FDIC
Office of Inspector General

Semiannual Report to the Congress

October 1, 2025 – March 31, 2026

Integrity
Independence
Objectivity
Transparency
Excellence

Office of Inspector General

250TH ANNIVERSARY OF AMERICA
1776–2026

Under the Inspector General Act of 1978, as amended, the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General 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 5,137 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data (December 31, 2025), the FDIC insured $10.82 trillion in domestic deposits in 4,336 institutions, of which the FDIC supervised 2,738. The Deposit Insurance Fund balance totaled $153.9 billion. Active receiverships totaled 44, with assets in liquidation of about $24.3 billion.

Semiannual Report to the Congress

October 1, 2025 – March 31, 2026

Office of Inspector General

Federal Deposit Insurance Corporation

Our Mission

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

Our Vision

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

Values

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

Inspector General's Statement

I am pleased to submit this report highlighting the work of the Federal Deposit Insurance Corporation Office of Inspector General (OIG) for the period October 1, 2025 through March 31, 2026.

Although the reporting period began with a government shutdown, we continued critical oversight work, including activities carried out by our law enforcement Special Agents and other essential personnel who were excepted from furlough. As full operations resumed in mid-November, we continued our work in earnest and can report significant results from the past 6 months.

Our Office of Audits issued a report that addressed improvements needed to determine cost benefits and organizational risks associated with the FDIC's Student Residence Center, a facility that provides lodging primarily for FDIC employees and Federal financial regulatory agency employees traveling to the Washington, D.C. metropolitan area to participate in courses and seminars offered by the FDIC and other training groups. A second report identified control weaknesses in the FDIC's contracting for infrastructure support services where we identified $4.6 million in questioned costs and $2 million in funds to be put to better use. The third report issued during the period was an In-Depth Review of a failed financial institution where we noted that the FDIC should consistently consider the presence and impact of dominant officials as part of the examination process and designate officials as such when appropriate and in accordance with FDIC procedures and guidance. We made a total of 12 recommendations to FDIC management in these reports.

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 21 indictments/informations, 38 convictions, 38 arrests, and more than $152 million in fines, restitution ordered, and other monetary recoveries. In this report we present the results of cases involving harmful financial crimes perpetrated by foreign nationals, business executives, an attorney, senior bank officials, former bank tellers, and a loan broker, among others.

We issued our Top Management and Performance Challenges report in March, an important project to highlight the FDIC's challenges and also to help focus the OIG's work going forward. Our document identifies eight challenges and provides information on what actions the FDIC has taken to address them. We noted this year that overall, the long-term success of the FDIC depends on a sufficient cadre of skilled personnel, a safe and accountable workplace, effective governance and interdivisional coordination, resolution and receivership readiness, effective supervision, adherence to established internal controls, strong information security, and identification of fraud risks within the banking industry. Maintaining public confidence and the FDIC's role in ensuring financial and banking system stability remain essential priorities.

Given the preponderance of fraud schemes that threaten consumers and banks, we seek to prevent those from happening via investigations, social media postings, pursuit of Hotline inquiries, website notifications, internal and external outreach, and support of other agency efforts. Several of these schemes are explained in this report, and we also cover a number of collaborations and outreach activities that we have undertaken to deter such schemes.

We have continued to promote productive relationships with stakeholders—not only internal to the FDIC, but also those in the IG community, law enforcement partners, Congress, the Government Accountability Office, and the public—making concerted efforts to apprise them of the results and impact of our work.

Similarly during the reporting period, we have carefully considered our resource needs to carry out the OIG mission, as conveyed in our Congressional Budget Justification for fiscal year 2027 and in discussions with the Office of Management and Budget and Congressional appropriators. We also continue advancing the use and value of data analytics and exploring best means of leveraging artificial intelligence.

Finally, and importantly, we revised the FDIC OIG's strategic goals and related initiatives in a new Strategic Plan. 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.

In closing, I note that Acting Chairman Travis J. Hill was confirmed on December 18, 2025 as the FDIC's 23rd Chairman. We appreciate his support and interest in our work and that of other FDIC Board Members and members of FDIC staff and management.

As we look to the future and the celebration of America's 250th Anniversary, we are honored to be among the Nation's public servants and proudly reaffirm our commitment to independent oversight at the FDIC.

Jennifer L. Fain
Inspector General
April 2025

Table of Contents

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

Acronyms and Abbreviations

AI	Artificial Intelligence
AML	Anti-Money Laundering
BOV	Bank of the Valley
CFO	Chief Financial Officer
CFT	Countering Financing of Terrorism
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
DIF	Deposit Insurance Fund
DOJ	Department of Justice
ECU	Electronic Crimes Unit
FBA	Federal Banking Agency
FBI	Federal Bureau of Investigation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act
FRB	Board of Governors of the Federal Reserve System
FSOC	Financial Stability Oversight Council
HSI	Homeland Security Investigations
IG	Inspector General
ISS	Infrastructure Support Services
IT	Information Technology
JPMC	JP Morgan Chase
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
ORMIC	Office of Risk Management and Internal Controls
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
RSP	Regional Service Provider
SBA	Small Business Administration
SRC	Student Residence Center
SSP	Significant Service Provider
USAO	United States Attorney's Office
USSS	United States Secret Service

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 (October 1, 2025 – March 31, 2026)	
Audit, Evaluation, and Other Products Issued	**4**
Recommendations (with $4.6 million in questioned costs and $2 million in funds put to better use)	**12**
Investigations Opened	**55**
Investigations Closed	**93**
Judicial Actions:	
Indictments/Informations	**21**
Convictions	**38**
Arrests	**38**
OIG Investigations Resulted in:	
Special Assessments	**$11,525.00**
Fines	**$249,250.00**
Restitution	**$130,703,211.32**
Asset Forfeitures	**$13,656,135.97**
Criminal Penalty	**N/A**
Civil Penalty	**$7,770,595.25**
Total	**$152,390,717.54**
Referrals to the Department of Justice	**23**
Investigative Reports Referred to FDIC Management	**9**
Responses to Requests Under the Freedom of Information/Privacy Act	**8**
Subpoenas Issued	**12**

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 three reports. One addressed improvements needed to determine cost benefits and organizational risks associated with the FDIC's Student Residence Center. A second report identified control weaknesses in the FDIC's contracting for infrastructure support services where we identified $4.6 million in questioned costs and $2 million in funds to be put to better use. The third report was an In-Depth Review of a failed financial institution. We made a total of 12 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. We issued our failed bank review, that of Pulaski Savings Bank on June 2, 2025. This bank failed on January 17, 2025, with losses to the DIF estimated at $28.4 million at the time. During the current reporting period, we completed and issued an In-Depth Review related to that failure.

Results of the audits, evaluations, and other reviews completed during the reporting period are summarized below. Results of a peer review of the Evaluation function of our Office of Audits are presented as well, as conducted by the Department of Education OIG. We also include a summary of the issues we highlighted in our Top Management and Performance Challenges report that we issued in March 2026. These challenges are largely driven by our audit and evaluation work throughout the year. Notably, however, the challenge related to identifying and combating fraud and misrepresentation derives principally from our investigations. A listing of ongoing assignments, prompted in part 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 related to the security of OIG emails. We also present information on recommendations unimplemented for more than one year.

Audits, Evaluations, and Other Reviews

Audit of The FDIC's Student Residence Center

In January 2024, the FDIC OIG received a Congressional request to perform work related to the Student Residence Center (SRC). Specifically, the Congressional request stated that, in light of a recent media report, the FDIC OIG should "determine whether [the SRC] still makes financial sense, and that the FDIC is taking meaningful steps to police the behavior of its workforce if they are to continue staying at the [SRC]." The FDIC OIG responded to this request in February 2024 noting that the FDIC OIG planned to review the FDIC's ownership and management of real estate assets, which included the SRC located on the FDIC's Virginia Square campus in Arlington, Virginia.

The objective of this audit was to assess the FDIC's efforts to determine the cost benefits of, and organizational risks associated with, operating the SRC. To address the objective, we reviewed relevant FDIC policies, procedures, and guidance. In addition, we reviewed Federal laws and regulations, as well as best practices related to real property management.

We found the FDIC has not determined the cost benefits of, or organizational risks associated with, operating the SRC. Specifically, the FDIC could not provide documentation that SRC cost benefits have been assessed since 1986 or that organizational risks specifically related to operating the SRC have been formally identified, assessed, or addressed. This was due, in part, to the FDIC's lack of (1) asset management processes and procedures; (2) centralized, accessible SRC-related financial and non-financial data; and (3) performance goals and objectives for SRC operations.

As a result, the FDIC cannot readily determine whether the SRC is achieving the best value for the agency. Additionally, without defined processes for capturing and maintaining relevant, quality information, the FDIC is limited in its ability to efficiently monitor the effectiveness of, and make informed decisions about, the current and future use and operations of the SRC.

We made four recommendations intended to improve the FDIC's efforts to determine SRC cost benefits and to identify organizational risks associated with operating the SRC. Implementing data-driven decision making related to SRC current and future operations would help ensure that the FDIC optimizes and effectively manages this real property asset. Further, establishing a risk assessment process for SRC operations would enhance the FDIC's ability to proactively identify, analyze, and manage risks, align efforts across FDIC Divisions and Offices, and achieve goals and objectives. The FDIC concurred with all four recommendations and plans to complete all corrective actions by September 30, 2026.

Oversight of the Infrastructure Support Services Contract

The FDIC relies on contractor support to accomplish its mission. Therefore, it is important that the FDIC ensure effective contract oversight and compliance with its acquisition policies and that contractors deliver goods or services according to the terms of the contract.

