies for students in a nearby county.

- Held our annual OIG Distinguished Achievement Awards ceremony for both individuals and teams to acknowledge their outstanding efforts and contributions in preventing, detecting, and deterring fraud, waste, abuse, misconduct, and mismanagement at the FDIC and in the banking sector, and promoting economy, efficiency, effectiveness, and integrity at the FDIC. Awards were given for the following: Collaboration Spirit, Leadership, Innovation, Business Support, New Staff Member, Individual Achievement, Team Achievement, and Excellence. Also recognized staff for other achievements during the past year, along with those celebrating Federal career milestones.

- Nominated FDIC OIG teams for CIGIE Awards for Excellence in Investigations and Evaluations and for the Special Barry R. Snyder Award. Received an Award for Excellence in Investigations *In recognition of exemplary investigative work in a highly elaborate transnational account takeover scheme*, and the Barry R. Snyder Joint Award *In recognition of outstanding contributions to public service and law enforcement as a member of the investigative team for the Washington Federal Bank for Savings investigation*.

- Nominated two Special Agents for CIGIE's Fellows Program and they were both accepted. The CIGIE Professional Development Committee offers this competitive leadership development program to cultivate leaders in the OIG community. The program provides selected individuals with impactful developmental rotations, curated leadership development "cohort activities," and one-on-one executive mentoring.

- Provided leadership and professional development opportunities for OIG staff. Specifically, arranged for OA Managers and the Deputy Assistant Inspector General for Audits to serve as Acting Assistant Inspector General for Audits to fill the temporary vacancy of that position. Also assigned Special Agents to serve as temporary Special Agent in Charge in the Dallas Region and continued to rotate OI's Special Agents in Charge to the position of Deputy Assistant Inspector General for Investigations to temporarily fill that vacancy. Members of Counsel's office also alternated in serving as Acting Counsel to the IG during the reporting period.

- Provided guidance to the staff on the OIG's Performance Management Program, with attention to staff's accurately capturing their significant accomplishments during the performance year in support of the OIG's mission, vision, and values.

- Shared helpful information with staff regarding activities of the FDIC's Office of Human Resources/Employee Life and Career Development. That office offers presentations designed to support employee work-life balance, professional growth, and well-being, and to create a workplace where employees can perform at their maximum potential.

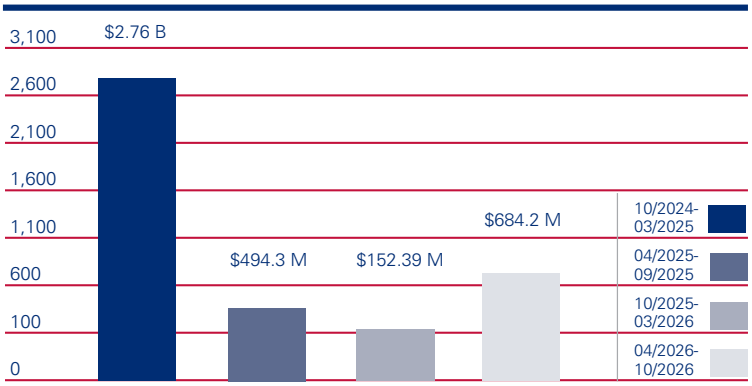
- Convened a meeting with Managers throughout the office to provide updates in some key areas, among those: IT—the OIG's operating environment and initiatives underway; HR: updates related to USA Staffing, GovTA, upcoming Benefits Connect session; Management Services: enhancements to the training request portal and procurement request portal, Employee Supplemental Payment System reminders, and a brief budget update; SI: SI policy update, Generative SI, Data Labeling, and Data Analytics Working Group; and Emergency Communications and Training information: latest training statistics, Occupant Emergency Plan and Floor Marshal refresher items.



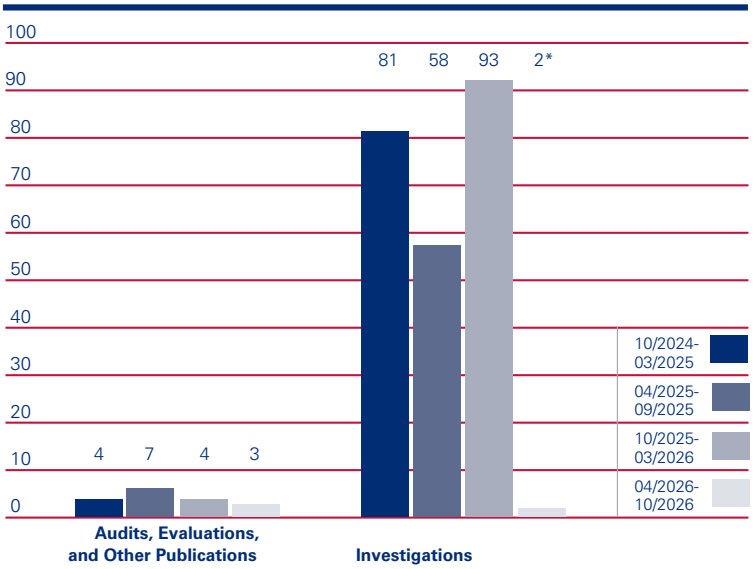
Cumulative Results (2-year period)

Recommendations	
October 2024 – March 2025	21
April 2025 – September 2025	23
October 2025 – March 2026	12
April 2026 – September 2026	4

Fines, Restitution, and Monetary Recoveries Resulting from OIG Investigations ($ in millions and billions)



Products Issued and Investigations Closed



*Note: OI cases were not formally closed during migration of data to the new Case Management Tracking System. This number merely reflects erroneous duplicate entries that were closed out as part of the migration process.



