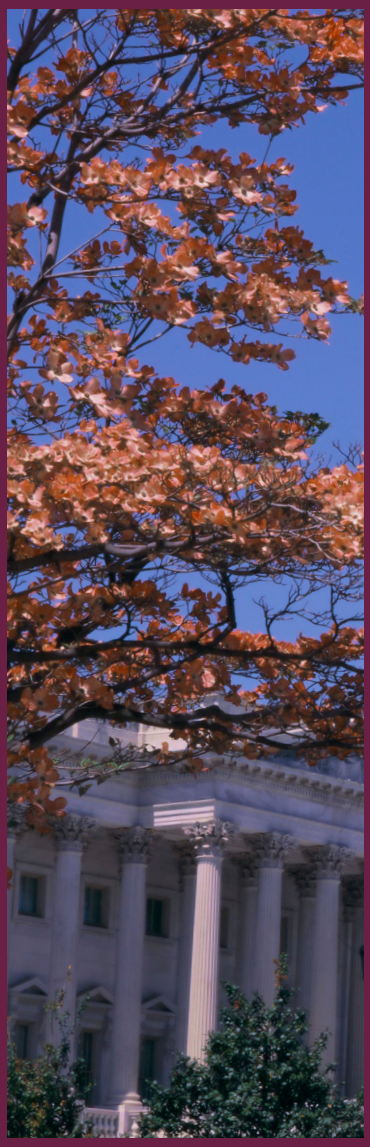
FDIC Office of Inspector General

Semiannual Report to the Congress

April 1, 2025 - September 30, 2025

Office of Inspector General

Integrity • Objectivity • Independence • Excellence • Transparency

Under the Inspector General Act of 1978, as amended, the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General 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 6,404 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data (September 30, 2025), the FDIC insured $10.66 trillion in domestic deposits in 4,379 institutions, of which the FDIC supervised 2,772. The Deposit Insurance Fund balance totaled $150.1 billion. Active receiverships totaled 44, with assets in liquidation of about $24.99 billion.

Semiannual Report to the Congress

April 1, 2025 – September 30, 2025

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*

Please note that this semiannual report is being issued later than usual, given the government shutdown period.

Inspector General's Statement

I am pleased to submit this report highlighting the work of the FDIC OIG for the period April 1, 2025 through September 30, 2025.

Over the past 6 months, the dedication and perseverance of all members of the OIG led to several significant results. We issued 7 reports with 23 recommendations on important, sensitive topics, including IT and cybersecurity, supervision, resolution and receivership, and Part 2 of our *Special Inquiry on the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct*, and in all instances, we reported results in an objective manner. In the case of the Special Inquiry, we reported that certain senior officials personally engaged in some degree of inappropriate workplace conduct. Further, certain actions of the senior officials did not protect victims of harassment, nor consistently align with the FDIC's applicable policies and core values.

In addition, our office continued to investigate fraud related to FDIC-regulated and insured banks, achieving several outcomes that strengthened integrity at the FDIC and within the financial sector. During the reporting period, our cases resulted in 60 indictments/informations, 59 convictions, 47 arrests, and more than $494 million in fines, restitution ordered, and other monetary recoveries. Of note during the period, a start-up Chief Executive Officer (CEO) was sentenced to 85 months in prison for a $175 million fraud relating to her student financial aid application assistance company, Frank. She and Frank's chief growth and acquisition officer were accused of fraudulently inflating customer numbers while negotiating the sale of her company to JPMorgan Chase for $175 million. The CEO was convicted after a 6-week trial, ordered to pay a forfeiture judgment of more than $22 million, and restitution of $287.5 million, joint and several with her co-defendant, the chief growth and acquisition officer. Another highlight of the period was the guilty plea of a Federal employee and government contractor 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 terms and conditions of the contracts.

Our Office of Audits also received a "Pass" on the peer review conducted by the Board of Governors of the Federal Reserve System/Consumer Financial Protection Bureau OIG, indicating that the OIG's system of quality control provided reasonable assurance of conforming in all material respects with Government Auditing Standards. As further evidence of quality work, we were also notified that members of our office were chosen to receive the IG community's Awards for Excellence in Evaluations and Investigations, along with a special award for efforts leading a Monetary Benefits Working Group.

We experienced significant Congressional interest in our work and our office itself during the period. In response, we briefed several Committee staff and provided written responses to Congressional questions and concerns, with full transparency.

To remain true to our role at the FDIC and provide the best possible value to the FDIC, we recently reconsidered and re-formulated our Strategic Plan for going forward—starting with our mission, vision, and values. As restated, our mission is: *To deliver credible results that drive meaningful change, enhance integrity and accountability, and maintain public trust in the FDIC.* Our vision is: *To be a leader within the IG community through proactive, agile, and innovative oversight of FDIC programs and operations.* And we espouse five core values: *Integrity, Objectivity, Independence, Excellence, and Transparency*.

Our strategic direction remains focused on our statutorily mandated responsibilities. We are refining our strategic goals and will share them once they are finalized.

The achievements in this report reflect the dedication and expertise of FDIC OIG staff. I sincerely appreciate their ongoing commitment and hard work, which are essential to fulfilling our responsibilities.

As we move into 2026, we build on our foundation and remain committed to our values and independent oversight responsibilities at the FDIC. We will pursue our mission in cooperation with FDIC senior leadership and management, along with the invaluable support of partners, stakeholders, and the Congress, and in service to the American people.

/S/

Jennifer L. Fain
Inspector General
December 2025

Table of Contents

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

Acronyms and Abbreviations

ACH	Automated Clearing House
AI	Artificial Intelligence
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CEO	Chief Executive Officer
CFPB	Consumer Financial Protection Bureau
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
DHS CISA	Department of Homeland Security's Cybersecurity and Infrastructure Security Agency
DIF	Deposit Insurance Fund
DOJ	Department of Justice
ECU	Electronic Crimes Unit
FAEC	Federal Audit Executive Council
FBA	Federal Banking Agency
FBI	Federal Bureau of Investigation
FCBC	First Community Bank of Cullman
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act
FRB:	Board of Governors of the Federal Reserve System
FTC	Federal Trade Commission
HSI	Homeland Security Investigations
IDFPR	Illinois Department of Financial and Professional Regulation
IG	Inspector General
IRMA	Inherent Risk Methodology Analysis
IT	Information Technology
JPMC	JP Morgan Chase
MMI	Murex Management, Inc.
OCC	Office of the Comptroller of the Currency
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
ORMIC	Office of Risk Management and Internal Control
PRAC	Pandemic Response Accountability Committee
RMS	Division of Risk Management Supervision
RSP	Regional Service Provider
SSP	Significant Service Provider
USAO	United States Attorney's Office
WFBS	Washington Federal Bank for Savings

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 continues to conduct its work in line with a set of a set of Guiding Principles that we have adopted, and the results of our work during the reporting period are presented in this report within the framework of those principles. Our Guiding Principles focus on Impactful Audits and Evaluations; Significant Investigations; Partnerships with External Stakeholders (the FDIC, Congress, whistleblowers, and our fellow OIGs); efforts to Maximize Use of Resources; Leadership skills and abilities; and importantly, Teamwork.

The following table presents overall statistical results from the reporting period.

Overall Results (April 1, 2025 – September 30, 2025)	
Audit, Evaluation, and Other Products Issued	**7**
Recommendations	**23**
Investigations Opened	**60**
Investigations Closed	**58**
Judicial Actions:	
Indictments/Informations	**60**
Convictions	**59**
Arrests	**47**
OIG Investigations Resulted in:	
Special Assessments	**$12,925.00**
Fines	**$6,073,049.24**
Restitution	**$448,479,171.78**
Asset Forfeitures	**$39,774,481.60**
Criminal Penalty	**N/A**
Civil Penalty	**N/A**
Total	**$494,339,627.62**
Referrals to the Department of Justice (U.S. Attorney and DOJ Antitrust)	**63**
Investigative Reports Referred to FDIC Management	**9**
Responses to Requests Under the Freedom of Information/Privacy Act	**30**
Subpoenas Issued	**6**

Audits, Evaluations, and Other Reviews

In keeping with our first Guiding Principle, the **FDIC OIG conducts superior, high-quality audits, evaluations, and reviews**. We do so by:

- Performing audits, evaluations, and reviews in accordance with the highest professional standards and best practices.
- Issuing relevant, timely, and topical audits, evaluations, and reviews.
- Producing reports based on reliable evidence, sound analysis, logical reasoning, and critical thinking.
- Writing reports that are clear, compelling, thorough, precise, persuasive, concise, readable, and accessible to all readers.
- Making meaningful recommendations focused on outcome-oriented impact and cost savings.
- Following up on recommendations to ensure proper implementation.

During the reporting period, we issued seven reports addressing control improvements needed in workplace culture, supervision, IT and cloud security, and resolutions and receiverships. We made a total of 23 recommendations to FDIC management in these reports.

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. As of the end of the reporting period, we had issued one failed bank review, that of Pulaski Savings Bank. This bank failed on January 17, 2025, with losses to the DIF estimated at $28.4 million at that time. We currently have an In-Depth Review in progress related to that failure.

Results of the audits, evaluations, and other reviews completed during the reporting period are summarized below. We also include a summary of the issues we highlighted in our Top Management and Performance Challenges report that we issued in March 2025. A listing of ongoing assignments, in large part driven by our assessment of the Top Management and Performance Challenges Facing the FDIC, is also presented. Additionally, we provide an update on a matter that we have been addressing with the FDIC's Chief Information Officer Organization (CIOO) related to the security of OIG emails. We also present information on recommendations unimplemented for more than one year.

Audits, Evaluations, and Other Reviews

Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct – Part 2.
We issued Part 2 of our Special Inquiry on the *FDIC's Workplace Culture with Respect to Harassment and Related Misconduct*. This report is a follow-on to Part 1 of our report, issued in December 2024. Our objective in Part 2 was to provide factual findings regarding selected allegations that senior officials personally engaged in harassment or related misconduct.

An Agency's overall performance and reputation can be undermined by employee perceptions that an Agency's workplace culture does not demonstrate commitment to its core values. In addition, if management does not hold personnel accountable and foster an environment where employees can report harassment and related misconduct without fear of retaliation, employees will mistrust the Agency's efforts.

The preliminary evidence we gathered led us to conduct investigations into allegations of harassment and related misconduct against five FDIC senior officials. While the scope and severity of conduct varied, our investigations developed evidence supporting that each of the senior officials personally engaged in some degree of inappropriate workplace conduct. Our report discusses the factual evidence related to each official.

We also reviewed how the FDIC handled allegations against the senior officials and each official's role in reviewing incoming allegations against each other. In our previous report, we found that many FDIC employees perceived that FDIC management had tolerated harassment and related misconduct and that management had not been effective in supporting victims of workplace harassment and encouraging the reporting of harassment they experienced.

Our investigations developed evidence supporting that certain actions of these senior officials did not protect victims of harassment, nor consistently align with the FDIC's applicable policies and stated core values (including accountability, fairness, and integrity).

The evidence developed in our investigations also corroborated the validity of employee perceptions of FDIC culture that were described in Part 1 of this project. In Part 1, the OIG reported that many of the employees we interviewed perceived that the FDIC would not effectively implement its action plan to address harassment because some of the executives leading the efforts have had allegations against them.

Our investigations also developed evidence that three of the senior officials assisted one another in discreetly and expeditiously resolving complaints when allegations of misconduct arose against them.