In January 2021, the FDIC awarded a $300 million Basic Ordering Agreement to provide day-to-day information technology operational support for its infrastructure facilities, hardware, software, and systems. The services provided under the agreement are a critical component of the FDIC's capability to sustain normal operations and respond to bank failures in a timely and effective manner.

The objective of our audit was to determine whether the FDIC provided effective oversight of the Infrastructure Support Services (ISS) contract to ensure compliance with service level metrics, invoice review and approval procedures, and data protection and security controls.

While the FDIC made significant progress to address the weaknesses identified during our audit, we determined the FDIC did not provide effective oversight to ensure key contract personnel and the Contractor complied with internal policies and procedures or the ISS contract terms and conditions. Specifically, we found that the FDIC did not always:

- Monitor contractor performance against agreed-upon metrics nor enforce the requirement for the Contractor to provide the supporting data needed to verify compliance with service level metrics and to determine the accuracy of the service level credits due to the FDIC.
- Review and verify the accuracy of invoice charges and service level credits for Critical Service Level defaults nor consistently retain supporting data for invoices.
- Verify that all contractors completed training prior to being granted privileged access to the FDIC's network and systems and ensure the Contractor reported a data leakage incident in accordance with internal policy.

We made eight recommendations intended to improve the FDIC's oversight of ISS contracts. We identified $2 million in funds to be put to better use for service level credits due to the FDIC and $4.6 million in questioned costs because the FDIC did not retain the data to support those charges on the ISS contract invoices. The FDIC concurred with the eight recommendations and plans to complete all corrective actions by December 31, 2026.

In-Depth Review of Pulaski Savings Bank

On January 17, 2025, the Illinois Department of Financial and Professional Regulation, Division of Banking, took possession and control of Pulaski Savings Bank and appointed the FDIC as the receiver. Pulaski Savings Bank was a state-chartered mutual savings bank that first became FDIC insured on August 9, 1989. Pulaski Savings Bank was a certified Community Development Financial Institution primarily focused on single family residential loans that operated from a single branch office location in Chicago, IL. The bank's funding largely came from local, core deposits. According to the FDIC, the estimated loss to the DIF from Pulaski Savings Bank's failure was $28,449,000 or 62 percent of the bank's $45,919,248 in total assets.

We conducted an in-depth review to (1) determine the cause(s) of Pulaski Savings Bank's failure and resulting loss to the DIF and (2) evaluate the FDIC's supervision of the bank, including the FDIC's implementation of the Prompt Corrective Action requirements of Section 38 of the FDI Act.

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

Consistent with Prompt Corrective Action provisions, the FDIC notified Pulaski Savings Bank that it was "critically undercapitalized" and required it to take actions necessary to increase capital. Ultimately, the Illinois Department of Financial and Professional Regulation determined that the bank was impaired, took possession, and appointed the FDIC as receiver.

The FDIC conducted its examinations in a timely manner and identified weaknesses in the bank's management since 2017. While the FDIC did not formally designate a dominant official at Pulaski Savings Bank, its supervisory actions sought to mitigate weaknesses in the bank's management including certain key person risks in the most recent examination cycles. For that reason, we did not make a formal recommendation in this report. However, we encouraged the Division of Risk Management Supervision to consistently consider the presence and impact of dominant officials as part of the examination process and designate officials as such when appropriate and in accordance with FDIC procedures and guidance. The FDIC had no comments on this report.

Peer Review of the FDIC OIG Evaluation Function

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

In the Department of Education OIG's opinion, the system of quality control for the FDIC OIG in effect for the year ended September 30, 2025, had been suitably designed and complied with to provide the FDIC OIG with reasonable assurance of performing and reporting in conformity with the Blue Book. Inspection and Evaluation organizations can receive a rating of pass, pass with deficiencies, or fail. The FDIC OIG received an External Peer Review rating of pass. (See also Appendix 3.)

Top Management and Performance Challenges

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

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

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

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

1. Optimizing the FDIC Workforce.

- Human Capital Risks and Workforce Challenges.

2. Maintaining a Safe and Accountable Workplace Culture.

3. Strengthening Organizational Governance.

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

4. Sustaining Readiness to Execute Resolution and Receivership Responsibilities.

- Improving Readiness for Large Regional Bank Failures.
- Procurement of Resolution and Receivership Services.

5. Ensuring Effective Supervision.

- Escalating Supervisory Actions.
- Supervision of Third-Party Service Providers.
- Reforming the FDIC's Supervisory Framework.

6. Improving Contract Management.

- Adhering to Contracting Requirements and Internal Controls.
- Improving Procurement of Services.

7. Enhancing Cyber and Data Security.

- Implementing the Use of Artificial Intelligence.

8. Identifying and Combating External Fraud and Misrepresentation.

- Insider Fraud.
- Scams Targeting Unwitting Customers.
- Addressing Misuse of the FDIC Name and Logo.

Ongoing 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:

- **Cyber Incident Detection and Response:** Our objective is to determine to what extent the FDIC has implemented processes to detect, respond, and actively defend against cyber threats.
- **Valuation Process for Large Regional Bank Resolutions:** Our objective is to determine whether the FDIC adhered to established policies and procedures for the valuation function in response to the failures of Silicon Valley Bank, Signature Bank of New York, and First Republic Bank.
- **FDIC Examinations of Banks' Anti-Money Laundering (AML)/Countering Financing of Terrorism (CFT) and Sanctions Compliance:** The objective is to determine whether (1) the FDIC effectively conducted AML/CFT examination scoping and planning activities, and to what extent planning decisions align with identified risks, and (2) the examiners have the necessary training and skills to evaluate AML/CFT and sanctions compliance.

- **Failed Bank Review of Metropolitan Capital Bank & Trust:** The objective is to determine (a) the grounds identified by the state banking agency for appointing the FDIC as receiver and (b) if the circumstances surrounding the failure of the bank warrant an in-depth review of the loss.
- **FDIC's Franchise Marketing Process for Large Regional Bank Resolutions:** The objective is to determine the extent to which the FDIC adhered to established policies and procedures consistent with FDI Act requirements for the Franchise Marketing function in response to the failures of Silicon Valley Bank, Signature Bank, and First Republic Bank.
- **Council of Inspectors General on Financial Oversight (CIGFO) - Audit of FSOC's Designation of Nonbank Financial Companies:** The objectives of this audit are to assess (1) the sufficiency of the new guidance to effectively respond to financial stability threats as authorized under Section 113 of Dodd-Frank; (2) the extent that the Financial Stability Oversight Council (FSOC) Members were engaged in the development of the new guidance considering such factors as lessons learned and any identified barriers from earlier guidance; and (3) the impact on the nonbank designation process as a result of the new guidance compared to prior guidance and processes.

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 the Federal Information Security Modernization Act (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 the project. We reported in our previous semiannual report that the first phase had been mostly implemented, while the second phase was still incomplete.

We note, however, that the OIG has worked with the CIO to establish a process and procedure that mitigates the security and privacy risks that existed under the FDIC's process of handling OIG email. We will continue to work with the CIO to ensure that all risks are appropriately mitigated.

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 16 recommendations that the OIG made to management that remained open for more than one year. We routinely coordinate with the FDIC's Office of Risk Management and Internal Controls to determine whether the OIG's recommended and agreed-upon corrective actions have been completed. In reviewing the status of these open recommendations, the OIG believes that 5 of the 16 should have been closed in a timelier manner. Four of these recommendations were identified as concerns in the previous semiannual report.

Additionally, we have recently identified one of the recommendations in our report on *FDIC Readiness to Resolve Large Regional Banks* (EVAL-25-02) as unimplemented for over one year and of concern to us. A listing of these reports and associated recommendations follows:

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)** (Note: The OIG was reviewing a corrective action closure form for this recommendation as of March 31, 2026.)

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. **(Repeat)**

(Note: The FDIC has submitted information on parts a, b, and c; however, part d is outstanding, with a due date of December 31, 2026.)

REV-24-01
Review of the 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)**

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

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

The above discussion reflects the status of the recommendations listed as of March 31, 2026. The FDIC may have taken action to implement these recommendations subsequent to that date. Our website presents the most current status of unimplemented recommendations at Unimplemented Recommendations | Federal Deposit Insurance Corporation OIG.

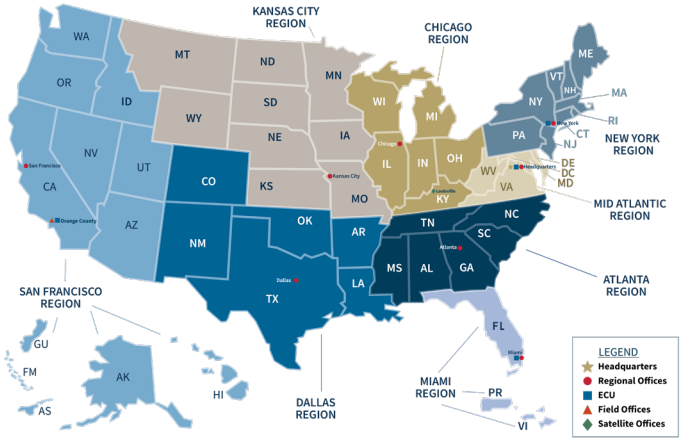
Investigations

As reflected in our 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 of Investigations (OI) plays a key role in investigating sophisticated schemes of bank fraud, embezzlement, money laundering, cybercrime, and currency exchange rate manipulation—fraudulent activities affecting FDIC-supervised or insured institutions. Whether it is bank executives who have caused the failures of banks, or criminal organizations stealing from Government-guaranteed loan programs—these cases often involve bank directors and officers, Chief Executive Officers, attorneys, real-estate insiders, bank tellers, financial professionals, crypto-firms and exchanges, Financial Technology (FinTech) companies, and international financiers.