Reporting Requirements

Index of Reporting Requirements

This listing reflects IG reporting requirements based on certain changes in Section 5 of the IG Act, pursuant to Section 5273 of the National Defense Authorization Act for Fiscal Year 2023. (Also listed in Section 405 (b), 5 U.S.C.)

Reporting Requirements	Page
Section 4(a)(2): Review of legislation and regulations.	47
Section 5(a)(1): A description of significant problems, abuses, and deficiencies relating to the administration of programs and operations of the establishment and associated reports and recommendations for corrective action made by the Office.	5-7
Section 5(a)(2): An identification of each recommendation made before the reporting period, for which corrective action has not been completed, including the potential cost savings associated with the recommendation. (Recommendations open for more than one year are noted.)	48-56
Section 5(a)(3): A summary of significant investigations closed during the reporting period.	19-28
Section 5(a)(4): An identification of the total number of convictions during the reporting period resulting from investigations.	3
Section 5(a)(5): Information regarding each audit, inspection, or evaluation report issued during the reporting period, including– (A) a listing of each audit, inspection, or evaluation; (B) if applicable, the total dollar value of questioned costs (including a separate category for the dollar value of unsupported costs) and the dollar value of recommendations that funds be put to better use, including whether a management decision had been made by the end of the reporting period.	57
Section 5(a)(6): Information regarding any management decision made during the reporting period with respect to any audit, inspection, or evaluation issued during a previous reporting period.	58
Section 5(a)(7): The information described under section 804(b) of the Federal Financial Management Improvement Act of 1996.	58
Section 5(a)(8): (A) An appendix containing the results of any peer review conducted by another Office of Inspector General during the reporting period; or (B) if no peer review was conducted within that reporting period, a statement identifying the date of the last peer review conducted by another Office of Inspector General.	61-63

Reporting Requirements (continued)	Page
Section 5(a)(9): A list of any outstanding recommendations from any peer review conducted by another Office of Inspector General that have not been fully implemented, including a statement describing the status of the implementation and why implementation is not complete.	61-63
Section 5(a)(10): A list of any peer reviews conducted by the Inspector General of another Office of Inspector General during the reporting period, including a list of any outstanding recommendations made from any previous peer review (including any peer review conducted before the reporting period) that remain outstanding or have not been fully implemented.	61-63
Section 5(a)(11): Statistical tables showing, for the reporting period: • number of investigative reports issued during the reporting period; • the total number of persons referred to the Department of Justice for criminal prosecution during the reporting period; • the total number of persons referred to State and local prosecuting authorities for criminal prosecution during the reporting period; and • the total number of indictments and criminal informations during the reporting period that resulted from any prior referral to prosecuting authorities.	58
Section 5(a)(12): A description of metrics used for Section 5(a)(11) information.	58
Section 5(a)(13): A report on each investigation conducted by the Office where allegations of misconduct were substantiated involving a senior Government employee or senior official (as defined by the Office) if the establishment does not have senior Government employees.	58
Section 5(a)(14): (A) A detailed description of any instance of whistleblower retaliation, including information about the official found to have engaged in retaliation; and (B) what, if any, consequences the establishment actually imposed to hold the official described in subparagraph (A) accountable.	59
Section 5(a)(15): Information related to interference by the establishment, including— (A) a detailed description of any attempt by the establishment to interfere with the independence of the Office, including— (i) with budget constraints designed to limit the capabilities of the Office; and (ii) incidents where the establishment has resisted or objected to oversight activities of the Office or restricted or significantly delayed access to information, including the justification of the establishment for such action; and (B) a summary of each report made to the head of the establishment under section 6(c)(2) during the reporting period.	59
Section 5(a)(16): Detailed descriptions of the particular circumstances of each - (A) inspection, evaluation, and audit conducted by the Office that is closed and was not disclosed to the public; and (B) investigation conducted by the Office involving a senior Government employee that is closed and was not disclosed to the public.	59



Appendix 1

Information in Response to Reporting Requirements

Review of Legislation and Regulations

Much of the FDIC OIG's activity considering and reviewing legislation and regulation occurs in connection with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Legislation Committee, on which the FDIC OIG is a member. The Legislation Committee provides timely information to the IG community about congressional initiatives; solicits the technical advice of the IG community in response to proposed legislation; and presents views and recommendations to Congress and the Office of Management and Budget on legislative matters that broadly affect the IG community. At the start of each new Congress, the Committee issues Legislative Priorities to improve oversight and effectiveness of OIGs and strengthen the integrity of Federal programs and operations. The FDIC OIG supports the efforts of CIGIE as it works with Congress on these priorities and other government reform issues.