In Part 1 of this report and in our 2024 report on the FDIC's Sexual Harassment Prevention Program, we made recommendations to improve reporting, investigative, and disciplinary processes for harassment issues. The FDIC is continuing to implement these recommendations. Upon completion of this administrative investigation, we provided our factual findings to the FDIC for their review and action.

FDIC Management in turn responded on July 25, 2025, indicating that there is no higher priority than ensuring every person at the Agency feels safe, valued, and respected. The response lists corrective actions taken to implement an effective anti-harassment program structure. It also includes actions taken with respect to the senior leaders who were the subjects of our review, none of whom remain employed by the FDIC. The FDIC stated that in response to the OIG's investigations of the five senior officials discussed in this report, the FDIC reviewed the reports of investigation, conducted its own investigations in several cases, and took corrective action, as appropriate.

The response further noted that the FDIC is under new leadership, including a new Acting Chairman, new Board Members, and new executive leadership atop the majority of FDIC Divisions and Offices, which report directly to the Acting Chairman. As well, reoccurring training is on the horizon, along with an improved complaint tracking system and a climate assessment and surveys to monitor Agency progress in these areas.

Procurement of Resolution and Receivership Services

We issued our report on *The FDIC's Procurement of Resolution and Receivership Services*. 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.

Our objective was to determine whether the FDIC awarded certain resolution and receivership contracts in accordance with best practices for government contracting and FDIC requirements.

We reported that 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. Enhancing the FDIC's preparedness could improve the FDIC's ability to ensure an adequate supply of contractors, obtain fair and reasonable pricing, oversee contractor performance, protect and ensure the FDIC's contractual rights, and retain key sources of data and analysis.

We also found that FDIC personnel did not adhere to some emergency acquisition procedures while awarding two resolution and receivership contract actions. FDIC management did not ensure that all aspects of the FDIC's emergency acquisition process were followed because they perceived the need to employ "maximum flexibility" due to the historic nature of the potential crisis and the need to facilitate procurement actions that met the FDIC's immediate need. The FDIC's lack of compliance with some of its acquisition policies and procedures hindered its ability to ensure proper contract oversight management.

We made 10 recommendations intended to improve the FDIC's emergency contracting procedures and control environment. The FDIC concurred with all of these recommendations and plans to complete the corrective actions by June 30, 2026.

FDIC's Succession Management and Employee Retention Efforts

Also during the reporting period, we issued a memorandum, *FDIC Succession Management and Employee Retention Efforts*.

According to the FDIC, its workforce is the most critical factor in achieving its mission of maintaining stability and public confidence in the nation's financial system. In addition, the Government Accountability Office has recognized strategic human capital management, including aspects of succession management and employee retention management, as a high-risk area across the Federal Government since 2001.

Over the last several years, the FDIC has taken steps to develop and implement a coordinated, organization-wide approach to succession management and employee retention management. We spoke with FDIC officials and reviewed documentation related to challenges the FDIC was facing in implementing a succession management and employee retention program.

Our memorandum cites four areas:

- **Governance:** The FDIC has not provided executive sponsorship, developed appropriate governance, obtained sufficient resources, or developed roles and responsibilities to enable a centrally managed program for succession and retention to exist and succeed.
- **Data Governance and Management:** The FDIC does not have centralized, clearly defined data for managing succession and retention and may not be using its data efficiently for succession management purposes or to inform and assess the effectiveness of retention strategies.
- **Coordinated Contracting Efforts:** The FDIC does not have a coordinated approach among Divisions and Offices for requesting and obtaining contracts related to workforce management.
- **Information Technology Infrastructure:** The FDIC does not have the information technology infrastructure to support an organization-wide effort in succession and retention management.

The Administration's Executive Orders and directives over the past months aim to reshape and restructure Federal agencies and the Federal workforce. As a result, the FDIC workforce is evolving, and as the FDIC implements organizational changes, it must ensure that it can effectively and efficiently accomplish its mission with a smaller workforce. It is important for the FDIC to maintain a sustained focus on workforce planning.

In our earlier report, *FDIC Readiness to Resolve Large Regional Banks* (December 2024), we found that the FDIC had not ensured that it fully met human and technology resource needs or that it sufficiently coordinated those resources among its Divisions and Offices. We recommended that FDIC leadership, including the Chief Operating Officer 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. The FDIC agreed to implementing an agency-wide committee to monitor, report, and support its resource efforts. According to the FDIC, in response to the Executive Orders, it is developing plans to strengthen resource planning and response capabilities in line with the FDIC's statutory authorities.

We believe that the FDIC has an opportunity to leverage our previous recommendation and fully integrate its anticipated agency-wide resource committee into its workforce optimization efforts. Such integration would align the prioritization of existing resources across the FDIC, facilitate succession management discussions and activities, and enhance workforce optimization strategies throughout the FDIC.

The OIG will reexamine the FDIC's efforts in these areas once the FDIC has had the opportunity to more fully implement its Workforce Optimization Initiative.

Failed Bank Review – Pulaski Savings Bank, Chicago, IL

On January 17, 2025, the Illinois Department of Financial and Professional Regulation (IDFPR), Division of Banking, took possession and control of Pulaski Savings Bank and appointed the FDIC as the receiver. According to the FDIC, the estimated loss to the DIF at that time was $28,449,000 or 62 percent of the bank's $45,919,248 in total assets. Following a period of supervisory actions by regulators, the IDFPR took possession of Pulaski Savings Bank because FDIC and IDFPR examiners verified significant unresolved and unexplained discrepancies within suspense accounts as well as large deposits maintained off the bank's core system.

As noted above, when the DIF incurs a loss under $50 million, the FDI Act 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.

Based on our review of key FDIC documents, including examination reports and prompt corrective action letters to the bank, Pulaski Savings Bank's failure occurred due to impaired capital. We determined that an In-Depth Review of the loss was warranted given the high estimated loss rate (62 percent) and unaccounted for deposit liabilities. Specifically, the bank had deposit liabilities of at least $20.7 million not accounted for in its core system. The recording of these deposits depleted the bank's capital.

Our review identified unusual circumstances that warrant an In-Depth Review of the loss, and as of the end of the reporting period, that review was ongoing.

Significant Service Provider Examination Program

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

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

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

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

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

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

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

We observed that the vendor selection process in place when we began our review was highly subjective, poorly documented, and would benefit from additional quantitative analysis. In that regard, the FBAs set out to establish a new FBA Inherent Risk Methodology Analysis (IRMA) that was a risk-based methodology for measuring and risk-ranking service providers. IRMA is designed to (1) prioritize service providers who are currently supervised to determine the appropriate examination frequency and commensurate resourcing, (2) evaluate whether new service providers should be supervised and added to the program, and (3) evaluate whether existing service providers should no longer be supervised and removed from the program.

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

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

In its response, the FDIC concurred with our recommendation and plans to complete corrective actions by March 31, 2026.

Audit of Security Controls for a Cloud Platform and Application

The FDIC has increasingly adopted cloud services to support its business functions. As of July 2025, the FDIC had migrated several of its mission essential and mission critical applications into a cloud environment. There are many benefits for organizations like the FDIC to migrate to the cloud; notably, the cloud service provider has some responsibility for security, lessening the administrative overhead for the FDIC. However, as a cloud customer, the FDIC is still accountable for ensuring that its systems and data that operate in the cloud are secured in accordance with its own security standards.

In September 2024, the FDIC OIG issued a report on the *Audit of Security Controls for the FDIC's Cloud Computing Environment*. In that audit, we assessed security controls on four cloud platforms and one Application Program Interface platform. For that audit, our scope originally included a fifth cloud platform – which we refer to as "Platform." We decided not to perform Platform and Application testing because the Application was undergoing a major upgrade at that time, including the addition of external users (e.g., state regulators and bank users).

We engaged Sikich CPA LLC (Sikich) to conduct a performance audit of security controls for this fifth cloud platform and application. The objective of this audit was to assess the effectiveness of their security controls. To address this objective, Sikich performed tests of nine IT security control areas for the cloud platform and application. Sikich also assessed policies and procedures, conducted interviews of responsible officials, and conducted penetration testing procedures. Sikich determined that the FDIC had not effectively implemented security controls in the cloud platform and application in two areas: Identity and Access Management and Protecting Cloud Secrets. The report includes seven technical findings for the cloud platform and application attributed to two overarching themes:

1. **Insecure Coding Practices:** The FDIC teams developing cloud platforms did notconsistently implement secure coding practices or functions.
2. **Cloud Service Provider Vulnerabilities:** The Cloud Service Provider was solely responsible for causing certain vulnerabilities and should be responsible for their remediation.

Sikich made eight recommendations related to the identified control deficiencies and security weaknesses that, if effectively addressed, should strengthen the security controls for the cloud platform and application. The FDIC concurred with all recommendations and plans to complete all corrective actions by March 31, 2026.

The FDIC's Information Security Program–2025

The FDIC OIG issued its 2025 report on the FDIC's Information Security Program in accordance with statutory Federal Information Security Modernization Act (FISMA) requirements. The objective of this evaluation was to assess the effectiveness of the FDIC's information security program and practices. We contracted with the firm KPMG LLP to perform this work.

In response to the threat environment and technology ecosystem, which continue to evolve and change at a faster pace each year, the Office of Management and Budget implemented a new framework regarding the timing and focus of FISMA assessments in Fiscal Year (FY) 2022. This effort yielded two distinct groups of metrics: Core and Supplemental. The goal of this new framework was to maintain a consistent focus on annual assessments while allowing for greater flexibility for the Federal community. The "Core" metrics are associated with high value controls, whereas the "Supplemental" metrics provide additional insights to support and enhance the understanding of the overall effectiveness of a security program.

Based on the ratings of the core and supplemental metrics, KPMG determined that the FDIC information security program was rated a Level 4 maturity, Effective. A Level 4 maturity is typically categorized as having quantitative and qualitative measures of the effectiveness of policies, procedures, and strategies that have been defined and consistently implemented across the organization that are used to assess and make necessary changes.

Specifically, KPMG found that the FDIC established several information security program controls and practices that were consistent with FISMA requirements, Office of Management and Budget policy and guidelines, and applicable National Institute of Standards and Technology standards and guidelines. However, KPMG noted the following with respect to the evaluated domains for FY 2025:

- **Cybersecurity Governance** was identified as a Level 3 maturity due to a lack of policy and procedures to maintain current and target cybersecurity profiles.
- **Identity and Access Management** was identified as a Level 3 maturity with two, prior-year open recommendations and four new open recommendations.
- **Security Training** was also rated as a Level 3 maturity. Although the FDIC has performed a workforce assessment to identify gaps in skills and resources, the gaps identified as a result of this assessment had not yet been addressed during our evaluation scope period.

All other domains evaluated had no open recommendations reported during the FY 2025 FISMA evaluation and obtained an effective, Level 4 or higher maturity rating.

In sum, KPMG found the FDIC's information security program was generally effective. 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 following:

- The FDIC did not implement privileged access review frequency requirements for both of the systems that KPMG tested.
- The FDIC utilized an incomplete and inaccurate listing for user recertification for one of the systems that KPMG tested.

KPMG made four new recommendations related to weaknesses identified during this year's evaluation. In addition, there were two outstanding recommendations from prior FISMA reports still warranting the FDIC's continued attention. The FDIC concurred with the four recommendations and plans to complete corrective actions by May 29, 2026.