FDIC OIG investigations during the reporting period resulted in 21 indictments/informations, 38 convictions, 47 arrests, and more than $152 million in fines, restitution ordered, and other monetary recoveries. We opened 55 cases and closed 93 during the reporting period. We referred 9 investigative reports to FDIC management for action.

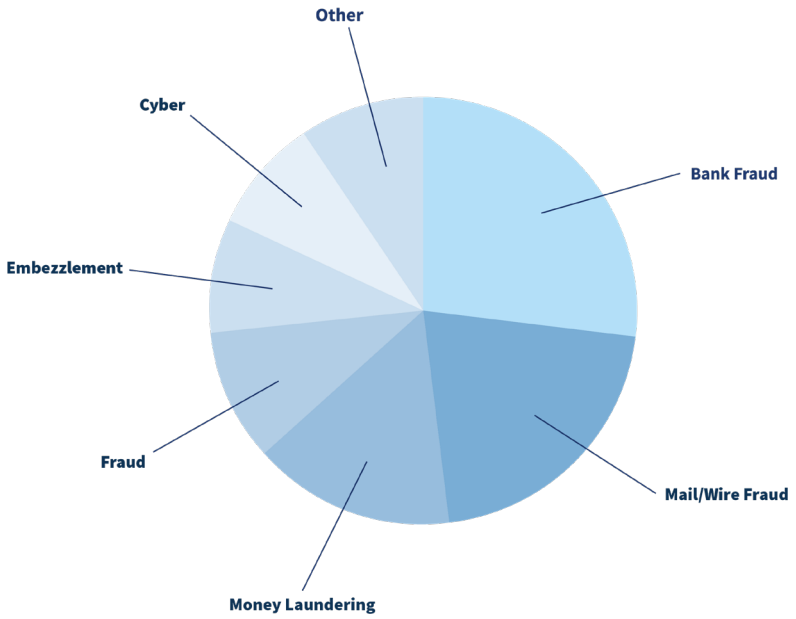


OIG Regional Map

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 Identity Theft, Conspiracy, CARES Act Fraud, Abuse of Position, Elderly Fraud, Bank Secrecy Act Violations, Employee Integrity, Bribery, Ethics, Misuse of Government Property, Misappropriation of Funds, Misrepresentation of FDIC, False Personation, Kickbacks, False Claims, Contract Fraud, False FDIC Affiliation, Network Intrusion, Larceny/Theft, Lack of Candor, Extortion, Assault, and Obstruction of Justice.

Management Advisory on Risks of Applications Installed on FDIC Mobile Devices

The OIG issued a management advisory memorandum to the FDIC Chairman in February 2026, based on OI forensic analysis. The memorandum advised that user-installed mobile applications pose risk to the FDIC's data and information systems. Such applications may inadvertently expose sensitive information, introduce malware, or facilitate data leakage, particularly if connected to non-FDIC accounts. The intent of the memorandum was to assist the Chairman in his consideration of actions to mitigate potential risks posed by employee-installed applications on FDIC mobile devices. In response, the FDIC implemented certain policy and technology changes intended to address these risks.

Electronic Crimes Unit

Our Electronic Crimes Unit (ECU) is an important component within our Office of Investigations. 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 program and operations. Investigative priorities include intrusions, cryptocurrency, impersonation, ransomware, Darkweb, business email compromises, and account takeovers targeting banks and financial institutions. The ECU continues to focus on early-warning notifications to enable prompt and coordinated law enforcement responses to adversarial cyberattacks.

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.)

FDIC OIG Special Agents share information proactively to raise awareness of harmful scams.

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 8 charging actions (indictments, informations, and superseding indictments and informations), 7 arrests, and 11 convictions involving fraud in the CARES Act-related programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases totaled $10,047,744.22.

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 continued to migrate 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 coordinated a joint session at the 2026 FDIC Data Summit with the Federal Trade Commission on fraudsters impersonating FDIC officials. Our ultimate goal is to proactively identify tips and leads for further investigations and high-impact cases, detect high-risk areas at the FDIC for possible audit or evaluation coverage, and recognize emerging threats to the banking sector.

Our data analytics efforts with respect to our 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, Federal Trade Commission, and others. These efforts have resulted in expanded access to investigative data tools and capabilities for OIG investigations; identification of potential data sets relevant to OIG efforts; new opportunities for collaboration with external partners; identification of additional data analytics pilot projects; and information sharing agreements to help inform overall strategic planning within the OIG.

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 a 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 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.

Nicaraguan National Extradited from Spain for International Extortion and Wire Fraud Scheme Sentenced

On March 19, 2026, Ernesto Ortega Padgett (Ortega), a Nicaraguan national who was deported from the United States in early 2020, was sentenced to 15 years' imprisonment, and 3 years of supervised release for his role in a $65 million Account Takeover (ATO) which he orchestrated from Panama, as well as Spain. The ATO involved over 200 victims and at least six FDIC-insured institutions. Previously on November 5, 2025, he had pled guilty for his role in the scheme. Ortega was charged on February 2, 2023, via a sealed 27 count indictment which included 18 U.S.C. § 1343 - Wire Fraud, 18 U.S.C. § 1349 - Conspiracy to Commit Wire Fraud, 18 U.S.C. § 1951(a) - Conspiracy to Commit Hobbs Act Extortion, and 18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering. He was extradited from Madrid, Spain, to Miami, Florida, on June 13, 2025. Ortega was paroled into the United States by the Department of Homeland Security, Immigration and Customs Enforcement, and was subsequently officially arrested. The indictment was unsealed on June 16, 2025. Ortega pled guilty to one count of Conspiracy to Commit Wire Fraud, and one count of Conspiracy to Transport Stolen Property; all other charges were dismissed. A restitution hearing will be scheduled.

In early 2020, Ortega began conducting a sophisticated bank Account Takeover operation that would span nearly 4 years, and targeted businesses across the United States. He gained access to the victim accounts by posing as a representative of the victims' financial institutions and using an intricate combination of technology combined with social engineering.

Ortega used various methods of information harvesting to obtain the phone numbers and email addresses of executives at various companies and used that information to conduct a multi-faceted spear phishing attack on those executives by posing as a member of their bank's cybersecurity fraud prevention team. This attack was typically initiated with a text message appearing to be from the victim's bank, attempting to verify a specific fictitious transaction. These text messages were followed shortly thereafter with phone calls and targeted emails. Ortega employed software programs to "spoof" his phone number to appear as if it originated from the victim's respective bank.

Once inside the victim accounts, Ortega contacted his money mule recruiters in Miami, who provided Ortega with bank accounts to receive the fraudulent wire transfers. Ortega initiated multiple wire transfers to drain the victims' accounts and transfer the funds to an array of money mule accounts in both the United States and Spain.

Among the mule accounts Ortega utilized in the United States, some belonged to his girlfriend, Daphne Gonzalez, as well as Daphne's parents, Angel Gonzalez and Amarilis Claro, all three of whom were charged, pled guilty, and were sentenced. In addition, Ortega employed a team of money mule recruiters in South Florida who recruited mostly young, college-aged, individuals to open bank accounts specifically for the purpose of receiving victim funds wired by Ortega. Ortega's money mule recruiting team in South Florida consisted primarily of Collins Oleh and Nevordo Gordon, who were also charged, pled guilty, and were sentenced.

Ortega also employed a team of money mules in Spain to open bank accounts for the specific purpose of receiving victim funds that he wired to them. The mules in Spain were often vagrants who were given nominal amounts of money in return for opening the mule accounts. All account information, including online login information, for the mule accounts was forwarded to Ortega, for him to oversee and control the flow of victim funds. Once the victim funds were received in the mule accounts, Ortega would direct his proxies to physically transport the money mules to their respective banks to facilitate the withdrawal of the fraudulent funds and turn them over to the recruiters, who would, in turn, return the funds back to Ortega in Spain, often in the form of cryptocurrency.

The FDIC OIG ECU worked closely with the Spanish National Police to coordinate Ortega's apprehension and seizure of electronic evidence. In addition, the ECU liaised with Spanish prosecutors to expedite Ortega's extradition to the United States to face prosecution here.

Source: This investigation was initiated based on a referral from the United States Secret Service (USSS).
Responsible Agencies: This is a joint investigation by the FDIC OIG and USSS. The matter is being prosecuted by the USAO for the Southern District of Florida.

"Frank's" Former Chief Growth Officer Sentenced

On November 5, 2025, in the Southern District of New York, Olivier Amar was sentenced to 68 months in prison, 3 years of supervised release, and ordered to pay $168,531,713 in restitution and $5,690,70.31 in forfeiture. Charlie Javice and Amar were 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.

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. JPMC ultimately purchased 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, they discovered that Javice and Amar had fabricated a data set of users during the due diligence process. Also 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.

Source: USAO, 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.

Former Credit Union Manager Pleads Guilty to Embezzlement

On March 23, 2026, Nedra Young pled guilty in the Western District of Kentucky to three counts of bank fraud. Young was previously charged via information with three counts of bank fraud on March 6, 2026. Young, a former manager at LouVAH Federal Credit Union in Louisville, Kentucky, used her position at LouVAH to embezzle approximately $163,000 from client accounts held at Republic Bank & Trust Company, an FDIC-regulated institution.

The investigation determined that LouVAH, a credit union established to service employees of the Louisville Veterans Affairs Medical Center, is a small (single branch) financial institution that uses Republic for deposit and clearing operations. All client funds are deposited with Republic, and LouVAH serves as a loan originator, underwriter, and provider of specific insurance products. Young used her position of trust to defraud clients of LouVAH and Republic. Specifically, she issued multiple proceeds checks at the closing of LouVAH loans and led clients to believe only a single proceeds check was issued. Young deposited the illicit checks into the LouVAH operating account at Republic. Young then laundered the illicit proceeds through Republic and used them to her benefit or the benefit of her family members. Additionally, Young used her position and access to accounts at Republic to make fraudulent withdrawals directly from client accounts without the knowledge or consent of the account holders.