Listed below are legislative proposals that CIGIE considered as high priority at the start of the 119th Congress in January 2025. According to CIGIE, if enacted, the legislative priorities and initiatives supported by the Legislation Committee would strengthen government oversight and accountability, as well as prevent and detect fraud, waste, and abuse in federal programs:

- Permanent Data Analytics Capability for the IG Community
- Prohibiting the Use of Appropriated Funds Government-wide to Deny IGs Full and Prompt Access
- Enhancing Oversight Independence and Efficiency by Providing Separate and Flexible OIG Funding

We note that more recently, the Legislation Committee has focused its attention on tracking anti-fraud-related bills, in which the FDIC OIG has an interest as we work to combat fraud. A recent presentation to the community listed 24 such bills. Of particular interest to the IG community are the following:

- Pre-Payment Fraud Prevention and Treasury Data Access Act
- Zeroing Out Monetary Benefits Improperly Expended Act
- Stop Secret Spending Act (became law on September 11, 2026 and applies to Chief Financial Officer Agencies only)
- Fraud Prevention and Accountability Act

We will continue to keep current with legislation and regulations that affect the IG community and that may impact the FDIC as well.

Table I: Unimplemented Recommendations from Previous Semiannual Periods

Notes:

1. A current listing of each of the unimplemented recommendations is available at https://www.fdicoig.gov/unimplemented-recommendations. The listing is updated monthly.
2. Recommendations open for more than one year are marked **. These total 9 recommendations.
3. Information below is as of September 30, 2026.

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-23-004 **The Federal Deposit Insurance Corporation's Information Security Program – 2023** September 13, 2023	The Federal Information Security Modernization Act of 2014 (FISMA), Public Law No. 113-283, requires Federal agencies, including the FDIC, to conduct annual independent evaluations of their information security programs and practices and to report the results to the Office of Management and Budget (OMB). FISMA requires the independent evaluations to be performed by the Agency IG, or an independent external auditor as determined by the IG. We engaged the professional services firm of Cotton & Company Assurance and Advisory, LLC (Cotton) to conduct this audit. The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. Cotton planned and conducted its work based on OMB's Office of the Federal Chief Information Officer Fiscal Year (FY) 2023 – 2024 Inspector General FISMA Reporting Metrics (Department of Homeland Security FISMA Reporting Metrics). Cotton determined that the FDIC's overall information security program was operating at a Maturity Level 4 (Managed and Measurable) with respect to the FY 2023 FISMA Metrics. In reaching this determination, Cotton's assessment was aligned with the methodology and scope required by the Department of Homeland Security FISMA Reporting Metrics. The report contained two new recommendations to address weaknesses identified during this audit. Recommendation 1 is unimplemented.	2	1**	N/A

Table I: Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-23-004 **The FDIC's Orderly Liquidation Authority** September 28, 2023	Before the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (DFA), the FDIC only had the authority to resolve FDIC-insured depository institutions. Title II of the DFA, Orderly Liquidation Authority (OLA), aimed to provide the necessary authority to the FDIC to liquidate failing financial companies that pose a significant risk to the financial stability of the U.S. in a manner that mitigates such risk and minimizes moral hazard. We conducted an evaluation to determine whether the FDIC maintained a consistent focus on implementing the OLA program and established key elements to execute the OLA under the DFA, including: (1) comprehensive policies and procedures; (2) defined roles and responsibilities; (3) necessary resources; (4) regular monitoring of results; and (5) integration with the Agency's crisis readiness and response planning. We determined that the FDIC had made progress in implementing elements of its OLA program, including progress in OLA resolution planning for the global Systemically Important Financial Companies based in the U.S. However, the report found that in the more than 12 years since the enactment of the DFA, the FDIC had not maintained a consistent focus on maturing the OLA program and had not fully established key elements to execute its OLA responsibilities. The report contained 17 recommendations to improve key elements for executing the FDIC's OLA responsibilities. Recommendation 2 is unimplemented.	17	1**	N/A

Table I: Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
REV-24-01 **Review of FDIC's Ransomware Readiness** March 20, 2024	Ransomware can severely impact business processes and leave organizations without the data needed to operate or deliver mission-critical services. The organizations affected often experience reputational damage, significant remediation costs, and interruptions in their ability to deliver core services. The FDIC relies heavily on information systems to carry out its responsibilities of insuring deposits; examining and supervising financial institutions for safety, soundness, and consumer protection; making large and complex financial institutions resolvable; and managing receiverships. The FDIC needs effective controls for safeguarding its information systems and data to reduce the risk that a ransomware incident could disrupt critical operations and allow inappropriate access to, and disclosure, modification, or destruction of, FDIC information. We conducted a review to assess the adequacy of the FDIC's process to respond to a ransomware incident. We determined that the FDIC had an adequate process to respond to a ransomware incident and generally followed applicable guidance and best practices within the control areas we assessed. However, the FDIC did not fully adhere to Federal standards, FDIC policies, and/or industry best practices related to: (1) protecting backup data and testing the capability to restore systems from backups; (2) maintaining a current, complete, and accurate Continuity Implementation Plan; (3) enabling Wireless Priority Service access for all FDIC Chief Information Officer Organization Executive Management Emergency Command Team Members; and (4) ensuring that key individuals completed Disaster Recovery Awareness Training. We made eight recommendations to address these issues and strengthen the FDIC's process to respond to a ransomware incident. Recommendation 4 is unimplemented.	8	1**	N/A