OA Peer Review

The IG responded to the results of the Audit Peer Review conducted by the Board of Governors of the Federal Reserve System/Consumer Financial Protection Bureau (FRB/CFPB) OIG. The independent review resulted in a Pass rating and concluded that the OIG's system of quality control in effect for the year ended March 31, 2025 provided reasonable assurance of conforming in all material respects with Government Auditing Standards. With regard to the Letter of Comment, the IG expressed appreciation for the observations that FRB/CFPB OIG made and agreed with two recommendations in the letter. (See also Appendix 3.)

Top Management and Performance Challenges

Our Top Management and Performance Challenges document summarizes the most serious challenges facing the FDIC and briefly assesses the Agency's progress to address them, in accordance with the Reports Consolidation Act of 2000 and Office of Management and Budget Circular A-136 (revised July 14, 2025). The Top Challenges document that we issued in March 2025 was based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities. By statute, the FDIC OIG is required to include this assessment in the FDIC's Annual Report, which was issued on March 20, 2025.

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

We identified the following eight Top Challenges facing the FDIC.

1. Enhancing Governance

- Fostering Agency-wide Coordination to Work as One-FDIC
- Measuring Progress Towards Mission Goals

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

2. Establishing Effective Human Capital Management

- Understanding the Impact of Staffing Changes at the FDIC
- Sustaining a Safe and Accountable Workplace Culture

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

3. Ensuring Readiness to Execute Resolution and Receivership Responsibilities

- Improving Planning for Large Regional Bank Resolutions and Orderly Liquidations

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

4. Identifying and Addressing Emerging Financial Sector Risks

- Escalating Supervisory Actions through Forward-Looking Supervision and Consideration of Non-Capital Triggers
- Examining for Financial Crimes and Sanctions Risks
- Assessing Crypto-Related Activities Risks

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

5. Assessing Operational Resilience in the Financial Sector

- Examining for Third-Party Operational Risks
- Assessing Banks' Cybersecurity Risks

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

6. Improving Contract Management

- Adhering to Contracting Requirements and Internal Controls
- Ensuring the FDIC's Contracting Process is Free from Conflicts of Interest

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

7. Ensuring Information Technology (IT) Security and Scalability

- Fostering IT Systems Security
- Providing IT Scalability During Crises

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

8. Guarding Against Harmful Schemes

- Keeping Pace with Payment Schemes
- Addressing Misuse of the FDIC Name and Logo

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

While the above challenges are not rank ordered, we believe that enhancing FDIC governance is critical to ensure that FDIC Divisions and Offices work together to address all identified Top Challenges.

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:

- **Oversight of the Infrastructure Support Services Contract:** Our objective is to determine whether the FDIC provided effective oversight of the Infrastructure Support Services contract to ensure compliance with service level metrics, invoice review and approval procedures, and data protection and security controls.
- **FDIC's Student Residence Center:** Our objective is to assess the FDIC's efforts to determine the cost benefits of, and organizational risks associated with, operating the Student Residence Center.
- **Cyber Incident Detection and Response:** Our objective is to determine the effectiveness of the FDIC's incident response function to detect, analyze, and respond to cyber threats related to FDIC Value Assets.
- **Valuation Process for Large Regional Bank Resolutions:** Our objective is to determine whether the FDIC adhered to established policies and procedures for the valuation function in response to the failures of Silicon Valley Bank, Signature Bank of New York, and First Republic Bank.
- **In-Depth Review of Pulaski Savings Bank:** Our objectives are to (1) determine the causes of failure and the resulting loss to the DIF; and (2) evaluate the FDIC's supervision of the bank, including implementation of Prompt Corrective Action provisions of Section 38 of the FDI Act.

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.

On July 11, 2022, we issued a Memorandum to senior FDIC officials expressing our concerns regarding the FDIC's handling of OIG emails. On July 28, 2022, the FDIC's Chief Information Officer (CIO) responded that the organization takes very seriously the security and proper handling of FDIC email. Subsequently, on February 16, 2023, we received a written plan for modernizing the OIG's email infrastructure, which, based on the OIG's feedback, was updated and provided to the OIG on March 31, 2023. The revised plan was broken into two phases, and outlined the challenges, solutions, and milestones planned for 2023 and 2024 to modernize the FDIC and OIG email infrastructure. The first phase began in the second quarter of 2023 and was scheduled to end in the fourth quarter of 2023. The second phase was planned to begin in the first quarter of 2024 and be completed by the end of calendar year 2024. On April 22, 2024, the CIO communicated that the project was on track for completion in 2024. Throughout the duration of this project, the OIG has requested updates concerning the completion of project. Currently, the first phase has been mostly implemented, while the second phase is still incomplete.

Implementation of both phases is critical to meet the OIG's mission and ensure the confidentiality and timely receipt of OIG email from complainants, whistleblowers, and law enforcement partners. We will continue to coordinate with the CIO on this matter and hope to resolve the issues promptly.

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 27 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 (ORMIC) 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 9 of the 27 should have been closed in a timelier manner. As of September 30, these nine were being worked on by the FDIC.

We note that we included five of these nine open recommendations over one year old as needing priority attention in our prior semiannual report. Those are indicated below as "repeat."

ORMIC had also indicated that going forward, it would take steps to better ensure timely completion of outstanding OIG and Government Accountability Office recommendations.

To that end, ORMIC's Power BI dashboard provides Senior Executives with greater insight into the status of all open recommendations (e.g., on-time, extension likely, past due). Additionally, ORMIC works with Divisions and Offices to track, monitor, and provide feedback on closing recommendations that remain open beyond one year. The number of unimplemented recommendations over one-year old has gone from 29 as reported in our prior semiannual report to 27 as of the end reporting period.

A listing of the nine recommendations of concern follows. The OIG will continue its efforts to ensure the timely implementation of all open recommendations.

With FDIC Management for Action

EVAL-23-002, *Sharing of Threat and Vulnerability Information with Financial Institutions* (August 29, 2023)

Recommendation #10: Ensure that all data sets within the FDIC that contain relevant threat and vulnerability information are assessed and natural language processing or alternative technological capabilities are considered for enhancing threat and vulnerability information sharing operations. **(Repeat)**

AUD-23-004, *The Federal Deposit Insurance Corporation's Information Security Program – 2023*, (September 13, 2023)

Recommendation #1: Implement process improvements to ensure prompt notification and removal of user network accounts on or before the user's separation date. **(Repeat)**

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

Recommendation #2: 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.

Recommendation #3: Apply Tier III policies and procedures to develop and consistently maintain institution-specific resolution planning documents for all nonbank financial companies and financial market utilities designated by the Financial Stability Oversight Council as systemically important.

Recommendation #9: Conduct and document a representative survey or other assessment of the Orderly Liquidation Authority-related skill sets existing or needed within the Division of Complex Institution Supervision and Resolution and ensure the Division's Professional Development Plan incorporates the results.

Recommendation #11: Regularly conduct and document Orderly Liquidation Authority general and functional training and ensure that training is clearly linked to the key components of the systemic resolution framework and processes.

EVAL-24-02, *Material Loss Review of Signature Bank of New York* (October 23, 2023)

Recommendation #5: Implement target metrics and monitor variances for key supervisory outputs consistent with requirements contained in Continuous Examination Process Procedures, such as: a. Supervisory Plan percentage completed to actual percentage completed to identify and take timely corrective action when examination teams are not on track to achieve objectives detailed in annual supervisory plans. b. Target review start date to actual review start date to identify and take timely corrective action when examination teams are not on track to achieve objectives detailed in annual supervisory plans. c. Number of days elapsed between target review start date and exit meeting to expectation to identify and take corrective action when reviews are not being completed and informal results communicated to the bank timely. d. Number of days elapsed between target review start date and issuance of Supervisory Letter to expectation to identify and take corrective action when the results of reviews are not being completed and results communicated to the bank timely. e. Number of days elapsed between year-end and Reports of Examination issuance to expectation to identify and take corrective action when Reports of Examination are not being completed and results communicated to the bank timely. f. Number of days elapsed between quarter-end and issuance of Ongoing Monitoring Reports to expectations to identify and take corrective action when ongoing monitoring is not being completed timely. **(Repeat)**

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

Recommendation #2: Evaluate and consider enhanced solutions to store backup data, as described in the report, and update the Storage Systems Backup Data Protection Standard Operating Procedures, as appropriate. **(Repeat)**

Recommendation #4: 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. **(Repeat)**

The above discussion reflects the status of the recommendations listed as of September 30, 2025. 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 second Guiding Principle, the **FDIC OIG investigates significant matters of wrongdoing and misconduct relating to FDIC employees, contractors, and institutions**. We do so by:

- Working on important and relevant cases that have the greatest impact.
- Building and maintaining relations with FDIC and law enforcement partners to be involved in leading banking cases.
- Enhancing information flow to proactively identify law enforcement initiatives and cases.
- Recognizing and adapting to emerging trends in the financial sector.

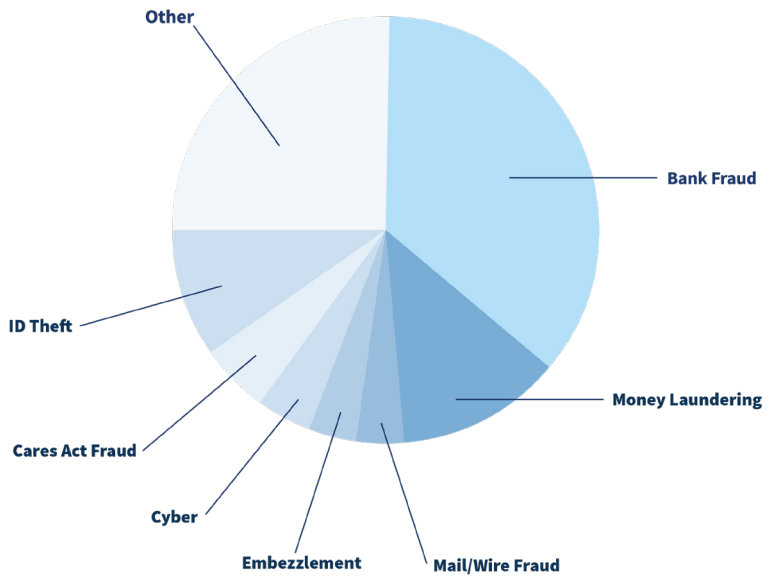
Our investigations are largely based upon referrals from the FDIC; our law enforcement partners, including other OIGs; the Department of Justice (DOJ), including U.S. Attorneys' Offices (USAO) and the Federal Bureau of Investigation (FBI); and referrals from our OIG Hotline. Our Office plays a key role 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 60 indictments/informations, 59 convictions, 47 arrests, and more than $494 million in fines, restitution ordered, and other monetary recoveries. We opened 60 cases and closed 58 during the reporting period. We referred nine investigative reports to FDIC management for action.

Open Investigations

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

Open Investigations – Allegations



Other includes allegations such as Abuse of Position, Bank Secrecy Act Violations, Misappropriation, Theft, Kickbacks/Bribery, Mortgage Fraud, Elder Fraud, Contract Fraud, Conspiracy, Misrepresentation of FDIC/False Personation, False FDIC Affiliation, Theft of Government Property, Disclosure of Information, Conflicts of Interest, Ethics Violations, and Employee Matters.