Source: This investigation was based on a referral from the FBI.
Responsible Agencies: This investigation was conducted by the FDIC OIG. The matter is being prosecuted by the USAO for the Western District of Kentucky.

Former Wells Fargo Bank Teller Sentenced

On February 24, 2026, Cedrina Grant, a former bank teller at Wells Fargo, was sentenced to one day time served, 3 years of supervised release, and ordered to pay restitution of $59,900 for her role in a bank fraud conspiracy. Previously on April 25, 2025, Grant was indicted on one count of conspiracy to commit bank fraud, three counts of bank fraud and one count of structuring. On July 28, 2025, she pled guilty to one count of conspiracy to commit bank fraud.

On January 16, 2025, co-conspirator Ethan Brown was sentenced to 34 months of incarceration and ordered to pay restitution of $973,692 to Wells Fargo. Brown was indicted along with the other co-conspirators, Hunter Hudson, Rueben Brown, Brandon Gage, Kerry Hawthorne, Destinie James, Joey Payne, and Keenan Watson, for their respective roles in the conspiracy.

From 2021 through 2023, while employed as a teller at Wells Fargo, Brown utilized his position and authority to override bank systems to allow ill-gotten funds to be deposited and subsequently withdrawn by his co-conspirators. The co-conspirators stole checks from the mail and created counterfeit checks, subsequently deposited the altered and counterfeit checks, and ultimately withdrew the funds. The stolen checks were altered by the co-conspirators to change the payee, and counterfeit checks were created using the account information from the stolen checks. The checks were then deposited into accounts of uninvolved third parties before being withdrawn by the co-conspirators. Grant participated in the conspiracy by using her access as a Wells Fargo teller to assist co-conspirators who were withdrawing the fraudulent funds. Specifically, Grant conducted structured transactions and aided and assisted other conspirators with withdrawals of funds from the previously deposited fraudulent checks.

Source: USAO, Middle District of Alabama. Responsible Agencies: This is a joint investigation by the FDIC OIG, U.S. Postal Inspection Service, U.S. Postal Service OIG, and the FBI. The matter is being prosecuted by the USAO for the Middle District of Alabama.

Attorney Sentenced in DC Solar Case

On March 9, 2026, Ari J. Lauer was sentenced to 11 years and 5 months in prison for his role in the biggest criminal fraud scheme in the history of the Eastern District of California. Lauer previously pled guilty on October 14, 2025, to all 23 counts from an October 2023 indictment that included conspiracy to commit bank and wire fraud, bank fraud, and wire fraud affecting a financial institution. Lauer was indicted on October 5, 2023, for his role in an estimated $912 million Ponzi scheme involving California solar power supply company DC Solar.

From approximately 2009 to early 2019, Lauer, an attorney licensed to practice law in California, served as outside counsel for DC Solar. Lauer provided legal and business advice concerning DC Solar's operations. According to court documents, between 2011 and 2018, DC Solar manufactured mobile solar generators that were mounted on trailers. The company touted the versatility and environmental sustainability of the generators and claimed they were used to provide emergency power to cellphone towers, as well as lighting at sporting and other events. A significant incentive for investors were generous Federal tax credits due to the solar nature of the generators. As discussed in previous semiannual reports that we have issued, Jeff Carpoff, Paulette Carpoff, and their co-conspirators solicited investors to invest in the generators in large multimillion-dollar transactions using a variety of fraudulent techniques.

A key part of the fraud was that investors would never actually take possession of the generators. Instead, DC Solar typically leased the generators back from the investors and claimed to sublease them to third parties to generate revenue. In reality, there was very little third-party rental demand for the generators. However, when Lauer and the other co-conspirators learned this, they continued to falsely represent to investors that the rental market for the generators was robust.

Between March 2011 and December 2018, investors directly provided approximately $759 million to DC Solar. Several financial institutions and other investors transferred additional funds to DC Solar totaling nearly $153 million. The funds were part of related transactions for the purchase and lease of generators. In total, DC Solar closed transactions with investors that contributed an aggregate of more than $912 million to purchase generators. Those transactions purportedly involved approximately 17,000 generators worth about $2.5 billion. Court records indicate that about half of the 17,000 generators did not exist, and DC Solar used false financial statements and lease contracts to conceal the fraud. Lauer transferred investor funds from one account to another to conceal the lack of revenue DC Solar was generating from rentals to third parties. He also took part in creating documents to hide those transfers.

As reported earlier, DC Solar's owners, Jeff and Paulette Carpoff, pled guilty to Federal charges in 2020. Jeff Carpoff was sentenced to 30 years in prison and ordered to pay more than $790 million in restitution. Paulette Carpoff was sentenced to 11 years in prison.

Source: FBI.
Responsible Agencies: This was a joint investigation conducted by the FDIC OIG, FBI, and Internal Revenue Service-Criminal Investigation. This matter was prosecuted by the USAO for the Eastern District of California, Sacramento.

Former Bank CFO Found Guilty of Bank Fraud

On March 6, 2026, Aaron Luneke, former Chief Financial Officer (CFO) of Bank of the Valley (BOV), was found guilty on two counts of bank fraud, 18 U.S.C. § 1344, after a 2-week trial in the District of Nebraska. Luneke was previously indicted by a Federal grand jury on July 15, 2024. He is scheduled to be sentenced on June 10, 2026.

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

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

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

Source: The FDIC's Division of Risk Management Supervision. Responsible Agencies: This is a joint investigation by the FDIC OIG, Federal Housing Finance Agency OIG, Federal Reserve Board (FRB) OIG, and the FBI. The matter is being prosecuted by the USAO for the District of Nebraska.

Loan Broker Sentenced

On February 20, 2026, Bun Khath was sentenced to 10 years in prison followed by 3 years of supervised release and ordered to pay $10,901,107 in restitution for his role in a bank fraud scheme. Previously, on February 11, 2025, he pled guilty to a one count superseding criminal information charging him with money laundering. Khath was indicted on July 26, 2023, along with co-conspirators Hugo Villanueva, William Mills, and Jennifer Williams, on charges of bank fraud, conspiracy to commit bank fraud, false statement to obtain credit, and conspiracy to commit money laundering in connection with a scheme to defraud multiple financial institutions by obtaining loans using fraudulent financial statements and collateral documentation.

Villanueva fled the country prior to indictment and was arrested in Lima, Peru, in November 2025 based on an Interpol notice. The government is currently in the process of extraditing Villanueva to the United States. Co-conspirator Jeremiah Almaguer was previously charged with money laundering via a superseding criminal information on May 31, 2024. Mills, Williams, and Almaguer have all pled guilty for their roles in the bank fraud conspiracy and are awaiting sentencing.

From at least 2016 and continuing through June 2021, loan brokers Khath and Almaguer conspired with tax preparer Villanueva to obtain fraudulent loans for multiple business borrowers, including Williams, using fraudulent documentation. Khath and loan broker Mills used connections with multiple financial institutions to introduce business owners seeking loans from the victim financial institutions. As part of the scheme, Khath and Mills formed shell companies and created fictitious contracts and equipment invoices to present to financial institutions in support of the borrower's loan requests to purchase new equipment; however, Khath and Mills did not sell equipment to the borrowers.

Khath and Mills would receive the loan proceeds, deduct their fee for assisting with the loan, and then transfer the remaining loan proceeds to the borrowers. Almaguer received proceeds from fraudulently obtained loans and laundered the funds through his bank accounts for his own benefit and the benefit of his co-conspirators. Villanueva allegedly prepared fraudulent financial statements and income tax returns with inflated figures to submit with the borrower's loan applications. Williams purported to own a pharmacy in Houston, Texas, and fraudulently obtained over $8 million in loan proceeds and caused a loss of over $6 million to an FDIC-insured institution. In total, the bank fraud scheme included dozens of loans from the victim financial institutions, at least $60 million in loan proceeds, and over $11 million in losses to FDIC-insured financial institutions.

Source: USAO for the Southern District of Texas.
Responsible Agencies: This is a joint investigation by the FDIC OIG, Federal Housing Finance Agency OIG, Internal Revenue Service-Criminal Investigation, and FBI. This matter is being prosecuted by the USAO for the Southern District of Texas.

OIG Special Agents' outreach explains aspects of their role in law enforcement.

KeyBank Agrees to $7.8 Million Settlement Agreement

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

In 2020 and early 2021, Hawkins worked as the branch manager of the Conshohocken, Pennsylvania, branch of KeyBank. Hawkins worked with co-conspirators to recruit individuals who owned companies with little or no operations to open bank accounts at Hawkins' branch and apply for PPP loans. Hawkins helped the recruited individuals submit PPP loan applications that contained materially false representations about the companies' number of employees and payroll expenses. The applications also included false documentation, including tax forms. Based on these fraudulent applications, Hawkins' bank approved at least 38 PPP loans and disbursed approximately $5 million. Hawkins received incentive compensation through the bank for opening business bank accounts for the companies that received the fraudulent PPP loans. Hawkins also had an agreement with his co-conspirators to pay him $5,000 for each PPP loan that he helped to secure.

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

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

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

Former Teller Sentenced

On January 5, 2026, Sarah Wilson, a former employee of First Citizens Bank & Trust Company, was sentenced to 21 months of incarceration, 3 years of supervised release, and ordered to pay a money judgment in the amount of $150,450, following her August 2025 guilty plea to three counts of Theft, Embezzlement, or Misapplication by a Bank Officer or Employee in violation of 18 U.S.C. § 656. Wilson had previously been indicted and was arrested and arraigned in the Middle District of North Carolina in May 2025. As part of Wilson's guilty plea, she stipulated and consented to the issuance of an Order of Prohibition from further participation with the FDIC.