Table I: Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-24-01 **Audit of Security Controls for the FDIC's Cloud Computing Environment** September 4, 2024	Cloud computing offers many potential benefits, including optimizing costs, flexibility, scalability, and enhanced security. It enables organizations to do more with less by eliminating their on-premises infrastructure with the reduction of servers and staff to support that infrastructure. While cloud computing offers many benefits, it does not eliminate the customer's responsibility to manage security risks appropriately. The FDIC continues to expand its cloud presence by migrating its mission essential and mission critical applications into the cloud. The FDIC must ensure that its systems and data within the cloud are secured and that control weaknesses are effectively addressed. Failure to do so could result in damage and harm to FDIC systems and data, hindering its ability to maintain stability and confidence in the nation's financial system. We engaged Sikich CPA LLC (Sikich) to conduct an audit of security controls for the FDIC's cloud computing environment. The objective of this performance audit was to assess the effectiveness of security controls for the FDIC's cloud computing environment. Sikich found that the FDIC had effective controls in four of nine security control areas assessed. However, Sikich determined that the FDIC had not effectively implemented security controls in its cloud computing environment in five areas, including Identity and Access Management, Protecting Cloud Secrets, Patch Management, Flaw Remediation, and Audit Logging. Sikich made seven formal recommendations and 48 related technical recommendations to improve cloud security controls in 6 common themes of security weaknesses: Insecure Coding Practices, Misconfigured Security Settings, Least Privilege, Outdated Software, Ineffective Monitoring, and Cloud Service Provider Vulnerabilities. Recommendation 7 is unimplemented.	7	1**	N/A

Table I: Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-25-02 **Readiness to Resolve Large Regional Banks** December 10, 2024	Readiness to resolve large regional banks is key to the FDIC's mission of maintaining stability and public confidence in the U.S. financial system. In Spring 2023, the FDIC responded to the unanticipated failures of Silicon Valley Bank (SVB), Signature Bank of New York (Signature), and First Republic Bank (First Republic), three of the largest bank failures in FDIC history. The FDIC resolved each bank through a purchase and assumption agreement, facilitated in part by a systemic risk exception for SVB and Signature. We conducted an evaluation to assess the FDIC's readiness to resolve large regional bank failures under the Federal Deposit Insurance (FDI) Act, prior to the failures of SVB, Signature, and First Republic. The FDIC's readiness to resolve large regional banks under the FDI Act was not sufficiently mature to facilitate consistently efficient response efforts in a potential crisis failure environment. At the time of the Spring 2023 failures, the FDIC had not ensured that it fully met its human and technology resource needs or that it sufficiently coordinated resources among its divisions and offices. The FDIC could have been more effective in demonstrating its readiness to resolve large regional bank failures by: completing, communicating, and coordinating the regional resolution framework guidance; improving large regional bank resolution plans; training key staff on their resolution roles; conducting interdivisional exercises to test resolution procedures; and periodically evaluating and monitoring large bank resolution readiness. The report contained 11 recommendations to enhance the FDIC's ability to conduct resolutions in the most efficient and effective manner, reduce strain on staff, and strengthen interdivisional relationships. Recommendations 1 and 6 are unimplemented.	11	2**	N/A

Table I: Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-25-01 **The FDIC's Procurement of Resolution and Receivership Services** June 10, 2025	Emergency preparedness to procure the services needed to resolve unexpected financial institution failures and systemic financial risks is key to the FDIC's mission of maintaining stability and public confidence in the U.S. financial system. In Spring 2023, the FDIC was appointed receiver for Silicon Valley Bank, Signature Bank, and First Republic Bank, three of the largest bank failures in FDIC history. In response, the FDIC engaged two contractors for advisory services to support the resolution of these failed banks and mitigate a potential systemic financial crisis. We conducted an audit to determine whether the FDIC awarded certain resolution and receivership contracts in accordance with best practices for government contracting and FDIC requirements. While the FDIC established emergency acquisition procedures with a focus on allowing "maximum flexibility," we identified seven best practices that would continue to permit flexibility while also enhancing controls and emergency acquisition preparedness. We also found that FDIC personnel did not adhere to some emergency acquisition procedures while awarding two resolution and receivership contract actions. This report contained 10 recommendations intended to improve the FDIC's emergency contracting procedures and control environment. Recommendations 2 and 10 are unimplemented.	10	2**	N/A

Table I: Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-25-03 **The FDIC's Information Security Program – 2025** September 26, 2025	The Federal Information Security Modernization Act of 2014 (FISMA), Public Law No. 113-283, requires Federal agencies, including the FDIC, to conduct annual independent evaluations of their information security programs and practices and to report the results to the Office of Management and Budget (OMB). FISMA requires the independent evaluations to be performed by the Agency IG, or an independent external auditor as determined by the IG. We contracted with the firm KPMG LLP to perform this work. The objective of this evaluation was to assess the effectiveness of the FDIC's information security program and practices. KPMG determined that the FDIC's overall information security program was operating at a Maturity Level 4 (Managed and Measurable) with respect to the FY 2025 FISMA Metrics. KPMG found the FDIC's information security program was generally effective and that the FDIC established several information security program controls and practices that were consistent with FISMA requirements. However, the report describes security control weaknesses that diminished the effectiveness of certain aspects of the FDIC's information security program and practices. Newly identified security control weaknesses included: • The FDIC did not implement privileged access review frequency requirements for both of the systems we tested. • The FDIC utilized an incomplete and inaccurate listing for user recertification for one of the systems we tested. KPMG made four new recommendations related to weaknesses identified during this year's evaluation. Recommendation 1 is unimplemented.	4	1**	N/A