The OIG's Body Worn Camera Program

Our Office of Investigations (OI) successfully implemented its body worn camera program in the summer of 2023. OI collaborated with our Office of General Counsel to design a comprehensive training curriculum spanning 2 days, covering legal aspects, policy compliance, technical proficiency, application of skills, and scenario-based tactics training. OI agents were trained in Maryland, Texas, and Virginia. Upon the completion of the training, online refresher courses were also given. We continue to conduct refresher training and have incorporated the training as part of our New Agent Training.

Electronic Crimes Unit

Our Electronic Crimes Unit (ECU) is an important component within our OI. It is responsible for investigating complex financial cybercrimes and providing forensic support, cryptocurrency tracing, and technical program assistance to our Special Agents. The ECU remains committed to ensuring that Special Agents are equipped with the most advanced hardware, software, and technology available to investigate financial crimes that directly and indirectly impact FDIC programs and operations.

In support of this mission, the ECU is continually assessing emerging technologies, fostering strategic partnerships, and delivering expert forensic support to Special Agents.

Over the past several years, the ECU has invested in the development of the ECU Forensic Laboratory to enhance the ability of Special Agents to process substantial volumes of electronic evidence in support of cyber and complex financial fraud investigations. The state-of-the-art Forensic Laboratory enables Special Agents to conduct investigations from virtually any location, using advanced hardware and software solutions. Additionally, the Forensic Laboratory serves as a platform for conducting complex data analysis, eDiscovery, and forensic examinations of electronically stored information.

ECU Special Agents are tasked with investigating complex financial cybercrimes that directly and indirectly affect FDIC programs 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.

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.)

Pandemic-Related Financial Crimes

Since many of the programs in the Coronavirus Aid, Relief, and Economic Security (CARES) Act and related legislation have been administered through banks and other insured institutions, our Office of Investigations 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.

Notably, during the reporting period, the FDIC OIG's efforts related to the Federal government's COVID-19 pandemic response resulted in 11 charging actions (indictments, informations, and superseding indictments and informations), 8 arrests, and 11 convictions involving fraud in the CARES Act programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases totaled $31,333,546.97.

Leveraging Data Analytics to Advance Audits and Investigations
Importantly, our office continues to develop its data analytics capabilities – to use technology in order to cull through large datasets and identify anomalies that the human eye cannot ordinarily detect. We are gathering relevant internal and external datasets, developing cloud-based tools and technology in conjunction with the Corporation, and in 2023 hired in-house data science expertise – in order to marshal our resources and harness voluminous data.

During the reporting period, we migrated numerous mission critical data sets into the data lake to permit access to advanced analytical tools. In particular, the OIG has focused on access to data that assists in the prevention of commercial and residential real estate-related bank fraud. The OIG has finished deploying data management and query tools and a suite of natural language processing tools. The OIG is currently testing generative artificial intelligence (AI) tools--to be available in fiscal year 2026--to enhance our data analytic capabilities and improve the efficiency of OIG operations. Roughly one-third of the OIG completed dashboard and data visualization training. The OIG is also engaged in data analytics outreach and partnerships with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and is coordinating a joint session at the 2026 FDIC Data Summit with the Federal Trade Commission (FTC) 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 Office of Investigations, in particular, also involve collaboration with the Pandemic Response Accountability Committee, the FDIC, Financial Crimes Enforcement Network, and as noted above, DOJ, FBI, FTC, 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.

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.

As noted in our prior semiannual report, after conducting a peer review of OI, the Department of Veterans Affairs 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 other applicable guidelines and statutes. Our investigative work continues to adhere to these quality standards and guidelines.

Startup CEO Charlie Javice Sentenced to 85 Months in Prison for $175 Million Fraud

On September 29, 2025, in the Southern District of New York, company CEO Charlie Javice (Javice) was sentenced to 85 months in prison, 3 years of supervised release, and ordered to pay a forfeiture judgment of $22,360,977.48 and restitution in the amount of $287,501,078.00 (joint and several with a co-defendant). Javice was previously convicted in March 2025 after a 6-week trial for conspiracy to commit wire fraud and bank fraud, wire fraud, bank fraud, and securities fraud. Olivier Amar, the company's Chief Growth Officer, was also convicted at trial and was scheduled to be sentenced on October 20, 2025.

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

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

Personal Banker Sentenced for Embezzling

On September 26, 2025, Norlen Hurtado Rodriguez (Rodriguez) was sentenced to 7 months' imprisonment, 8 months of home confinement, and 3 years of supervised release for embezzling over $200,000 from Regions Bank. A restitution hearing was scheduled for December 18, 2025.

Rodriguez was a Personal Banker at Regions Bank in Coral Gables, FL. In or about October 2023, Rodriguez was approached by four unknown individuals at an establishment in Hialeah, FL who began threatening Rodriguez with physical violence. A fifth unknown individual intervened and prevented any altercation from occurring. The fifth unknown individual, who introduced himself to Rodriguez only as "Papo", apologized to Rodriguez and invited him to return to the establishment the following night as Papo's guest. At the subsequent meeting, Papo told Rodriguez that he knew where Rodriguez lived, and that he knew Rodriguez worked for Regions Bank. Papo told Rodriguez that he had to use his position at Regions Bank to repay Papo for saving him from physical assault during the altercation the prior day. Rodriguez conceded, fearful of the fact that Papo knew where he lived and worked.

Papo initially instructed Rodriguez to wire funds from Regions Bank customers directly to Papo, but Rodriguez declined stating that wires required the approval of a supervisor and thus would not be approved. Papo then instructed Rodriguez to provide him with account information for Regions Bank's high net worth clients. Rodriguez accessed the Regions Bank client database and provided the account information for two high net worth Regions Bank clients to Papo, resulting in fraudulent Automated Clearing House (ACH) transactions totaling approximately $110,000. In addition, Rodriguez ordered blank checks using the account information of another high net worth individual. These checks were subsequently used to make numerous fraudulent payments to various parties, totaling approximately $96,000.

Source: This investigation was initiated from a referral by Regions Bank Corporate Security.
Responsible Agencies: This investigation was conducted by the FDIC OIG and United States Secret Service and is being prosecuted by the USAO for the Southern District of Florida - Miami.

Bank Insider Pleads Guilty to Conspiracy to Commit Wire Fraud

On August 14, 2025, Bernard Petit-Frere (Petit-Frere) pled guilty to one count of conspiracy to commit wire fraud, a violation of 18 U.S.C. § 1349. Previously, on June 11, 2025, Petit-Frere was arrested via self-surrender and charged with conspiracy to commit wire fraud, in West Palm Beach County, FL.

From in or around March of 2022, and continuing through in or around May of 2022, while employed as the lead teller and vault custodian at JPMC Bank in West Palm Beach County, FL, Petit-Frere utilized his position and authority to override bank systems to allow ill-gotten proceeds to be withdrawn by his alleged co-conspirators. Petit-Frere's alleged co-conspirators stole checks from a non-profit organization in the State of Florida (checks from private citizens) and subsequently deposited checks into JPMC accounts owned by witting money mules. Additionally, Petit-Frere's alleged co-conspirators conducted fraudulent ACH transfers into accounts owned by witting money mules. Petit-Frere contributed to the conspiracy by aiding and assisting his alleged co-conspirators with withdrawing cash from deposited fraudulent checks, fraudulent ACH transfers, and conducting structured transactions. Petit-Frere received cash kickback payments for his role in the conspiracy. The loss to JPMC was approximately $919,962.

Source: JPMC, Internal Investigations.
Responsible Agencies: This is a joint investigation by the FDIC OIG and FBI. The case is being prosecuted by the USAO for the Southern District of Florida.

Former Bank Vice President Sentenced to 5 Years in Prison for Embezzlement Scheme
On August 12, 2025, Kellie Johnson (Johnson) was sentenced to 60 months in prison, followed by 5 years of supervised release, and ordered to pay $2,111,943.21 in restitution. Previously on May 14, 2025, Johnson was convicted on one count of bank embezzlement (18 U.S.C. 656) in the Northern District of Alabama for embezzling over $2.3 million from First Community Bank of Cullman (FCBC).

Johnson served as Vice President, Chief Operations Officer, Information Security Officer, and Bank Secrecy Act Officer. Johnson had access to and was responsible for maintaining FCBC's ACH account with the Federal Reserve Bank of Atlanta (Federal Reserve). Specifically, Johnson was responsible for reconciling FCBC's Federal Reserve account and periodically reporting the account balance to FCBC's President, external auditors, and others. From at least July 2013 through June 2023, Johnson stole money belonging to FCBC to pay personal expenses, primarily credit card bills, by posting ACH transactions from FCBC's Federal Reserve account to her personal accounts. To conceal her scheme, Johnson falsified transactions to reconcile the balance of the Federal Reserve account in FCBC's general ledger and deleted her unauthorized ACH transactions. Further, Johnson repeatedly altered account statements sent by the Federal Reserve that she was required to provide to FCBC's President, auditors, and others. For over a decade, Johnson conducted approximately 273 fraudulent ACH transactions and embezzled approximately $2,376,325 in FCBC funds. Additionally, Johnson deprived FCBC of approximately $138,185 of interest income that would have been earned had she not stolen money from FCBC's Federal Reserve account.

Source: This investigation was initiated from a referral by the FDIC Division of Risk Management Supervision (RMS) and FCBC.
Responsible Agencies: This case was investigated by the FDIC OIG and prosecuted by the USAO for the Northern District of Alabama.

Former FDIC Employee Pleads Guilty to Exploiting a Child

On August 7, 2025, Jonathan Mackey (Mackey), a former FDIC Acting Supervisory Examiner in RMS, pleaded guilty in the Southern District of Ohio to 18 U.S.C. § 2251(a) & (e) - Sexual Exploitation of Children. Mackey faces a sentence of 180 to 262 months in prison. Mackey was previously indicted on April 30, 2025 for Sexual Exploitation of a Child and Receipt of Child Pornography.

On February 4, 2025, Homeland Security Investigations (HSI) contacted the FDIC OIG regarding a child sexual abuse material investigation with allegations involving Mackey. The Ohio's Internet Crimes Against Children Task Force identified a username belonging to Mackey where he was chatting with a user purporting to be an underaged female and images were exchanged. On February 10, 2025, a search warrant was executed at Mackey's residence. Based on the results of that search warrant and the investigation, agents identified that Mackey was communicating with underaged victims using the usernames "john370000#0" and "johnm1861#0." A review of the chats identified additional possible victims and child sexual abuse material.

According to court documents, in May 2024, Mackey sexually exploited an 11-year-old and created photos of the abuse. As part of his plea, Mackey immediately resigned from the FDIC.

Source: This investigation was initiated based on a referral by HSI. Responsible Agencies: This investigation was conducted by the FDIC OIG and HSI and is being prosecuted by the USAO for the Southern District of Ohio.

Federal Employee and Government Contractor Pleads Guilty to Conspiracy to Commit Wire Fraud

On July 17, 2025, in the U.S. District Court for the District of Columbia, Melanie James (James) pled guilty to one count of 18 U.S.C. § 1349 (conspiracy to commit wire fraud). James was charged by criminal information on June 27, 2025 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 terms and conditions of the contracts.

Beginning in January 2019, and continuing through at least June 2025, James 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 electronic Official Personnel Folder). 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, James and others billed more than 40 hours in a single day across multiple contracts. Additionally, James served as a career permanent GS-14 Management and Program Analyst at the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA) while simultaneously working on five other government contracts. One of James' co-conspirators worked as a career permanent GS-15 at DHS CISA and another worked as a career permanent GS-13 at the Department of Housing and Urban Development while involved in the scheme. All three 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 James 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 James was approximately $708,000.