According to court documents, Wilson was a teller at the Pilot Mountain branch of First Citizens Bank when, from December 2023 through May 2024, she stole $150,450 in cash from her teller drawer. To hide her theft, she entered numerous fraudulent transactions into the Bank's computer system – fraudulent buy/sell transactions associated with the bank's vault and fraudulent withdrawal transactions from the accounts of two elderly customers, then 89-years old and 90-years old, with whom Wilson was familiar.

When the 89-year-old customer asked Wilson about the suspicious account activity, she told him the account looked fine. By then, Wilson's fraudulent entries had effectively depleted his savings and certificate of deposit accounts by $59,700. She moved on to the 90-year-old customer's certificate of deposit account, effectively depleting it by $42,650. An audit in late May 2024 revealed an imbalance with Wilson's teller drawer. The bank launched an investigation and discovered the extent of Wilson's criminal conduct. The bank terminated Wilson and made the customers whole.

Source: This investigation was initiated based on a referral from First Citizens Bank's Special Investigation Unit.
Responsible Agencies: This case was investigated by the FDIC OIG. The matter was prosecuted by the USAO for the Middle District of North Carolina.

Former PNC Teller Pleads Guilty to Embezzling $80,000 from Customer Accounts

On March 23, 2026, former PNC Bank teller Rhodesia Zaire Jones pled guilty to one count of felony embezzlement and one count of misdemeanor filing a fraudulent tax return. Jones' sentencing is scheduled for May 11, 2026.

Jones was a bank teller at PNC Bank located in Troy, Michigan. PNC identified suspicious withdrawals related to a customer's account. PNC initiated an investigation into the withdrawals and discovered that Jones had performed 28 unauthorized withdrawals from personal and business accounts belonging to a PNC customer between September 11, 2023, and April 26, 2024. The withdrawals totaled $80,000.

Source: As a result of the growing partnership with the National Cyber Forensics and Training Alliance, PNC referred the matter to the FDIC OIG.
Responsible Agencies: This is a joint investigation by the FDIC OIG and the State of Michigan Department of Attorney General. The matter is being prosecuted by the State of Michigan Attorney General.

Former FDIC Employee Sentenced to Nearly 22 Years in Prison for Exploiting Child

On January 13, 2026, Jonathan Mackey, a former FDIC Acting Supervisory Examiner was sentenced in U.S. District Court to 262 months in prison and a lifetime of supervised release for sexually exploiting an 11-year-old. On August 7, 2025, he pled guilty in the Southern District of Ohio to 18 U.S.C. § 2251(a) & (e) - Sexual Exploitation of Children. 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 earlier 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.

Special Feature

Fraud Alerts

The FDIC OIG is continuing to focus attention on fraudulent schemes and efforts to prevent those from harming consumers and banks. Past semiannual reports have featured information on the nature of fraud and the OIG's outreach efforts to combat fraud, and warned about Pig Butchering scams and Impersonation schemes. In this report, we highlight "Call Spoofing" and "ATM Jackpotting."

Call Spoofing Scams

The FDIC OIG is warning banks and bank business customers about sophisticated telephone spoofing scams. These scammers initiate transactions using the business customers' bank accounts. The fraudsters are sophisticated and may offer details that give the appearance of legitimacy to bank business customers. Such scams could involve millions of dollars. For example, one FDIC supervised financial institution reported $5 million in recent call spoofing attempts.

How does it work?

- Fraudsters use call spoofing, a technique where they falsify the information transmitted to a caller ID display to disguise their identity. The phone number then appears to be the bank name and the phone number associated with the bank where a business maintains an account.
- In some instances, the fraudster may know and use the actual names of employees working at the business.
- The fraudster informs the business that they are seeing fraudulent activity associated with the business's bank account.
- To resolve this supposed activity, the fraudster informs the account holder that they need the user's online account login credentials.
- Once those credentials are received, the fraudster attempts to reset the customer's password to gain access to the account to initiate funds transfers.

Warning Signs:

- **High-Pressure Tactics:** A caller may create a false sense of urgency, or demand immediate action.
- **Suspicious Requests for Data:** Banks, companies, and government agencies will not call or send unsolicited correspondence asking for sensitive personal information.

Special Feature (continued)

How to Protect Yourself:

- Assume any caller, even from what appears to be a known number, could be a scammer.
- Hang up and verify the phone number by calling the number on the legitimate bank website. Do not redial the number that called.
- Do not provide any information to an unsolicited caller, including verifying your name, business name, phone number, or account information.
- If you suspect a spoofed or suspicious call, hang up immediately.
- Let the call go to voicemail instead of answering.

If you suspect that your business has been a victim of a spoofing scam, contact the FDIC OIG Hotline.

Consumers may experience similar spoofing calls, and in that event, should also contact the FDIC OIG Hotline.

ATM Jackpotting

The FDIC OIG is alerting banks about an increase in a type of fraud known as "ATM Jackpotting." ATM Jackpotting involves criminal actors accessing ATMs and placing malware software on the system, enabling them to illegally dispense cash from the bank's cash supply. The process is often run by sophisticated and organized crime rings at both the physical location (accessing machine and hard drive) and operating in foreign jurisdictions (transmitting malware codes). The FBI estimates 700 instances of ATM Jackpotting and losses totaling more than $20 million in 2025.

How this Fraud Targets ATMs: A criminal actor will access the ATM, most often by opening an ATM face, and remove the hard drive to place malware onto the device before returning the hard drive to the ATM. Once the malware is installed, the perpetrator will dispense the cash from the ATM. The malware interacts directly with the ATM hardware, bypassing any communications or security of the original ATM software. Other methodologies utilize devices to connect directly with the ATM hard drive.

ATM Jackpotting Warning Signs: Prior to committing fraud, perpetrators might do the following:

- Initiate surveillance of an ATM location to look for re-stocking and personnel routines, or CCTV placement.
- Take photographs of the ATM to determine the necessary key to access the system.
- Try to access an ATM and quickly leave to observe law enforcement response time and determine if there are any alarms on the machine. These criminals will then access the machine, download the malware, and receive instructions from the foreign actors to go through the process of dispensing the cash.

Special Feature (continued)

Typically, these criminals will access multiple ATMs from one financial institution on the same day, or consecutive days, if they can confirm their ability to access the machines. The most common target locations are standalone ATMs in more rural locations. Other warning signs include:

- ATM door open outside of planned maintenance schedule.
- New executable files that are not expected, appearing on the ATM hard drive.
- Detection of unauthorized devices such as USB keyboards, USB hubs, or flash drives.
- Removal of an ATM hard drive.
- Low or no cash indicators outside of expected use schedule.

Mitigation and Prevention: To mitigate or prevent the occurrence of this type of fraud, the following tactics should be considered:

- Re-key all ATMs with unique access keys.
- Add an ATM security gate to the front of the machine.
- Encrypt ATM software.
- Install ATM hood alarms that must be disengaged with a code.
- Utilize CCTV cameras and license readers.
- Change standard locks on ATM devices to prevent the use of keys available for purchase online.
- Add tamper-resistant screws to hold the ATM hard drive in place.
- Train employees on surveillance awareness:
    - Unusual vehicle activity in or around the branch location.
    - Individuals photographing the facility.
    - Unexpected alarms on ATMs late at night.

Responding to Potential Fraud: If you believe that an ATM has been targeted by this type of fraud, you should:

- Immediately contact local law enforcement, the FBI https://www.fbi.gov/contact-us/field-offices or the FBI Internet Crime Complaint Center at https://www.ic3.gov/), and the FDIC OIG hotline.
- Preserve all applicable surveillance footage.
- Close the ATM lane and treat the area as a crime scene.

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 40 locations in the U.S.