Table I: Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-26-01 **The FDIC's Student Residence Center** January 6, 2026	In January 2024, the FDIC OIG received a Congressional request to perform work related to the Student Residence Center (SRC). Specifically, the Congressional request stated that, in light of a recent media report at that time, the FDIC OIG should "determine whether [the SRC] still makes financial sense, and that the FDIC is taking meaningful steps to police the behavior of its workforce if they are to continue staying at the [SRC]." The FDIC OIG responded to this request in February 2024 noting that the FDIC OIG planned to review the FDIC's ownership and management of real estate assets, which included the SRC located on the FDIC's Virginia Square campus in Arlington, Virginia. We conducted an audit to assess the FDIC's efforts to determine the cost benefits of, and organizational risks associated with, operating the SRC. We reviewed relevant FDIC policies, procedures, and guidance. In addition, we reviewed Federal laws and regulations, as well as best practices related to real property management. We found the FDIC has not determined the cost benefits of, or organizational risks associated with, operating the SRC. Specifically, the FDIC could not provide documentation that SRC cost benefits have been assessed since 1986 or that organizational risks specifically related to operating the SRC had been formally identified, assessed, or addressed. This was due, in part, to the FDIC's lack of (1) asset management processes and procedures; (2) centralized, accessible SRC-related financial and non-financial data; and (3) performance goals and objectives for SRC operations. The report contained four recommendations intended to improve the FDIC's efforts to determine SRC cost benefits and to identify organizational risks associated with operating the SRC. Recommendations 2 and 4 are unimplemented.	4	2	N/A

Table I: Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-26-02 **Oversight of the Infrastructure Services Contract** January 30, 2026	In January 2021, the FDIC awarded a $300 million Basic Ordering Agreement to provide day-to-day information technology operational support for its infrastructure facilities, hardware, software, and systems. The services provided under the agreement are a critical component of the FDIC's capability to sustain normal operations and respond to bank failures in a timely and effective manner. We conducted an audit to determine whether the FDIC provided effective oversight of the Infrastructure Support Services (ISS) contract to ensure compliance with service level metrics, invoice review and approval procedures, and data protection and security controls. While the FDIC made significant progress to address weaknesses identified during our audit, we determined the FDIC did not provide effective oversight to ensure key contract personnel and the Contractor complied with internal policies and procedures or the ISS contract terms and conditions. Specifically, we found that the FDIC did not always: • Monitor contractor performance against agreed upon metrics nor enforce the requirement for the Contractor to provide the supporting data needed to verify compliance with service level metrics and to determine the accuracy of the service level credits due to the FDIC. • Review and verify the accuracy of invoice charges and service level credits for Critical Service Level defaults nor consistently retain supporting data for invoices. • Verify that all contractors completed training prior to being granted privileged access to the FDIC's network and systems and ensure the Contractor reported a data leakage incident in accordance with internal policy. The report contained eight recommendations intended to improve the FDIC's oversight of ISS contracts. We also identified $2 million in funds to be put to better use and $4.6 million in questioned costs. Recommendations 1, 2, 3, 5, and 6 are unimplemented.	8	5	$6.6 million

Table II: Audit and Evaluation Reports

Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	**Title***	**Total**	**Unsupported**	
REV-26-01 May 29, 2026	*Failed Bank Review, Metropolitan Capital Bank & Trust, Chicago, IL.*			
AUD-26-03 August 31, 2026	*The FDIC's Incident Detection and Response Program*			
EVAL-26-02 September 25, 2026	*The FDIC's Information Security Program - 2026*			
Totals for the Period		**$0**	**$0**	**$0**

*Management decisions were made for all recommendations in the reports listed in this table.

Note: On July 30, 2026, CIGFO issued its memorandum report on its *Audit of the Financial Stability Oversight Council's Designation of Nonbank Financial Companies.* The FDIC OIG was a member of the team behind this project, and the report is discussed earlier in this report in the Audits, Evaluations, and other Reviews section.

Table III: Status of Management Decisions on OIG Recommendations from Past Reporting Periods

There are currently no recommendations from past reporting periods without management decisions and no management decisions from past reporting periods with which the OIG disagreed.

Table IV: Information Under Section 804(b) of the Federal Financial Management Improvement Act of 1996

Nothing to report under this Act.

Table V: Investigative Statistical Information

Number of Investigative Reports Issued	6*
Number of Persons Referred to the Department of Justice for Criminal Prosecution	37
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	0
Number of Indictments and Criminal Informations	46

*Reflects six reports to FDIC management on internal investigations. Customary close-out reports on other investigations were not sent this reporting period, due to investigation system migration.

Note: Description of the metrics used for the above information: Reports issued reflect case closing memorandums issued to FDIC management. Our total indictments and criminal informations includes indictments, informations, and superseding indictments, as applicable.