Source: This investigation was initiated based on a request for assistance from the AmeriCorps OIG's Office of Investigations.
Responsible Agencies: This is a joint investigation by the FDIC OIG, AmeriCorps OIG, FBI, Defense Criminal Investigative Service, DHS OIG, Health and Human Services OIG, General Services Administration OIG, Treasury Inspector General for Tax Administration, Housing and Urban Development OIG, Department of Energy OIG, and Pension Benefit Guaranty Corporation OIG. This matter is being prosecuted by the USAO for the District of Columbia.

Financial Advisor Who Conspired in Multi-Million Dollar Bank Fraud Pleads Guilty

On June 16, 2025, Jesse T. Hill (Hill), a former investment advisor, pled guilty to one count of conspiracy to commit bank fraud for his role in an investment fraud scheme. Additionally, Hill agreed to pay restitution and forfeit his interest, if any, in a property in Puerto Rico, a PC-12/47E Pilatus Aircraft, and funds in a Charles Schwab account.

Hill was an investment advisor operating in Nebraska. Individual 1 operated a real estate business in Nebraska (deceased on November 2, 2022). Beginning in November 2020, Hill and Individual 1 began attempting to obtain loans from financial institutions throughout Nebraska and western Iowa. The loans were sought in the name of Individual 1 and/or Individual 1's entities. Representations were made to the financial institutions that these loans would be used for real estate investments, and the alleged collateral for the loans was an investment account of Individual 1 and/or Individual 1's entity that was managed by Hill. Hill and Individual 1 would grant a surety with the financial institution, typically in the form of a control agreement, a commercial security agreement, or an assignment of account. Hill would falsely claim that Individual 1 and/or Individual 1's entities were clients of his through his own investment entities JT Equity Trading, LLC or First SOJO. Hill would prepare and present fraudulent invoices to the financial institutions. Hill would falsely represent values of alleged funds that Individual 1 and/or an entity of Individual 1 had in an account that Hill managed. Hill would falsely represent that no other financial institution had a security interest in these fictitious accounts.

Throughout the process of obtaining or attempting to obtain the loans, Hill and Individual 1 would meet with and/or communicate with each financial institution to facilitate the loan process. Hill knew that the representations being made to the financial institutions to obtain loans by Individual 1 and/or Individual 1's entity were false and were being done with the intent to defraud the financial institutions. As a result of this scheme, Hill and Individual 1 attempted to obtain at least $45,650,000.00 in loans from at least 19 different financial institutions. The majority of the funds that were fraudulently obtained went into a failed investment scheme. A portion of the proceeds from the fraudulent loans obtained later in the scheme were used to pay off or pay down fraudulent loans obtained earlier in the scheme. Proceeds were deposited in a Charles Schwab account, were used to purchase a property in Puerto Rico, and were used to purchase an ownership interest in a PC-12/47E Pilatus Aircraft.

Source: USAO for the District of Nebraska.
Responsible Agencies: This is a joint investigation by the FDIC OIG, FBI, Federal Housing Finance Agency (FHFA) OIG, and Federal Reserve Board OIG. Additional assistance was provided by the Nebraska State Patrol, Lincoln Police Department, and the Lancaster County Sheriff's Office. The matter is being prosecuted by the USAO for the District of Nebraska.

Bank Employee Who Conspired with Others to Embezzle Sentenced to Prison

On September 29, 2025, in the Northern District of Illinois, Alicia Mandujano (Mandujano) was sentenced to 1 day of time served and 12 months of home confinement for her role in the failure of Washington Federal Bank for Savings (WFBS). Mandujano was also ordered to pay $27 million in restitution to the FDIC.

Mandujano was employed at WFBS for over 20 years until the bank's failure in 2017. Beginning in at least 2004, Mandujano conspired with other WFBS employees (and co-defendants) to embezzle funds from WFBS for the benefit of WFBS borrowers and co-defendants Robert Kowalski (Kowalski), Boguslaw Kasprowicz (Kasprowicz), Miroslaw Krejza (Krejza), and Marek Matczuk (Matczuk), and to conceal the embezzlement through false entries in WFBS's books and records.

Specifically, Mandujano worked with her co-defendants to embezzle and misapply WFBS funds totaling approximately $66 million for the benefit of favored borrowers of former WFBS President John Gembara (Gembara). Mandujano conspired to distribute embezzled WFBS funds to her co-defendants under the guise that the embezzled funds were legitimate loan proceeds. Each month, Mandujano made journal entries to "advance" the payments on the fraudulent loans to her co-defendants, causing the balance of each loan to increase by the amount of the payment – effectively loaning the defendants the money to make each monthly payment, knowing no loan payments were actually coming into WFBS. Mandujano and her co-defendants then altered WFBS records to conceal the fraudulent loans from regulators.

Gembara disappeared from WFBS during the bank's final regulatory examination in 2017 and was later found dead in the home of co-defendant Matczuk in December 2017. Mandujano subsequently acknowledged the advanced payment scheme to the Office of the Comptroller of the Currency, and WFBS failed shortly thereafter. Mandujano began cooperating with the government immediately and was the last of 16 defendants to be sentenced in the investigation related to the failure of WFBS.

Source: USAO for the Northern District of Illinois.
Responsible Agencies: This investigation was conducted jointly by the FDIC OIG, FBI, Housing and Urban Development OIG, Federal Housing Finance Agency OIG, Internal Revenue Service-Criminal Investigation, Treasury OIG, City of Chicago OIG, and the Chicago Housing Authority. The case was prosecuted by the USAO for the Northern District of Illinois.

Texas Company Guilty of Aiding and Abetting Fraudulent Transactions Related to False Ethanol Sales Pays Over $15,000,000 in Fines, Restitution

On July 10, 2025, Murex Management, Inc. (MMI) entered a guilty plea and was sentenced for aiding and abetting transactions that defrauded financial institutions (18 U.S.C. § 1005 and 18 U.S.C. § 2), including failed New Orleans-based First NBC Bank. MMI was sentenced to pay $15,745,846.10 in fines and restitution, a sum that MMI paid on the day of sentencing as part of its plea agreement in this case.

According to court documents, MMI was the management company and affiliate of Murex LLC, a privately-owned ethanol marketing and logistics company. Another company, named as "Company A" in court records, was the U.S.-based subsidiary of a separate, foreign publicly traded company that operated ethanol production plants. Beginning in 2013, Company A and its parent companies began to experience financial stress. In order to ameliorate cash flow issues and to manufacture additional financing for its debts, Company A initiated a strategy called "buy/sells" and approached MMI to assist in this strategy. Company A's plan called for Company A and MMI, through its affiliate, to create fictitious invoices purporting to be sales of ethanol between the two companies, which could then be sold as accounts receivable to unwitting buyers via a New Orleans-based online marketplace. This strategy would provide cash flow for Company A and a profit to MMI. Although these invoices purported to show the bona fide sale of ethanol between MMI and Company A, in fact, no ethanol was exchanged between the companies through these transactions. The unwitting buyers of these fraudulent accounts receivable included FDIC-insured financial institutions First NBC Bank and First National Bank of Pennsylvania.

In plea documents, MMI admitted that, between October 28, 2013, and September 18, 2015, Company A and MMI conducted approximately $1.2 billion in fraudulent "buy/sell" transactions, with MMI making a profit of approximately $6,073,049. Company A eventually defaulted on paying the financial institutions for the accounts receivable that had been posted for auction by MMI. The defaulted auctions caused a loss of approximately $73,073,683.05 to First NBC Bank, and a loss of approximately $8,330,427.02 to FNB Pennsylvania. As part of MMI's plea agreement, it agreed to a fine of $6,073,049.24. Furthermore, MMI agreed as part of its plea to pay $4,263,145.30 in restitution to the FDIC as Receiver for First NBC Bank, as well as $5,409,651.56 to First National Bank of Pennsylvania.

Source: The FDIC Division of Resolutions and Receiverships. Responsible Agencies: This is a joint investigation by the FDIC OIG and Environmental Protection Agency-Criminal Investigation Division. The matter is being prosecuted by the USAO for the Eastern District of Louisiana.

Special Feature

FDIC OIG Combats Fraud Through Awareness and Education

The OIG supports global efforts to minimize the impact of fraud by promoting anti-fraud awareness and education. As an independent office at the FDIC that works to detect and deter waste, fraud, and abuse, the OIG wants to inform readers of the impact fraud can have and how the OIG works to combat fraud in the banking system.

What is fraud? The term fraud encompasses actions that are meant to deceive for financial or personal gain. It's any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means.

Why should we care about fraud? Fraud causes billions of dollars in damage to companies, governments, and individuals each year. Additionally, fraud can dramatically affect the quality of life of its victims — and the employees of its victims — resulting in job losses, the loss of savings and investments, weakened trust in public institutions, and a significant strain on resources.

How does fraud impact the banking system? Fraud directly impacts FDIC-insured financial institutions when insiders abuse their positions of trust to commit fraud, collude with borrowers and third parties to commit fraud, fail to appropriately monitor and report suspicious activities, or conceal material information from Federal and state regulators. Insider fraud adversely affects a financial institution's financial condition, and, in some cases, can lead to the failure of a financial institution. Bad actors within the financial system pose a risk to FDIC-insured financial institutions and undermine the stability and public confidence in the Nation's financial system.

Cyber-related fraud also impacts FDIC-insured financial institutions and FinTech companies, particularly in cases where employees compromise banking or personally identifiable information using social media and other digital platforms to then sell the information.

How does the FDIC OIG address fraud? The FDIC OIG Office of Investigations investigates allegations of crimes involving FDIC-regulated and -insured banks and FDIC activities, and has specialized expertise in financial crimes, fraud investigations, and cybercrimes. Recent investigative outcomes found on our website at fdicoig.gov/news/investigations-press-releases showcase the importance of fraud detection and prevention.

How does the FDIC OIG provide education about fraud? The FDIC OIG helps educate the FDIC workforce and regulatory stakeholders on fraud by teaching classes through the Federal Financial Institutions Examination Council (FFIEC) that help examiners identify red flags for fraud during examinations, teach them the document types they may want to examine if they identify potential fraud, and understand techniques for examining those documents (including tracing funds).

Special Feature (continued)

The FDIC OIG also regularly participates in FFIEC- and FDIC-sponsored conferences, including, most recently, the 2025 FDIC Data Summit, FFIEC 2025 Financial Crimes Seminar, 2024 FDIC Accounting and Auditing Conference, 2024 FDIC/DOJ Financial Crimes Conference, and 2024 Financial Crimes Seminar.

Additionally, the FDIC OIG engages in outreach efforts across the country to educate the public and other stakeholders on fraud. We participate in task forces, partnerships, and initiatives aimed at identifying and stopping the flow of illicit funds.

The FDIC OIG also participates in the FBI's "Operation Level Up," which is a proactive approach to identify and notify victims of cryptocurrency investment fraud and halt fraud. Operation Level Up has prevented well over $400 million in fraud losses to date.

Visit the FDIC OIG's website, X account, and LinkedIn page for more information about common fraud scams and how to avoid becoming a victim. And, remember: If you suspect fraud, waste, abuse, mismanagement, or misconduct in FDIC programs or operations, or at FDIC-insured banks, you should report those allegations to the FDIC OIG Hotline.