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

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; Eastern District of Pennsylvania Money Laundering Working Group; New Jersey Security Association; Long Island Fraud and Forgery Association; Connecticut USAO Bank Secrecy Act Working Group; Connecticut Digital Assets Working Group; South Jersey SAR Task Force; Pennsylvania Electronic Crimes Task Force; NJ COVID-19 Fraud Task Force; Newark IRS-CI Financial Fraud Working Group; Western District of New York Payment Protection Program Working Group; District of New Hampshire USAO SAR Review Team; Financial Fraud Investigation Partnership with Southern District of NY; NY Cyber Confidence Fraud Schemes Working Group; Maryland Association for Bank Security; Virginia Crime Analysis Network; Florida Crime and Intelligence Analyst Association.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force; Northern District of Georgia Mortgage Fraud Task Force; Eastern District of North Carolina Bank Fraud Task Force; Northern District of Alabama Financial Fraud Working Group; Northern District of Georgia SAR Review Team; Middle District of Georgia SAR Review Team; South Carolina Financial Fraud Task Force; Eastern District of North Carolina Financial Crimes Task Force; Western District of North Carolina Financial Crimes Task Force; Middle District of North Carolina Financial Crimes Task Force.
Miami Region	COVID Working Groups-Southern District of Florida, Middle District of Florida, Northern District of Florida; SAR Review Groups-Miami, Palm Beach, Treasure Coast Financial Crimes Review Team, Key West/Monroe County; DOJ-COVID-19 Fraud Strike Force- Miami.
Kansas City Region	Kansas City SAR Review Team; USAO for the District of Montana's "Guardians Project;" St. Louis SAR Review Team; Minnesota Inspector General Council; Minnesota Financial Crimes Task Force; Nebraska SAR Review Team; Southern District of Iowa SAR Review Team; Iowa Agricultural Task Force in USAO-Northern District Iowa and USAO-Southern District Iowa (joint collaboration with U.S. Department of Agriculture OIG, FBI, FRB OIG, and FDIC OIG).
Chicago Region	Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Central District of Illinois Financial Fraud Working Group; Northern District of Illinois SAR Review Team; Cook County Region Organized Crime Organization; FBI Milwaukee Area Financial Crimes Task Force; FBI Northwest Indiana Public Corruption Task Force; Eastern District of Wisconsin SAR Review Team; Western District of Wisconsin SAR Review Team; Western District of Wisconsin Bankruptcy Fraud Working Group; Indiana Bank Fraud Working Group; Northern District of Indiana SAR Review Team; FBI Louisville Financial Crime Task Force; Western District of Kentucky SAR Review Team; Eastern District of Kentucky SAR Review Team; Southern District of Ohio SAR Review Team; Michiana Loss Prevention Working Group; AML Financial Institution/LE Networking Group; FBI Chicago Financial Crimes Task Force; Western District of Michigan SAR Review Team; Northern District of Ohio SAR Review Team; Southern District of Indiana SAR Review Team; Financial Crimes Investigators Madison; Financial Crimes Investigators Northeast Wisconsin; Financial Crimes Investigators Northwest Wisconsin; WDKY Bankruptcy Fraud Working Group; Midwest Interagency Supervision Working Group; SEC Interagency Securities Council; OIG Illinois Fraud Working Group; FBI Northwest Indiana Public Corruption Task Force.
San Francisco Region	Fresno Mortgage Fraud Working Group for the Eastern District of California; Sacramento Mortgage Fraud Working Group for the Eastern District of California; Sacramento SAR Working Group; Orange County Financial Crimes Task Force-Central District of California; Orange County SAR Review Team; Northern District of California Money Laundering SAR Review Task Force; San Diego Financial Investigations and Border Crimes Task Force; Northern Nevada Financial Crimes Task Force; Financial Services Roundtable coordinated by the USAO of the Northern District of California; Los Angeles Complex Financial Crimes Task Force – Central District of California; Los Angeles Real Estate Fraud Task Force – Central District of California; Homeland Security San Diego Costa Pacifica Money Laundering Task Force; DOJ National Unemployment Insurance Fraud Task Force; California Unemployment Insurance Benefits Task Force; Nevada Fight Fraud Task Force; Las Vegas SAR Review Team; COVID Benefit Fraud Working Group, USAO District of Oregon; Hawaii Financial Intelligence Task Force.
Dallas Region	Oklahoma City Financial Crimes SAR Review Working Group; Austin SAR Review Working Group; Houston High Intensity Drug Trafficking Area SAR Team; Western District of Oklahoma Economic Crimes Working Group and Fraud/SAR Review Team; Eastern District of Oklahoma White Collar Working Group/SAR Review Team; Northern District of Texas COVID Task Force; District of Colorado COVID Task Force; Southern District of Texas SAR Review Team.
Mid-Atlantic Region	Virginia Crime Analysts Network; Northern Virginia Financial Initiative SAR Review Team; Pandemic Response Accountability Committee (PRAC) Fraud Task Force; PRAC Law Enforcement Coordination Subcommittee; PRAC Data Analytics Subcommittee; CIGIE COVID-19 Working Group; DOJ Stimulus Funds Fraud Working Group; District of Maryland SAR Review Task Force; Western District of Virginia SAR Review Task Force, Roanoke, Virginia; Western District of Virginia SAR Review Task Force, Abingdon, Virginia; Eastern District of Virginia SAR Review Task Force; Central Eastern District of Virginia SAR Review Task Force; Northern Virginia Eastern District of Virginia SAR Review Task Force; DOJ Foreign Corrupt Practices Act SAR Initiative; District of Columbia SAR Review Task Force; Southern District of West Virginia SAR Review Task Force; Northern District of West Virginia SAR Review Task Force; Delaware SAR Review Task Force; Maryland Financial Intelligence Team; Global SAR Task Force via the IRS-CI Global Illicit Financial Team (GIFT); Bank Fraud Working Group, National Capital Region; FBI Maryland Financial Crimes Task Force.
Electronic Crimes Unit	Washington Metro Electronic Crimes Task Force; High Technology Crime Investigation Association; FBI Northern Virginia Cyber Task Force; DOJ Civil Cyber-Fraud Task Force; CIGIE Information Technology Committee; CIGIE Forensic Accountant Networking Group; CIGIE Financial Cyber Working Group; National Cyber Investigative Joint Task Force; FBI Headquarters Money Laundering, Forfeiture & Bank Fraud Unit; FBI Baltimore 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, 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 (now 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, and subsequently with the FDIC Chief of Staff who now Chairs the Audit Committee to provide status briefings and present the results of completed audits, evaluations, and related matters for the Audit Committee Chairman's and other Committee members' consideration. Presented the results of OIG audits, evaluations, and other 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.
- Sent out a Global message to all FDIC staff to remind them about the detrimental impact that fraud can have and how the OIG works to combat fraud in the banking system. The message highlighted certain OIG cases and the ways in which the OIG educates others about fraud and engages in outreach efforts across the country.
- 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. Added an information text box to our external website that captures our "Accomplishments by the Numbers." At a glance, visitors to the website will see the overall impact of our audit, evaluation, and investigative work.

- 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.
- Issued several Scam Alerts. These alerts covered scams of ATM Jackpotting, Call Spoofing, Impersonations, and Pig Butchering. We also shared news on these postings with a representative of the Conference of State Bank Supervisors, as we had received an inquiry from that organization related to Impersonation scams.
- Joined the Social Security Administration OIG and other OIGs in recognizing "National Slam the Scam Day," which is an annual initiative to raise awareness about government imposter scams.
- Supported the Association of Certified Fraud Examiners' International Fraud Awareness week with various social media postings reiterating to the public the need to be mindful of fraudulent schemes.
- Met with the IG and Assistant Inspector General for Investigations for the Securities and Exchange Commission to discuss future collaboration and coordination on investigations related to bank fraud and securities fraud.
- Updated website information on the OIG, Office of Audits, and Office of Investigations by revising and updating information for stakeholders on the OIG as a whole and the specific nature, focus, and results and impact of Office of Audits' and Office of Investigations' efforts.
- Supported efforts of 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. Also provided one of the OIG's Special Agents to assist the Federal Communications Commission OIG by leading criminal investigations in support of that office.
- 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.

- Replied to Senator Ernst's office in response to a letter received by the IG from the Senator regarding allegations of misconduct in the FDIC OIG. Provided extensive information to Senator Ernst's staff along with a written response, demonstrating that we take all allegations seriously. For many of the allegations, our reviews found that the allegations were not supported by the evidence we identified and shared with Congressional staff. Committed to continuing to work to understand, identify, and address all real or perceived issues at the FDIC OIG and to improve our office climate.

- 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 462 Hotline inquiries, 21 of which led to our opening investigations. Our online form, email, telephone, and regular mail were the most common vehicles for inquiries.

- 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 the CIGIE's Legislation Committee.

- Responded to a CIGIE Data Call in response to CIGIE's statutory requirement to transmit an annual report on behalf of the OIG community to the President and select congressional committees. Discussion of our Special Inquiry on the *FDIC's Workplace with Respect to Harassment and Related Misconduct* is included in the annual report under "Holding Government Employees Accountable."

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

- Participated as a member of the Council of Inspectors General on Financial Oversight (CIGFO), as established by the Dodd-Frank Wall Street Reform and Consumer Protection Act and coordinated with the IGs on that Council. This Council facilitates sharing of information among its member Inspectors General and discusses ongoing work of each member IG as it relates to the broader financial sector and ways to improve financial oversight. Participated on CIGFO's Working Group related to the Financial Stability Oversight Council's Designation of Non-Bank Financial Companies.

- 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 Government Accountability Office specifically related to its Congressional request to review the status of IG community senior level staffing shortages and assess the impact over the past 5 years, as well as future operations.
- Coordinated with the Office of Management and Budget to address matters of interest related to our 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 Commodity Futures Trading Commission's Interagency Campaign: *"Dating or Defrauding?"*, the Bank Fraud Working Group; the Bank Secrecy Act/Anti-Money Laundering Department at Central Pacific Bank in Honolulu, Hawaii; Annual Financial Crime Forum for the Association of Certified Anti-Money Laundering Specialists, San Diego, Baja California Section; Association of Certified Anti-Money Laundering Specialists' US Capital Chapter event: *Fighting Fentanyl: Lessons Learned for AML and Financial Crime Professionals*; AML Partnership Forum annual event; Maryland Association for Bank Security; and multiple sessions on TD Bank to New York area bankers and financial professionals. 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 $42.2 million – a $6.3 million reduction from the FY 2026 enacted level of $48.5 million—or a 13 percent reduction. The President's budget supports $39.2 million for personnel salaries and benefits for 97 full-time equivalents and $3 million for non-personnel expenses.
- Selected a new Case Management System for OI and awarded a contract in December 2025 after months of careful planning, analysis, and coordination. The new platform will meet immediate operational needs, strengthen case tracking, enhance data security, and improve efficiency, reliability, and scalability.
- 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.
- Finalized a draft Strategic Plan and goals for 2026-2031. The plan establishes areas of focus office-wide to ensure that in carrying out the OIG's statutory mission involving audits and investigations, we strengthen relationships with stakeholders and partners, optimize our administration of resources and technology, and remain focused on the value of our people and workplace culture.
- Joined with the Federal Trade Commission to present on Impersonation Schemes at the FDIC's Data Summit. Of particular interest to us, impersonation frauds can involve scammers who pretend to be either FDIC or FDIC OIG employees to provide a false sense of legitimacy as they seek to exploit unwitting victims. We conveyed the need to be mindful of these scams, and we are committed to combatting such frauds.
- Leveraged technology in an OA assignment by conducting in-house adversary emulation tests using an open-source module and in close coordination with the FDIC's Chief Information Officer Organization and Division of Information Technology. The tests simulate real-world attacks by threat actors in order to uncover risks and security gaps before they impact an organization.
- Updated the OIG's intranet site to inform staff of administrative, facilities, and operational services of importance to OIG staff.
- Updated our policy on permissible use of Artificial Intelligence (AI) and Machine Learning tools in the OIG in compliance with OMB-Memorandum M-25-21 and relevant privacy and security requirements. As a related initiative, planned a TEAMS forum for OIG staff to convey information on Microsoft CoPilot Chat, which will become available for OIG staff.