Table VI: OIG Investigations Involving Senior Government Employees Where Allegations of Misconduct Were Substantiated

During the reporting period, an OIG investigation substantiated an allegation that a Senior Compliance Examiner within the Division of Depositor and Consumer Protection downloaded mobile gambling applications in violation of FDIC Directives and Federal Regulations. The employee acknowledged using gambling applications on their FDIC-issued phone as well as utilizing the phone as their primary personal phone. The employee was issued a Letter of Warning addressing the misuse of FDIC information technology resources, specifically their agency-issued mobile phone.

Table VII: Instances of Whistleblower Retaliation

During this reporting period, there were no instances of Whistleblower retaliation.

Table VIII: Instances of Agency Interference with OIG Independence

(A) During this reporting period, there were no attempts to interfere with OIG independence with respect to budget, resistance to oversight activities, or delayed access to information.

(B) We made no reports to the head of the establishment regarding information requested by the IG that was unreasonably refused or not provided.

Table IX: OIG Evaluations and Audits that Were Closed and Not Disclosed to the Public; Investigations Involving Senior Government Employees that Were Closed and Not Disclosed to the Public

During this reporting period, there were no audits or evaluations involving senior government employees that were closed and not disclosed to the public. With respect to investigations, as noted earlier in this report, due to the migration of the OIG's investigative cases to a new Case Management Tracking System, the OIG did not close investigations—with the exception of two cases that we determined were erroneously included in our prior system. We will resume reporting of any investigations involving senior government employees that we close and do not disclose to the public in our next semiannual report.



Appendix 2

Information on Failure Review Activity

(required by Section 38(k) of the Federal Deposit Insurance Act)

FDIC OIG Review Activity for the Period April 1, 2026 through September 30, 2026 (for failures that occur on or after January 1, 2014 causing losses to the Deposit Insurance Fund of less than $50 million)

When the Deposit Insurance Fund (DIF) incurs a loss under $50 million, the Federal Deposit Insurance Act, 12 U.S.C. § 1831o(k)(5), requires the Inspector General of the appropriate federal banking agency to determine the grounds upon which the state or Federal banking agency appointed the FDIC as receiver and whether any unusual circumstances exist that might warrant an In-Depth Review of the loss.

During the reporting period, we issued a Failed Bank Review of the failure of Metropolitan Capital Bank & Trust, Chicago, Illinois, which failed on January 30, 2026. The FDIC preliminarily estimated that the failure would cost the DIF about $19.7 million. We issued our report on May 29, 2026. Our Failed Bank Review determined that there were no unusual circumstances that would warrant an In-Depth Review of the loss.



Appendix 3

Peer Review Activity

Federal Inspectors General are required to engage in peer review processes related to their audit and investigative operations. The IG community has also implemented a peer review program for the inspection and evaluation functions of an OIG. The FDIC OIG is reporting the following information related to the most current peer reviews that our organization has undergone or conducted.

Definition of Audit Peer Review Ratings

Pass: The system of quality control for the audit organization has been suitably designed and complied with to provide the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

Pass with Deficiencies: The system of quality control for the audit organization has been suitably designed and complied with to provide the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects with the exception of a certain deficiency or deficiencies that are described in the report.

Fail: The review team has identified significant deficiencies and concludes that the system of quality control for the audit organization is not suitably designed to provide the reviewed OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects or the audit organization has not complied with its system of quality control to provide the reviewed OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

Audit Peer Reviews

On a 3-year cycle, peer reviews are conducted of an OIG audit organization's system of quality control in accordance with the CIGIE *Guide for Conducting Peer Reviews of Audit Organizations of Federal Offices of Inspector General*, based on requirements in the Government Auditing Standards (Yellow Book). Federal audit organizations can receive a rating of pass, pass with deficiencies, or fail.

The OIG for the Board of Governors of the Federal Reserve System (FRB) and the Consumer Financial Protection Bureau (CFPB) conducted a peer review of the FDIC OIG's audit function and issued its report on the peer review on September 9, 2025. The FDIC OIG received a rating of Pass. In the FRB/CFPB OIG's opinion, the system of quality control for the audit organization of FDIC OIG in effect for the year ended March 31, 2025, had been suitably designed and followed to provide the FDIC OIG with reasonable assurance of performing and reporting in a manner consistent with applicable professional standards and applicable legal and regulatory requirements in all material respects.

The FRB/CFPB OIG communicated additional findings that required attention by FDIC OIG management but were not considered to be of sufficient significance to affect the FRB/CFPB OIG's opinion expressed in its peer review report.

This peer review report is posted on our Website.

FDIC OIG Peer Review of Another OIG

Our FDIC OIG Review Team reported on March 5, 2025, that in its opinion, the system of quality control for the audit organization of Amtrak OIG in effect for the year ended September 30, 2024, had been suitably designed and complied with to provide Amtrak OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards and applicable legal and regulatory requirements in all material respects.

Audit organizations can receive a rating of pass, pass with deficiencies, or fail. Amtrak OIG has received an External Peer Review rating of pass. In conducting this review, we identified no outstanding recommendations from prior peer review reports of Amtrak.

Inspection and Evaluation Peer Reviews

The Department of Education OIG reviewed the system of quality control for the FDIC OIG in effect for the year ended September 30, 2025. A system of quality control includes multiple aspects of an organization, including, but not limited to, policies and procedures designed to provide reasonable assurance of complying with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Quality Standards for Inspection and Evaluation, December 2020 (Blue Book).