Strong Partnerships with Law Enforcement Colleagues

The OIG has partnered with various USAOs throughout the country in bringing to justice individuals who have defrauded the FDIC or financial institutions within the jurisdiction of the FDIC or criminally impeded the FDIC's examination and resolution processes. The alliances with the USAOs have yielded positive results during this reporting period. 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 41 locations in the U.S.

Alabama	Kentucky	North Carolina
Arizona	Louisiana	Ohio
Arkansas	Maryland	Oklahoma
California	Massachusetts	Oregon
Colorado	Michigan	Pennsylvania
Connecticut	Minnesota	Rhode Island
District of Columbia	Mississippi	Tennessee
Florida	Missouri	Texas
Georgia	Montana	Virginia
Hawaii	Nebraska	Washington
Illinois	Nevada	West Virginia
Indiana	New Hampshire	Wisconsin
Iowa	New Jersey	Wyoming
Kansas	New York	

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 during the reporting period.

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; Philadelphia Financial Exploitation Prevention Task Force; 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 U.S. Secret Service Financial Crimes Task Force; 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.
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	SAR Review Team for Northern District of Mississippi; SAR Review Team for Southern District of Mississippi; 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 Key Priorities

In addition to the audits, evaluations, investigations, and other reviews conducted during the reporting period, our Office has emphasized other priority initiatives that complement our efforts. Specifically, in keeping with our Guiding Principles, we have focused on **strengthening relations with partners and stakeholders, efficiently and effectively administering resources, and promoting leadership and teamwork**. A brief listing of some of our key efforts in these areas follows.

Strengthening relations with partners and stakeholders.

- Communicated with the Acting 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 Acting Chairman, in his capacity as Chairman of the FDIC 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 reviews 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.
- Extended outreach to two new FDIC Board Members: the Comptroller of the Currency and the Acting Director, Consumer Financial Protection Bureau, offering to discuss our oversight role and work.
- Continued to enhance 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.
- Served as trainers for several forums, including offering a session on Material Loss Reviews at the FFIEC's conference on *Supervisory Updates and Examination Issues for Large, Complex Financial Institutions*; teaching a class offered by the FFIEC called *Fundamentals of Fraud;* and presenting at the *FFIEC Fraud Investigation Techniques for Examiners* course.

- Issued a joint announcement with the FDIC Acting Chairman to all FDIC staff to acknowledge Whistleblower Appreciation Day, reminding everyone of the obligation to report fraud, waste, abuse, mismanagement, and misconduct at the FDIC and provided information on how to report such instances.
- Participated in the Government Accountability Office/CIGIE Financial Statement Audit conference, with the FDIC IG presenting opening remarks.
- 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.
- Provided FDIC OIG input for the CIGIE annual report, to include audit, evaluation, and investigative results.
- Received acknowledgement from Arlington County, VA police when the OIG's Special Agent in Charge of the Electronic Crimes Unit and one of his Special Agents were awarded for a case they worked in conjunction with the police. Also recognized OIG and other Federal law enforcement personnel during National Police Week with social media mentions on X and other acknowledgments.
- Participated on CIGIE's Subcommittee on Quality Management—under the auspices of the IG community's Audit Committee and Federal Audit Executive Council (FAEC) to promote an understanding of updated standards in Chapter 5 of the Yellow Book and produce a toolkit. The IG community reviewed and approved the Yellow Book Chapter 5 Toolkit and related appendix.
- Served as Working Group Lead for the guide on Best Practices for Federal Agencies to Strengthen Cloud Security and as a member of the Working Group for the guide on OIG Best Practices for Cloud Computing.
- Supported the FAEC Audit Training Subcommittee and its annual FAEC conference. This year's theme was "Navigating the Future of Oversight: Modernization, Adaptability, and Leadership in Changing Times." The conference featured presentations from FAEC leadership, the CIGIE Training Institute, and Government Accountability Office Green Book updates.
- Participated in a virtual Association of Government Accountants panel for professional development training related to audits, evaluations, and inspections, focusing on the applicable professional standards to follow when conducting oversight work.
- Responded to a media inquiry related to the OIG's Material Loss Reviews and the relationship of fraud and bank failures. The inquiry provided the OIG an opportunity to view bank failures from both an audit and investigative perspective.
- Played an active role with the AARP in outreach activities that the organization is sponsoring to convey the FDIC OIG OI mission and priorities as well as to discuss the proliferation of Impersonation Scams that may target and exploit elder members of society, a vulnerable segment of our population.

- Arranged for two detailees from the Office of Audits on an as-needed, part-time basis to work with the Federal Communications Commission OIG's Investigative Support Services. They are providing 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 Office of Investigations.

- 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.

- 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; monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the FDIC's Office of Legislative Affairs on Congressional matters pertaining to the OIG.

- Interacted with Congressional staff: briefed staff from Senator Ernst's office on matters related to a letter received by the IG from the Senator regarding allegations of gross mismanagement; briefed Senate Banking Minority staff on the OIG's identification of the Top Management and Performance Challenges Facing the FDIC; and briefed Majority staff from the House Financial Services Committee on Part 2 of the OIG's Special Inquiry of the *FDIC's Workplace Culture with Respect to Harassment and Related Misconduct*.

- Responded to a letter from Senate Banking Ranking Member Elizabeth Warren and Senator Chris Van Hollen regarding the FDIC OIG's decision to suspend further work on succession management and employee retention practices.

- 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 513 Hotline inquiries, 22 of which led to our opening investigations. Our on-line form, email, telephone, and regular mail were the most common vehicles for inquiries.

- Reiterated the Scam Alert and accompanying visual on our website highlighting impersonation schemes whereby imposters claim to be FDIC or FDIC OIG employees to gain personal information from unsuspecting victims. Also reiterated warnings about "pig butchering" which is named in reference to the practice of fattening a pig before slaughter. It is a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally in the form of cryptocurrency, to a seemingly sound investment before the scammer disappears with the contributed monies.

- Supported the broader IG community by attending monthly CIGIE meetings and other meetings, such as those of the Integrity Committee (chaired by the FDIC IG), 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 CIGIE's Legislation Committee.

- 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. Provided FDIC OIG input to the CIGFO Annual Report and participated on CIGFO's Working Group related to the Financial Stability Oversight Council's Designation of Non-Bank Financial Companies.

- Communicated and coordinated with the Government Accountability Office on ongoing efforts related to our respective oversight roles, risk areas at the FDIC, and issues and assignments of mutual interest.

- Coordinated with the Office of Management and Budget to address matters of interest related to our FY 2025 budget, FY 2026 budget, and proposed budget for FY 2027.

- Worked closely with representatives of the DOJ, including Main Justice, FBI, and USAOs, 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.)

- Represented the OIG in a wide range of external and internal engagements to strengthen the OIG's overall fraud-fighting initiatives. Among those: the Pacific Partnership Against Cross-Border Fraud, the Securities and Exchange Commission's Interagency Security Council and its "Tech Against Scams Coalition," CFTC's Public-Private Working Group, and the Federal Trade Commission's Bureau of Consumer Protection Investigative Committee. Also continued to support FDIC learning and awareness efforts through presentations and outreach across FDIC Divisions and at agency-wide trainings.

- 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 accompanying certain reports; 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.

Administering resources prudently, safely, securely, and efficiently.

- Formulated our Congressional Budget Justification for FY 2027 in which we requested a total budget of $48.5 million – approximately 3 percent or $1.5 million above the OIG's budget request for FY 2026 of $47 million. The FDIC OIG's budget request seeks the funding necessary to enable the OIG to maintain its reduced staffing level of 123 positions and backfill seven necessary and critical positions to support OIG oversight efforts and investigations in key risk areas.

- 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 completion of such training.

- Formed a Working Group from all OIG component offices to update the OIG's Strategic Plan and goals for 2025-2030. 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.

- Implemented four unpaid furlough days for OIG staff in order to cover an unanticipated funding shortfall and carry out responsible financial stewardship.
- Updated the OIG's intranet site to inform staff of administrative, facilities, and operational services of importance to OIG staff.
- Finalized an interim policy on permissible use of Artificial Intelligence (AI) and Machine Learning (ML) tools in the OIG in compliance with OMB-Memorandum M-25-21 and relevant privacy and security requirements. As a related initiative, sponsored a TEAMS forum for OIG staff to convey information on Machine Learning and Generative AI tools that would become available for OIG staff.
- Administered a survey to OIG staff to determine how best our IT team could serve the mission responsibilities and needs of the OIG.
- Adopted new GovTA timekeeping system to facilitate more effective and efficient time and attendance recordkeeping for OIG staff.
- Presented Office of Audits' proposed Annual Plan to the IG, outlining planned projects and timeframes for FY 2026 based on the Office of Audits' risk assessment.
- Held various OIG Workforce Connect sessions on the FY 2025 Budget and overall budget planning based on the administration's changes, retirement planning, and evolving Artificial Intelligence activity. We also coordinated a supervisor-only session with the FDIC's Division of Administration on the OIG Continuity of Operations function and emergency management planning.
- Carried out a number of IT initiatives, including the following: Coordinated with Chief Information Officer Organization teams on the next iteration of the ECU Lab and continued close coordination between the OIG's IT group and OI to provide optimum law enforcement support, including for a new platform procurement for an investigative case management system and planning for its migration; upgraded the OIG security dashboards to provide better "at-a-glance" and alert capabilities around the OIG data and its infrastructure and also finalized a human resources (HR) dashboard that provides multiple HR-related metrics to enable data-driven decisions; completed tasks supporting OIG operations, including upgrading firmware, patching operating systems and software, decommissioning end-of-life hardware, developing PowerApps, performing security assessments, and mitigating vulnerabilities; began implementing modern Data Loss Prevention integration into M365 and provided insights to overarching FDIC Data Loss Prevention plans; and modernized the OIG's identity platform to provide a cleaner and more secure experience for OIG users.

- 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 information technology 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. In particular, the OIG has focused most recently on access to data that assists in the prevention of commercial and residential real estate-related bank fraud. Currently, all OIG employees can access cloud-based data management software, and we are currently testing generative AI tools that will be available later in FY 2026. Roughly one-third of the OIG completed dashboard and data visualization training, and the OIG is working on additional analytics training opportunities to modernize employee skills. The OIG will continuously work to integrate additional data and analytical tools each quarter as resources permit.

- Advanced the OIG's data analytics capabilities related to Payment Protection Program fraud through collaboration with the PRAC, FDIC, Financial Crimes Enforcement Network, FTC, DOJ, FBI, and private-sector entities. Additionally, the OIG is expanding our use of commercially available data 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 review and disseminate information on a number of 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.

- 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.

Exercising leadership skills and promoting teamwork.