- Held various OIG Workforce Connect sessions to keep OIG staff informed on issues of interest to them: benefits, FY 2026 and FY 2027 budget matters, options for the Deferred Resignation Program, Voluntary Early Retirement Authority, Voluntary Separation Incentive Payment, and the Federal Employees Retirement System.

- 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 dashboard that provides multiple human resources-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. Currently, all OIG employees can access cloud-based data management software and machine learning analytical tools. We are currently testing generative AI tools with the first launch in May, and several more powerful generative AI tools are planned to release in Fall 2026. The OIG is currently piloting AI tools in several audit and investigatory tools to determine the return on investment. The OIG will continuously work to integrate additional data and analytical tools each quarter as resources permit.

- Advanced the OIG's data analytics capabilities related to Payment Protection Program fraud through collaboration with the PRAC, FDIC, Financial Crimes Enforcement Network, Federal Trade Commission, DOJ, FBI, and private-sector entities. Additionally, the OIG is expanding our access to data related to commercial real estate and agriculture to detect bank fraud and threats to the integrity of the banking system.
- Relied on the OIG's General Counsel's Office to ensure the office complied with legal and ethical standards, rules, principles, and guidelines; provide legal advice and counsel to teams conducting audits, evaluations and other reviews; and support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.
- Continued to disseminate information on OIG internal policies related to audit, evaluation, investigation, operations, and administrative processes of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the Office. Also ensured adherence to Executive Orders as they pertain to operations of the OIG.
- Oversaw contracts to qualified firms to provide audit, evaluation, IT, and other services to the OIG to provide support and enhance the quality of our work and the breadth of our expertise as we conduct audits, evaluations, and investigations, and to complement other OIG functions, and closely monitored contractor performance.

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. The FDIC IG is also a member of the CIGIE Strategic Hiring Committee, established in accordance with the Office of Personnel Management's guidance implementing Executive Order 14356.
- Held an All-OIG Meeting in January 2026 to set the OIG's tone and agenda for the new year and to give all component office heads an opportunity to look back to their teams' accomplishments and look forward to new initiatives and priorities going forward.
- 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. Formed part of the CIGIE Working Group to update the Qualitative Assessment Review Guidelines for Investigative Operations of Federal Offices of Inspector General.
- 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. The Council installed new members to fill term vacancies and met several times to pursue its mission.
- 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.
- Informed OIG staff of the results of an independent review of the FDIC OIG's hiring and promotion processes to address concerns raised in an earlier report of the Workforce Council. At the IG's request, our Office of Management engaged two external human resources teams to review our processes and provide recommendations. The external reviewers confirmed compliance with applicable regulations and identified some areas for procedural improvement, which the OIG has pursued.
- 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.
- Solicited nominations for OIG Distinguished Achievement Awards for both individuals and teams to acknowledge their outstanding efforts and contributions in preventing, detecting, and deterring fraud, waste, abuse, misconduct, and mismanagement at the FDIC and in the banking sector, and promoting economy, efficiency, effectiveness, and integrity at the FDIC.
- 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. Also rotated in OI's Special Agents in Charge to the position of Deputy Assistant Inspector General for Investigations to temporarily fill that vacancy.
- Met monthly with our Data Analytics and Innovation Working Group members to educate staff on AI and Machine Learning tools currently deployed in the OIG. Coordinated with the FDIC's Chief Artificial Intelligence Officer and Legal Division representatives with regard to use of these tools.
- Held a 2-day event for Office of Audits' staff with the theme: *Organizationally Aligned*. The forum covered such topics as Resiliency, Office of Audits' Norms, the System of Quality Management, Work/Life Balance, Challenges, and Effective and Collaborative Oversight.

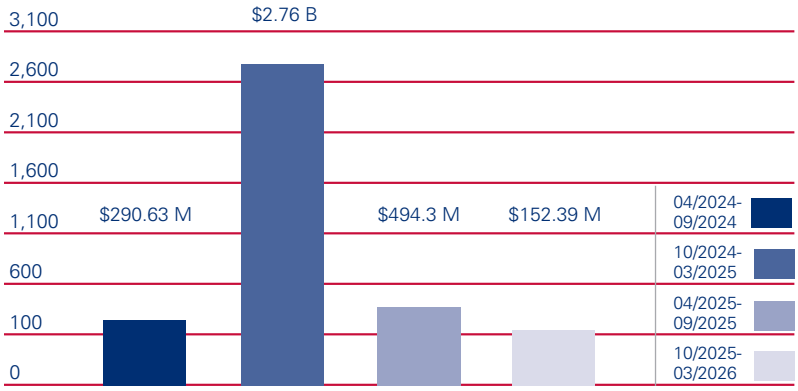
- Arranged sessions at the FDIC Library and the FDIC's Virtual Outreach Center, and a discussion with FDIC officials from the Office of Communications and the Office of Executive Secretary for Office of Management staff. The Office of Management team also visited the General Services Administration's OIG to meet with their peers -- and for a briefing on artificial intelligence, provided by the General Services Administration OIG's Chief Information Officer who also serves on CIGIE's IT Committee with responsibility for AI best practices in the OIG community.
- Held an OI Leadership Meeting covering the closeout of the former investigations case management system, the system transition and interim management processes and internal controls, the functioning and features of the future case management system, and a variety of other investigative and administrative topics. The intent of the session was to share information on the new system and help OI leadership ensure continued success going forward.
- Convened a meeting with Managers throughout the office to hear updates on their areas of responsibility and any concerns and ideas they might have with office-wide impact. Results of the discussions were shared with OIG senior management, as appropriate, and plans are to hold such meetings monthly.

Mission, Values, and Vision inspire the OIG's oversight of the FDIC.

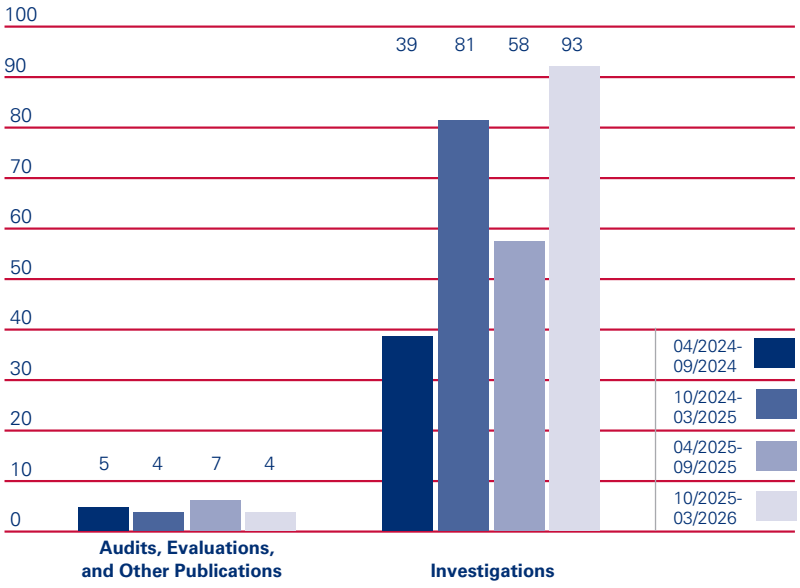
Cumulative Results (2-year period)

Recommendations	
April 2024 – September 2024	42
October 2024 – March 2025	21
April 2025 – September 2025	23
October 2025 – March 2026	12

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. (Also included in Section 405 (b), 5 U.S.C.)

Reporting Requirements	Page
Section 4(a)(2): Review of legislation and regulations.	44-45
Section 5(a)(1): A description of significant problems, abuses, and deficiencies relating to the administration of programs and operations of the establishment and associated reports and recommendations for corrective action made by the Office.	5-7
Section 5(a)(2): An identification of each recommendation made before the reporting period, for which corrective action has not been completed, including the potential cost savings associated with the recommendation. (Recommendations open for more than one year are noted.)	46-56
Section 5(a)(3): A summary of significant investigations closed during the reporting period.	17-26
Section 5(a)(4): An identification of the total number of convictions during the reporting period resulting from investigations.	3
Section 5(a)(5): Information regarding each audit, inspection, or evaluation report issued during the reporting period, including– (A) a listing of each audit, inspection, or evaluation; (B) if applicable, the total dollar value of questioned costs (including a separate category for the dollar value of unsupported costs) and the dollar value of recommendations that funds be put to better use, including whether a management decision had been made by the end of the reporting period.	57
Section 5(a)(6): Information regarding any management decision made during the reporting period with respect to any audit, inspection, or evaluation issued during a previous reporting period.	58
Section 5(a)(7): The information described under section 804(b) of the Federal Financial Management Improvement Act of 1996.	58
Section 5(a)(8): (A) An appendix containing the results of any peer review conducted by another Office of Inspector General during the reporting period; or (B) if no peer review was conducted within that reporting period, a statement identifying the date of the last peer review conducted by another Office of Inspector General.	61-63

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

Appendix 1

Information in Response to Reporting Requirements

Review of Legislation and Regulations

Much of the FDIC OIG's activity considering and reviewing legislation and regulation occurs in connection with the 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 has considered 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).
- **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 could 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.