The Department of Education OIG selected four FDIC OIG reports for review. Two were performed by the FDIC OIG, and two were performed in whole by contractors with FDIC oversight.

As conveyed on March 26, 2026, in the Department of Education OIG's opinion, the system of quality control for the FDIC OIG in effect for the year ended September 30, 2025, had been suitably designed and complied with to provide the FDIC OIG with reasonable assurance of performing and reporting in conformity with the Blue Book. Inspection and Evaluation (I&E) organizations can receive a rating of pass, pass with deficiencies, or fail. The FDIC OIG received an External Peer Review rating of Pass. The Department of Education OIG also issued a letter of comment that set forth findings that were not considered to be of sufficient significance to affect its opinion on the peer review. There were no recommendations made. This peer review report is also posted on our website.

Investigative Peer Reviews

Quality assessment reviews of investigative operations are conducted on a 3-year cycle. The Department of Veterans Affairs (VA) OIG reviewed the system of internal safeguards and management procedures for the investigative operations of the FDIC OIG in effect for the period ending October 2023. The review was conducted in conformity with the Quality Standards for Investigations and the Qualitative Assessment Review Guidelines established by the Council of the Inspectors General on Integrity and Efficiency.

The VA OIG reviewed compliance with the FDIC OIG system of internal policies and procedures to the extent considered appropriate. The review was conducted at the FDIC OIG headquarters office and field offices in Arlington, VA, Kansas City, MO, and New York, NY. Additionally, the VA OIG sampled case files for investigations closed between October 1, 2022, and September 30, 2023.

In performing its review, the VA OIG considered the prerequisites of the Attorney General's Guidelines for Office of Inspectors General with Statutory Law Enforcement Authority and Section 6(e) of the Inspector General Act of 1978, as amended. Those documents authorize law enforcement powers for eligible personnel of each of the various Offices of Inspectors General. Law enforcement powers may be exercised only for activities authorized by the IG Act, other statutes, or as expressly authorized by the Attorney General.

On November 21, 2023, the VA OIG reported that in its opinion, the system of internal safeguards and management procedures for the investigative function of the FDIC OIG in effect for the year ending 2023, complied with the quality standards established by CIGIE and the other applicable guidelines and statutes cited above. These safeguards and procedures provided reasonable assurance of conforming with professional standards in the planning, execution, and reporting of FDIC OIG investigations. There were no recommendations made.

FDIC OIG Qualitative Assessment Review of Another OIG

In a prior reporting period, we issued the results of our review of the system of internal safeguards and management procedures for the investigative operations of the Office of Inspector General (OIG) for the U.S. General Services Administration (GSA) for the 12 months ending September 2024. Our review was conducted in conformity with the *Quality Standards for Investigations and the Qualitative Assessment Review Guidelines for Investigative Operations of Federal Offices of Inspector General* established by the CIGIE, as applicable.

We reviewed GSA OIG's compliance with its system of internal policies and procedures to the extent we considered appropriate. The review was conducted at GSA offices in Kansas City, Missouri; Washington, District of Columbia; and Philadelphia, Pennsylvania. Additionally, we sampled 30 case files for investigations closed from October 2023 through September 2024.

In performing our review, we also considered the Attorney General's Guidelines for OIGs with Statutory Law Enforcement Authority and Section 6(e) of the Inspector General Act of 1978, as amended (IG Act). The aforementioned documents authorize law enforcement powers for eligible personnel of the various OIGs. Law enforcement powers may be exercised only for activities authorized by the IG Act, other statutes, or as expressly authorized by the Attorney General.

Our review found that the system of internal safeguards and management procedures for the investigative operations of the GSA OIG for the period ending September 2024 complied with the quality standards established by CIGIE and other applicable guidelines and statutes cited above. These safeguards and procedures provided reasonable assurance of conforming to professional standards in the planning, execution, and reporting of GSA OIG investigations and in the use of law enforcement powers. We made no recommendations as a result of this review.



OIG 250th

This year we proudly celebrated the fact that we are working as an OIG in a tradition going back almost 250 years….

The IG concept was derived in part from the military custom of having an IG provide an independent review of the combat readiness of the Continental Army's troops. Baron von Steuben was a Prussian-born army officer who played a leading role in the American Revolutionary War by reforming the Continental Army into a disciplined and professional fighting force. He served as Inspector General of the Continental Army for approximately 6 years, from his appointment to the role by George Washington at Valley Forge in May 1778 until his resignation from the military in March 1784.

Fast forward to the late 1960s and 1970s, when it became apparent to the Congress that the Federal government needed to broaden its notion of what Inspectors General could do and how their expertise could help to focus on the activities of civilian agencies. Scandals involving procurement activities within some Federal agencies prompted this move and resulted in the passage of the Inspector General Act of 1978. In signing the Act into law on October 12, 1978, President Jimmy Carter created independent audit and investigative offices in 12 Federal agencies.

The basic tenets of the IG Act have remained constant and strong over the past nearly half century. Although amended several times, for example, to add new IGs, increase authorities, clarify reporting requirements, and create a governing Council, the Act has given IGs the authority and responsibility to be independent voices for economy, efficiency, and effectiveness within the Federal government. Today the FDIC OIG joins 69 other OIGs to protect the integrity of government, improve program efficiency and effectiveness, and prevent and detect fraud, waste, and abuse in Federal agencies.