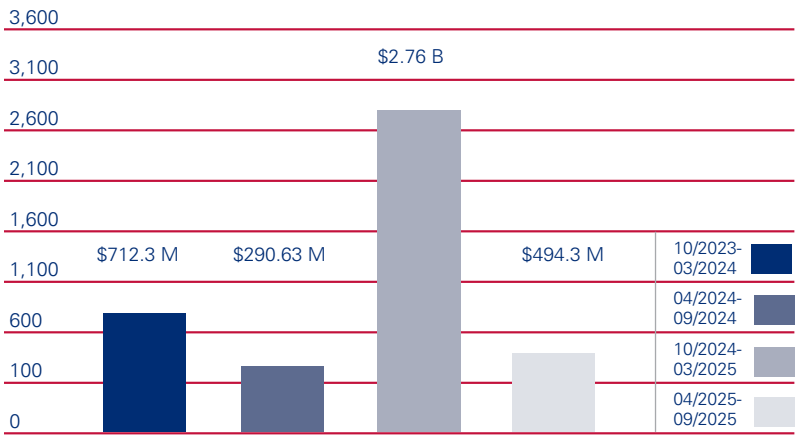
- Represented the FDIC OIG as a member of CIGIE and on its various Committees and Subcommittees. The FDIC IG served as Chair of the Audit Committee and as Chair of the Integrity Committee—with the latter role involving matters that would not relate to individuals in the FDIC OIG.
- Adhered to Attorney General training guidelines for Special Agents from Regional Offices and Headquarters with respect to use of force, firearms, and control tactics, among other law enforcement tools and best practices, to ensure Agent security and high performance.
- Held 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.
- 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. Also recruited for Workforce Council positions as several members' terms were expiring. The volunteer opportunity is open to anyone who is in a nonsupervisory or nonmanagement OIG role.
- Kept OIG staff engaged and informed of office priorities and key activities through regular meetings among staff and management; updates from senior management and CIGIE 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.
- Formulated a cross-cutting team in Office of Audits to assess risks in the FDIC and develop proposals for audit and evaluation coverage for the coming year.
- Shared information from our Training Officer throughout the OIG to promote employee engagement, teamwork, training, and career development.
- Established a mechanism for OIG staff to pose questions related to issues of concern to them—for example with respect to the government shutdown, telework policies, and other changes brought about in light of the new Administration's Executive Orders and related guidance.
- Worked with the OIG's Human Resources staff and component offices to review and update all of the OIG's Position Descriptions to ensure they are up-to-date and accurately reflect OIG roles and responsibilities.

- Held the OIG's annual Awards Ceremony to acknowledge excellent efforts and accomplishments of OIG staff and teams throughout the year.
- Submitted nominations for CIGIE Awards for Excellence in audits, evaluations, and efforts of a Monetary Benefits Working Group, on which FDIC OIG took a leadership role.
- Formed a Hotline Working Group team to address ways in which handling Hotline inquiries would best be handled and tracked.
- Posted updated information from the Office of Special Counsel in common areas to inform staff of prohibited personnel practices and whistleblower retaliation and held related training delivered by the Office of Special Counsel to all OIG staff in two sessions—one for staff and the other for managers.
- Ran a test of the OIG's Emergency Notification System to ensure safety and security of OIG staff in the event of an unforeseen incident or emergency.
- Provided leadership and professional development opportunities for Office of Audits Managers to serve as Acting Assistant Inspector General to fill the temporary vacancy of that position.
- Formed a cross-cutting team to handle formulation of the Top Management and Performance Challenges facing the FDIC. Under the Reports Consolidation Act of 2000, this analysis is submitted to the FDIC for inclusion in the FDIC Annual Report to be issued in early 2026.
- Formed a Data Analytics and Innovation Working Group to handle and educate staff on AI and Machine Learning tools currently under consideration in the OIG.
- Held a quarterly session for the OIG's Office of Management to discuss its FY 2025 accomplishments and FY 2026 initiatives and goals.

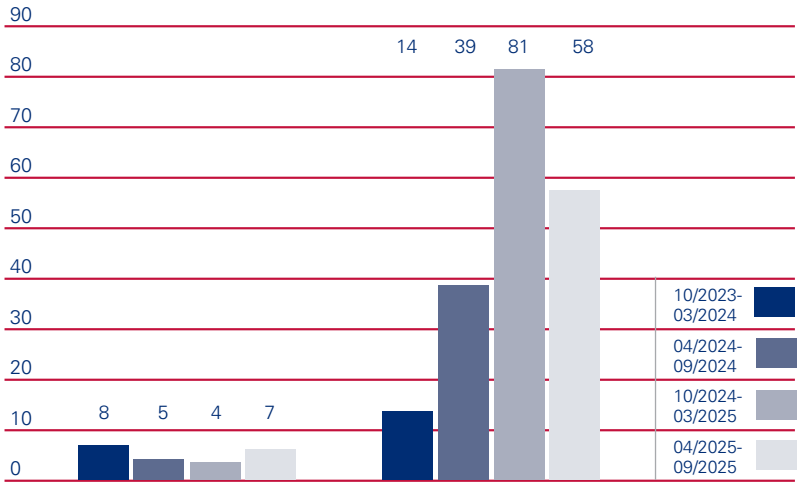
Cumulative Results (2-year period)

Recommendations	
October 2023 – March 2024	31
April 2024 – September 2024	42
October 2024 – March 2025	21
April 2025 – September 2025	23

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



Products Issued and Investigations Closed



Reporting Requirements

Index of Reporting Requirements

The following 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.

Reporting Requirements	Page
Section 4(a)(2): Review of legislation and regulations.	48-49
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.	4-12
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.)	50-61
Section 5(a)(3): A summary of significant investigations closed during the reporting period.	24-31
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.	62
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.	63
Section 5(a)(7): The information described under section 804(b) of the Federal Financial Management Improvement Act of 1996.	63
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.	66-69
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.	66-69

Reporting Requirements (continued)	Page
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.	66-69
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.	63
Section 5(a)(12): A description of metrics used for Section 5(a)(11) information.	63
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.	64
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.	64
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.	64
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.	64

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 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 considers as high priority. 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**
  - Establish a permanent, scalable data analytics platform for IGs and the agencies they oversee to help detect and prevent fraud and improper payments in all Federal spending, including for emergencies.
  - Unless Congress acts, one of the most significant tools that Congress helped create to improve program integrity and prevent fraud will be lost upon sunset on September 30, 2025: the data analytics center of CIGIE's Pandemic Response Accountability Committee (PRAC). (See update below.)
- **Prohibiting the Use of Appropriated Funds Government-wide to Deny IGs Full and Prompt Access**
  - CIGIE recommends a government-wide prohibition on the use of appropriated funds to deny an IG access and a requirement of congressional notification when access is denied.

- **Enhancing Oversight Independence and Efficiency by Providing Separate and Flexible OIG Funding**
    - CIGIE supports certain revisions to OIG funding that would help safeguard the oversight independence of OIGs, ensure effective management of OIG resources, and protect against budget cuts by agencies.

Importantly, we note that with respect to the PRAC, OMB apportioned $5 million for PRAC, ensuring that it can continue operations through the first quarter of FY 2026. Congress established the PRAC as part of the CARES Act to conduct and support government-wide oversight efforts associated with the emergency response to the Coronavirus pandemic, including through the use of a sophisticated data platform. The advanced data analytics capabilities play a critical role in detecting and preventing fraud, waste, and abuse across Federal programs.

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 27 recommendations.

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-23-002 **Sharing of Threat and Vulnerability Information with Financial Institutions** August 29, 2023	Financial institutions face a wide range of significant and persistent threats to their operations. Such threats include cyberattacks, money laundering, terrorist financing, pandemics, and natural disasters such as hurricanes, tornadoes, and floods. Whether man-made or natural, these threats can disrupt the delivery of financial services and inflict financial harm on consumers and businesses. The interconnected nature of the financial services industry further elevates the potential impact that threats can have on financial institutions. For example, many insured financial institutions rely on third-party service providers to provide critical banking services. An incident at a large service provider could have a cascading impact on a large number of financial institutions. If widespread, the impact could ultimately diminish public confidence and threaten the stability of the U.S. financial system. We conducted an evaluation to determine whether the FDIC had implemented effective processes to ensure that financial institutions receive actionable and relevant threat and vulnerability information. The FDIC had implemented processes for the sharing of threat and vulnerability information with financial institutions. For example, the FDIC established formal procedures to communicate cyber threat and vulnerability information. However, we reported that the FDIC could improve the effectiveness of its processes to ensure financial institutions receive actionable and relevant threat and vulnerability information. The report contained 10 recommendations to improve the FDIC's processes in order to ensure that financial institutions receive actionable and relevant threat and vulnerability information. Recommendation 10 is unimplemented.	10	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
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 Total	Recommendations Outstanding	Potential Cost Savings
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. Recommendations 2, 3, 9, and 11 are unimplemented.	17	4**	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-24-02 **Material Loss Review of Signature Bank of New York** October 23, 2023	On March 12, 2023, the New York State Department of Financial Services closed Signature Bank of New York (SBNY) and appointed the FDIC as receiver. On April 28, 2023, the FDIC estimated the loss to the Deposit Insurance Fund (DIF) to be approximately $2.4 billion. We engaged Cotton & Company Assurance and Advisory, LLC (Cotton) to perform a Material Loss Review. The objectives were to (1) determine why the bank's problems resulted in a material loss to the DIF, and (2) evaluate the FDIC's supervision of the bank, including the FDIC's implementation of the Prompt Corrective Action (PCA) requirements of section 38 of the Federal Deposit Insurance Act, and make recommendations for preventing any such loss in the future. SBNY's failure was caused by insufficient liquidity and contingency funding mechanisms, which impeded the bank's ability to withstand a run on deposits. In addition, SBNY management prioritized aggressive growth over the implementation of sound risk management practices needed to counterbalance the liquidity risk associated with concentrations in uninsured deposits. Cotton found that the FDIC: • Missed opportunities to downgrade SBNY's Management component rating and further escalate supervisory concerns; • Did not consistently perform supervisory activities in a timely manner and was repeatedly delayed in issuing supervisory products; • Appropriately downgraded SBNY's Liquidity component rating, but changing market conditions warrant the FDIC's review and potential revision of examination guidance; and • Determined that SBNY was well capitalized throughout each examination cycle prior to its failure based on defined capital measures. Cotton made six recommendations intended to improve the FDIC's supervision processes and its ability to apply effective forward-looking supervision in a changing banking environment. Recommendations 4 and 5 are unimplemented.	6	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	
EVAL-24-04 **The FDIC's Purchase and Deployment of the FDIC Acquisition Management System** January 25, 2024	The FDIC procures goods and services from contractors in support of its mission. In December 2020, the FDIC entered into an agreement to purchase an enterprise-wide acquisition management system. In June 2022, the FDIC went live with the system. However, the FDIC was unsuccessful in deploying the new system and abandoned it within 5 months. As a result, the FDIC incurred contract and staff labor-hour costs of nearly $10 million and had to revert to its legacy acquisition systems and manual reporting of some acquisition activities. We conducted an evaluation to review the primary factors that led to the FDIC's unsuccessful deployment of the FDIC Acquisition Management System and identify improvements for implementing future significant organizational changes. We determined that the FDIC's deployment of this new acquisition management system was unsuccessful because the FDIC did not employ an effective change management process as its policies and procedures did not require it. In addition, FDIC managers lacked awareness and training on when and how to implement a change management process. We made three recommendations for the FDIC to: (1) incorporate change management processes into the FDIC's policies and procedures and internal controls, (2) provide training on the change management process, and (3) implement a change management strategy and plan for the acquisition of a new acquisition management system. We also identified $9.9 million of funds to be put to better use that we reported in our Semiannual Report for the period ending March 30, 2024. Recommendation 2 is unimplemented.	3	1**	$9,900,000

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. Recommendations 2 and 4 are unimplemented.	8	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	
EVAL-24-05 **The FDIC's Sexual Harassment Prevention Program** July 31, 2024	Sexual harassment can have profound effects and serious consequences for the harassed individual, fellow colleagues, and the agency as a whole. It can undermine an agency's mission by creating a hostile work environment that lowers productivity and morale, affects the agency's reputation and credibility, and exposes the agency to judgments for monetary damages. Establishing an effective sexual harassment prevention program and addressing sexual harassment allegations in a prompt and effective manner can protect employees and the agency against the risk of such harm and costs. We conducted an evaluation to determine whether the FDIC implemented an effective sexual harassment prevention program to facilitate the reporting of sexual harassment allegations and address reported allegations in a prompt and effective manner. This was a follow-up to our 2020 evaluation, *Preventing and Addressing Sexual Harassment* (EVAL-20-006). The FDIC had not implemented an effective sexual harassment prevention program that facilitated the reporting of sexual harassment misconduct allegations and had not always investigated and addressed allegations of sexual harassment promptly and effectively. We found that FDIC leadership at several levels had not demonstrated sufficient commitment to, and accountability for, the Anti-Harassment Program (AHP); had not implemented an effective program structure or dedicated sufficient resources to the program; did not have an effective system for tracking, addressing, and documenting allegations; had not established adequate complaint procedures or an adequate AHP policy; and had not provided sufficient training to its supervisors and staff. This occurred because the FDIC had not sustained many program improvements that were initiated as a result of our prior 2020 evaluation. We made 24 recommendations to improve the FDIC's AHP and address the findings in our report. Recommendations 2, 3, 8,15, and 24 are unimplemented.	24	5**	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-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 7 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. Recommendations 1, 2, 5, 6, and 7 are unimplemented.	7	5**	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-24-06 **Conflicts of Interest in the Acquisition Process** September 23, 2024	Employees' adherence to principles of ethical conduct, to include not holding financial interests that conflict with duties and avoiding actions creating the appearance of violations of ethical standards, helps ensure public confidence and integrity of the Federal Government. Media reports in October and December 2022 regarding financial conflicts of interest of senior government officials included reference to three FDIC employees. Subsequently, the OIG received a Congressional request on February 28, 2023, to conduct a review of conflicts of interest at the FDIC and the effectiveness of existing rules and laws to prevent such conflicts. The objective of this evaluation was to determine the extent to which the FDIC has processes and procedures to identify, analyze, respond to, and monitor for conflicts of interest of FDIC employees engaged in the acquisition process. We found that the FDIC has processes and procedures to identify, analyze, respond to, and monitor for conflicts of interest in the acquisition process. However, improvements were needed to strengthen internal controls for conflicts of interest in the acquisition planning and approval processes. We also found that the FDIC could strengthen employee knowledge of ethics laws and regulations through specialized acquisition-related training. Additionally, we determined the FDIC could enhance its approach to confidential financial disclosure reviews by updating guidance and training. We made eight recommendations intended to improve the FDIC's internal controls related to conflicts of interest in the acquisition process and enhance its financial disclosure review program. Recommendations 1, 2, 3, 4, and 5 are unimplemented.	8	5**	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-24-07 **The FDIC's Information Security Program – 2024** September 25, 2024	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 KPMG to conduct this evaluation. The objective of the evaluation was to assess the effectiveness of the FDIC's information security program and practices. KPMG considered FISMA requirements, National Institute of Standards and Technology (NIST) security standards and guidelines, the NIST Cybersecurity Framework, Office of Management and Budget policy and guidance, FDIC policies and procedures, and Department of Homeland Security guidance and reporting requirements to plan and perform the work and to conclude on the objective. 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 2024 FISMA Metrics. While KPMG found that the FDIC established a number of information security program controls and practices that were consistent with FISMA requirements, the report describes security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. KPMG made three recommendations to address weaknesses identified during this evaluation. Recommendation 2 is unimplemented.	3	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-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, 3, 6, 7, 9, and 10 are unimplemented.	11	6	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
REV-25-01 **Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct – Part 1** December 18, 2024	An Agency's overall performance and reputation can be undermined by employee perceptions that an Agency's workplace culture does not demonstrate commitment to its core values. This can lead to long-term challenges in achieving the Agency's mission and retaining talent. In addition, if management does not hold personnel accountable and foster a safe environment where employees can report harassment and related misconduct without fear of retaliation, employees will mistrust the Agency's efforts. We conducted a review and found that a majority of FDIC employees who responded to a workplace culture survey stated they felt safe, valued, and respected and had generally positive views about their coworkers and immediate managers. However, employee views of FDIC management and leadership with respect to harassment and related misconduct were less favorable. More than one-third of respondents reported that they had either experienced or personally witnessed harassment. Additionally, our review of cases and settlement agreements supported some of the employee perceptions, specifically that some FDIC managers had not protected victims of harassment and retaliated against those who filed a complaint. These conditions occurred because FDIC leadership did not consistently implement the Agency's policies and stated core values, specifically, fairness, accountability, and integrity. The FDIC did not consistently maintain documentation related to disciplinary actions resulting from complaints of harassment and related misconduct. Additionally, the FDIC did not document its decision-making process for these disciplinary actions. This occurred because the FDIC did not have a centralized system to track all harassment and related misconduct complaints and the associated records, efforts, and actions from inception to resolution. Also, the FDIC did not have clear policy, standards, and procedures for documenting the process that it followed to make disciplinary decisions. FDIC executives had varying levels of knowledge regarding harassment and related misconduct complaints across the FDIC. Also, FDIC policies did not require allegations of harassment or related misconduct involving FDIC employees to be reported to the appropriate FDIC stakeholders. The report contained six recommendations regarding the FDIC's efforts to improve its workplace culture. Recommendation 1 is unimplemented.	6	1	N/A

Table II: Audit and Evaluation Reports				
Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	Title*	Total	Unsupported	
REV-25-02 June 2, 2025	*Failed Bank Review – Pulaski Savings Bank, Chicago, IL*			
AUD-25-01 June 10, 2025	*The FDIC's Procurement of Resolution and Receivership Services*			
MEMO-25-02 June 24, 2025	*FDIC Succession Management and Employee Retention Efforts*			
MEMO-25-03 August 12, 2025	*Significant Service Provider Examination Program*			
AUD-25-02 September 25, 2025	*Audit of Security Controls for a Cloud Platform and Application*			
EVAL-25-03 September 26, 2025	*The FDIC's Information Security Program - 2025*			
Totals for the Period		**$0**	**$0**	**$0**

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

On July 30, the OIG issued Part 2 of its *Special Inquiry on the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct*. This report was a follow-on to Part 1 of our report, issued in December 2024.

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	58
Number of Persons Referred to the Department of Justice for Criminal Prosecution	63
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	0
Number of Indictments and Criminal Informations	60

Note: Description of the metrics used for the above information: Reports issued reflects 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 this reporting period, we completed an administrative investigation and reported our results in Part 2 of our *Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct*. As noted earlier in this semiannual report, that investigation substantiated allegations of harassment and related misconduct against five senior FDIC officials, none of whom remained employed by the FDIC at the time we issued our report.

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 that were closed and not disclosed to the public and no investigations involving senior government employees that were closed and not disclosed to the public.

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, 2025 through September 30, 2025 (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, Section 38(k) of 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 completed our review of the failure of Pulaski Savings Bank, which failed on January 17, 2025, causing an estimated loss of $28.4 million to the DIF at that time. That review determined that circumstances existed that warranted an In-Depth Review. The In-Depth Review was in progress as of September 30, 2025. We plan to issue the final report in February.

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.

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 the 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.

Inspection and Evaluation Peer Reviews

The Tennessee Valley Authority OIG conducted a peer review of the FDIC OIG's evaluation function and issued its report on the peer review on June 28, 2022. This required external peer review was conducted in accordance with CIGIE Inspection and Evaluation Committee guidance as contained in the *CIGIE Guide for Conducting External Peer Reviews of Inspection and Evaluation Organizations of Federal Offices of Inspector General*, December 2020.

The External Peer Review Team assessed the extent to which the FDIC OIG complied with standards from CIGIE's Quality Standards for Inspection and Evaluation (Blue Book), January 2012. Specifically, the Review Team assessed quality control, planning, data collection and analysis, evidence, records maintenance, reporting, and follow-up. The assessment included a review of the FDIC OIG's internal policies and procedures implementing the seven covered Blue Book standards. It also included a review of selected inspection and evaluation reports issued between April 1, 2021, and March 31, 2022, to determine whether the reports complied with the covered Blue Book standards and FDIC OIG's internal policies and procedures.

The Review Team determined that the FDIC OIG's policies and procedures generally were consistent with the seven Blue Book standards addressed in the external peer review. Additionally, all three reports reviewed generally complied with the covered Blue Book standards and the FDIC OIG's associated internal policies and procedures. https://www.fdicoig.gov/reports-publications/peer-reviews/external-peer-review-report-federal-deposit-insurance-corporation.

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.

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 Offices of Inspector 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.

FDIC OIG Qualitative Assessment Review of Another OIG

During the 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 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, MO; Washington, District of Columbia; and Philadelphia, PA. 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.

Congratulations

We are proud of the members of the FDIC OIG who were recognized by the IG Community for their contributions and excellent work conducted during the past year.

The CIGIE Monetary Impact Working Group is the recipient of the prestigious Barry R. Snyder Joint Award.

Members from our Office who served on the Working Group were Luke Itnyre, Terry Gibson, and Stacey Luck. They took a lead role and joined nearly 50 other volunteers from 21 different OIGs who formed the Working Group.

The award is given: ***"For demonstrating outstanding collaboration across the OIG community and developing a significant resource to aid all OIGs in the consideration, estimation, and reporting of monetary impact identified from their audit, inspection, and evaluation efforts."***

Additionally, the team responsible for our report on the ***Federal Deposit Insurance Corporation's Sexual Harassment Prevention Program*** is the recipient of an Award for Excellence in Evaluations.

This award is given ***"In recognition of promoting significant improvements in the FDIC's sexual harassment program, resulting in 24 recommendations to facilitate reporting and promptly and appropriately addressing sexual harassment allegations."***

Team members were as follows: Lisa Conner, Melissa Mulhollen, Wendy Alvarado, Ebonyee Brincefield, Philip Hodge, Stacey Luck, Sharon Tushin, Jeffrey Cheung, Jane Kim, and Shakhan Simmons.

And finally, the investigative team responsible for the **TD Bank Investigation** is the recipient of an Award for Excellence in Investigations.

This award is given ***"In recognition of excellence in an investigation of Bank Secrecy Act and Money Laundering Conspiracy Violations."***

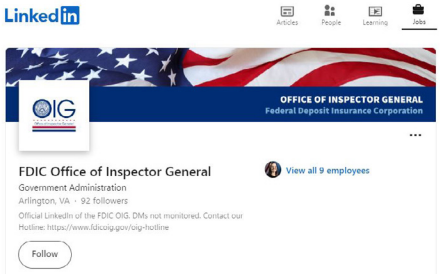
Investigative team from the FDIC OIG: Peter Chartier, Special Agent and Judith Phillips, Financial Analyst.

Others on the team included: Partners from the USAO in New Jersey; DOJ's Money Laundering and Asset Recovery Section, Bank Integrity Unit; Internal Revenue Service – Criminal Investigation; Morristown Police Department; U.S. Drug Enforcement Administration; and U.S. Department of Homeland Security – Homeland Security Investigations.

★**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-028-2025