The FDIC OIG is proud to be part of the historical evolution of the IG concept, and we look forward to continuing to serve the best interests of our Nation in the years ahead.



Congratulations!

We are pleased to announce that the following FDIC OIG accomplishments are being recognized with Council of the Inspectors General on Integrity and Efficiency Awards this year.

Barry R. Snyder Joint Award

Investigative Team - Bank Failure, Washington Federal Bank for Savings

- From the FDIC OIG: Jason Gibson, Special Agent; Jacob Evans, Special Agent; Pete Caggiano, Special Agent; Sean Stephenson, Special Agent (retired); Joseph Moriarty, Special Agent in Charge (retired); and other law enforcement partners.

In recognition of outstanding contributions to public service and law enforcement as a member of the investigative team for the Washington Federal Bank for Savings investigation.

The Washington Federal Bank for Savings (WFBS), located in Chicago, IL, failed in 2017. Beginning in October 2004, and continuing through December of 2017, WFBS employees conspired with attorney Robert Kowalski, and other high-ranking WFBS officials, to embezzle at least $31 million in bank funds in the years preceding WFBS's closure. WFBS officials transferred money to borrowers (co-conspirators), often without any documentation, and falsified bank records to conceal the embezzlement and financial condition of the bank from the OCC and FDIC. The FDIC ultimately became the receiver of the bank and provided approximately $90 million from the Deposit Insurance Fund to make depositors whole.

The Barry Snyder Award recognizes cooperative efforts in matters of importance to the OIG community, the government, and the public. The Washington Federal Bank for Savings case clearly illustrates people coming together with a common purpose and the power of collaboration when combatting harmful fraudulent activities. Four Federal OIGs, several city OIGs and local authorities, DOJ, the FBI, and the IRS joined forces to bring fraudsters to justice. Their outstanding investigative skills led to stiff sentences and substantial restitution ordered for the offenders. Importantly, their actions also served to restore faith and public confidence in the financial system. Together, they sent the message that law enforcement will be relentless in seeking punishment for those who would try to undermine the financial services industry, harm the nation's banks, and victimize consumers who trust that high-ranking bank officials and insiders will obey the laws and protect their savings.

Award for Excellence: Account Takeover Scheme

Dennis McCarty, Special Agent (SA), FDIC OIG Office of Investigations, and law enforcement partners from the U.S. Secret Service (USSS).

In recognition of exemplary investigative work in a highly elaborate transnational account takeover scheme.

Over 5-year period, multiple subjects used a combination of cyber-technology and social engineering tactics to trick hundreds of unsuspecting victims into providing their personally identifiable information and bank account information. The subjects posed as customer service representatives from the banks and used a Virtual Private Network (VPN), or Proxy Server, to obfuscate their IP address and take over the victims' accounts. The subjects then wired victim funds to individuals known as "money mules," who facilitated getting the illegal proceeds back to the main perpetrators of the fraud.

This international account takeover fraud scheme impacted at least six FDIC-regulated and insured financial institutions and caused over $29 million in losses to victims across the U.S.

SA McCarty and his USSS colleagues were determined in their efforts to unravel this highly complex and far-reaching international extortion and wire fraud scheme; seize and analyze large volumes of electronic evidence; trace funds across continents; coordinate with international law enforcement entities; arrest and prosecute one of the main conspirators; locate, arrest, and extradite two other co-conspirators to the U.S., and ultimately hold the offenders fully accountable. The fraudsters received stiff prison sentences and were ordered to pay millions of dollars in restitution.

SA McCarty combined his sharp investigative expertise and Spanish language skills to coordinate successfully with foreign partners. He and other USSS agents sacrificed personal time by traveling extensively and even during holidays to investigate this case. The case was subsequently highlighted in a press release issued by the U.S. Attorney's Office illustrating how law enforcement was taking action against money mules to disrupt transnational fraud schemes, while also educating the public.

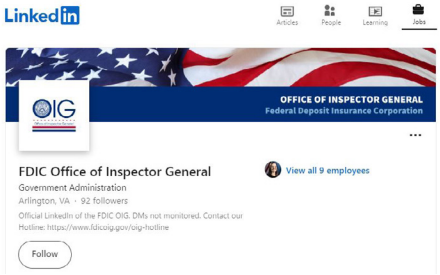
★**Learn more about the FDIC OIG.**
Visit our website: www.fdicoig.gov.



★**Follow us on X, formerly known as Twitter: @FDIC_OIG.**



★**Follow us on LinkedIn: www.linkedin.com/company/fdicoig**



★**View the work of Federal OIGs on the IG Community's Website.**

OVERSIGHT.GOV
ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE

★**Keep current with efforts to oversee COVID-19 emergency relief spending.**

PANDEMIC RESPONSE ACCOUNTABILITY COMMITTEE

www.pandemicoversight.gov

DESIGN: FDIC/OCOM/GRAPHIC DESIGN AND PRINTING UNIT

Federal Deposit Insurance Corporation
Office of Inspector General
3501 Fairfax Drive
Arlington, VA 22226



To learn more about the FDIC OIG and for more information on matters discussed in this Semiannual Report, visit our website: **http://www.fdicoig.gov**.

FDIC-008-2026