Also of interest to our office is S. 4099, Whistleblower Anti-Gag Act of 2026. This bill was introduced by Senator Chuck Grassley and referred to the Committee on Homeland Security and Governmental Affairs on March 16, 2026. Current law requires federal agency nondisclosure policies, forms, and agreements to notify employees of their right to make whistleblower disclosures to Congress, an Inspector General, or the Office of Special Counsel (5 U.S.C. § 2302(b)(13)). This bill would amend Section 2302(a)(2)(C)(i) of Title 5, United States Code, and expand this anti-gag provision coverage to executive agency employees of government corporations, such as the Federal Deposit Insurance Corporation and the Export-Import Bank.

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 16 recommendations.

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

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

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

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
REV-24-01 **Review of FDIC's Ransomware Readiness** March 20, 2024	Ransomware can severely impact business processes and leave organizations without the data needed to operate or deliver mission-critical services. The organizations affected often experience reputational damage, significant remediation costs, and interruptions in their ability to deliver core services. The FDIC relies heavily on information systems to carry out its responsibilities of insuring deposits; examining and supervising financial institutions for safety, soundness, and consumer protection; making large and complex financial institutions resolvable; and managing receiverships. The FDIC needs effective controls for safeguarding its information systems and data to reduce the risk that a ransomware incident could disrupt critical operations and allow inappropriate access to, and disclosure, modification, or destruction of, FDIC information. We conducted a review to assess the adequacy of the FDIC's process to respond to a ransomware incident. We determined that the FDIC had an adequate process to respond to a ransomware incident and generally followed applicable guidance and best practices within the control areas we assessed. However, the FDIC did not fully adhere to Federal standards, FDIC policies, and/or industry best practices related to: (1) protecting backup data and testing the capability to restore systems from backups; (2) maintaining a current, complete, and accurate Continuity Implementation Plan; (3) enabling Wireless Priority Service access for all FDIC Chief Information Officer Organization Executive Management Emergency Command Team Members; and (4) ensuring that key individuals completed Disaster Recovery Awareness Training. We made eight recommendations to address these issues and strengthen the FDIC's process to respond to a ransomware incident. 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 Total	Recommendations Outstanding	Potential Cost Savings
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, and 15 are unimplemented.	24	4**	N/A

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-24-01 **Audit of Security Controls for the FDIC's Cloud Computing Environment** September 4, 2024	Cloud computing offers many potential benefits, including optimizing costs, flexibility, scalability, and enhanced security. It enables organizations to do more with less by eliminating their on-premises infrastructure with the reduction of servers and staff to support that infrastructure. While cloud computing offers many benefits, it does not eliminate the customer's responsibility to manage security risks appropriately. The FDIC continues to expand its cloud presence by migrating its mission essential and mission critical applications into the cloud. The FDIC must ensure that its systems and data within the cloud are secured and that control weaknesses are effectively addressed. Failure to do so could result in damage and harm to FDIC systems and data, hindering its ability to maintain stability and confidence in the nation's financial system. We engaged Sikich CPA LLC (Sikich) to conduct an audit of security controls for the FDIC's cloud computing environment. The objective of this performance audit was to assess the effectiveness of security controls for the FDIC's cloud computing environment. Sikich found that the FDIC had effective controls in four of nine security control areas assessed. However, Sikich determined that the FDIC had not effectively implemented security controls in its cloud computing environment in five areas, including Identity and Access Management, Protecting Cloud Secrets, Patch Management, Flaw Remediation, and Audit Logging. Sikich made 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, 6, and 7 are unimplemented.	7	4**	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, 6, and 7 are unimplemented.	11	3**	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 I: Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-25-01 **The FDIC's Procurement of Resolution and Receivership Services** June 10, 2025	Emergency preparedness to procure the services needed to resolve unexpected financial institution failures and systemic financial risks is key to the FDIC's mission of maintaining stability and public confidence in the U.S. financial system. In Spring 2023, the FDIC was appointed receiver for Silicon Valley Bank, Signature Bank, and First Republic Bank, three of the largest bank failures in FDIC history. In response, the FDIC engaged two contractors for advisory services to support the resolution of these failed banks and mitigate a potential systemic financial crisis. We conducted an audit to determine whether the FDIC awarded certain resolution and receivership contracts in accordance with best practices for government contracting and FDIC requirements. While the FDIC established emergency acquisition procedures with a focus on allowing "maximum flexibility," we identified seven best practices that would continue to permit flexibility while also enhancing controls and emergency acquisition preparedness. We also found that FDIC personnel did not adhere to some emergency acquisition procedures while awarding two resolution and receivership contract actions. This report contained 10 recommendations intended to improve the FDIC's emergency contracting procedures and control environment. Recommendations 1, 2, 3, 5, 6, 8, 9, and 10 are unimplemented.	10	8	N/A

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
MEMO-25-03 **Significant Service Provider Examination Program** August 12, 2025	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 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. We conducted the 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 found that while the FDIC had developed strategic objectives and made progress in its performance management efforts, the FDIC had not established program-level performance goals and metrics to measure overall SSP Examination Program effectiveness and efficiency. The report contained a recommendation that the FDIC complete efforts to develop and implement program-level goals and metrics for its Service Provider Examination Programs. Recommendation 1 is unimplemented.	1	1	N/A

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-25-02 **Audit of Security Controls for a Cloud Platform and Application** September 25, 2025	The FDIC has increasingly adopted cloud services to support its business functions. As of July 2025, the FDIC has 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 engaged Sikich CPA LLC (Sikich) to assess security controls on four cloud platforms and one Application Program Interface platform. We later engaged Sikich to conduct a performance audit of security controls for a fifth cloud platform and application. (These were not included earlier because the application was undergoing a major upgrade at the time.) The objective of this audit was to again assess the effectiveness of their security controls. 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 not consistently 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. Recommendations 1, 2, 3, and 4 are unimplemented.	8	4	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-25-03 **The FDIC's Information Security Program – 2025** September 26, 2025	The Federal Information Security Modernization Act of 2014 (FISMA), Public Law No. 113-283, requires Federal agencies, including the FDIC, to conduct annual independent evaluations of their information security programs and practices and to report the results to the Office of Management and Budget (OMB). FISMA requires the independent evaluations to be performed by the Agency IG, or an independent external auditor as determined by the IG. We contracted with the firm KPMG LLP to perform this work. The objective of this evaluation was to assess the effectiveness of the FDIC's information security program and practices. KPMG determined that the FDIC's overall information security program was operating at a Maturity Level 4 (Managed and Measurable) with respect to the FY 2025 FISMA Metrics. KPMG found the FDIC's information security program was generally effective and that the FDIC established several information security program controls and practices that were consistent with FISMA requirements. However, the report describes security control weaknesses that diminished the effectiveness of certain aspects of the FDIC's information security program and practices. Newly identified security control weaknesses included: • The FDIC did not implement privileged access review frequency requirements for both of the systems we tested. • The FDIC utilized an incomplete and inaccurate listing for user recertification for one of the systems we tested. KPMG made four new recommendations related to weaknesses identified during this year's evaluation. Recommendation 1 is unimplemented.	4	1	N/A

Table II: Audit and Evaluation Reports				
Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	Title*	Total	Unsupported	
AUD-26-01 January 6, 2026	*The FDIC's Student Residence Center*			
AUD-26-02 January 30, 2026	*Oversight of the Infrastructure Support Services Contract*	$4,629,334	$4,629,334	$2,000,375
EVAL-26-01 March 2, 2026	*In-Depth Review of Pulaski Savings Bank*			
Totals for the Period		**$4,629,334**	**$4,629,334**	**$2,000,375**

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

Note: On March 26, 2026, the OIG issued its report on the Top Management and Performance Challenges Facing the FDIC. This report is required under the Reports Consolidation Act and is based on a compilation of audit, evaluation, and investigative work of our Office and other information resources.

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	93
Number of Persons Referred to the Department of Justice for Criminal Prosecution	23
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	0
Number of Indictments and Criminal Informations	21

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 the reporting period, we substantiated allegations of misconduct against four senior FDIC officials. In two instances, the officials were subjects of an administrative investigation for emailing confidential information and personally identifiable information to a personal email, in violation of the FDIC's IT policies on securing information. We did not refer these cases to DOJ. Reports of investigation were sent to the Corporation for any action it deemed appropriate. In a third case, we conducted an administrative investigation of a senior FDIC official for employee misconduct involving the use of the official's position to improperly influence the hiring and promotion of employees. Additionally, the senior FDIC official attempted to interfere with the OIG's investigation. We referred the matter to DOJ and it was declined in June 2024. The subject of this investigation voluntarily resigned through the Deferred Resignation Program in June 2025. In a final criminal case, and as described earlier in this report, a former senior government official had earlier pled guilty and was sentenced in January 2026 to nearly 22 years in prison for exploiting a child.

Table VII: Instances of Whistleblower Retaliation

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

Table VIII: Instances of Agency Interference with OIG Independence

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

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

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

During this reporting period, there were no audits or evaluations involving senior government employees that were closed and not disclosed to the public. With respect to investigations, we closed five investigations of senior FDIC officials that were not disclosed to the public. Three of these involved substantiated allegations—as noted in Table VI of this report above (two instances of emailing confidential information and one instance of misuse of official position to influence hiring and promotion of employees). Additionally, two other administrative cases were closed and not disclosed. The first related to a Hotline allegation that the senior official inappropriately authorized travel for a subordinate by providing the employee with repeated and arbitrary out-of-town assignments. The senior official resigned while under investigation and accepted the FDIC's Voluntary Separation Incentive Payment offer. As for the second case, the senior official was investigated for allegedly making false representations to the FDIC and other government entities regarding his citizenship status, employment status, as well as work status (i.e., circumventing FDIC IT systems to work remotely when he claimed to be in regular duty status). Additionally, the senior government official was alleged to have misused Economic Injury Disaster Loan funds and failed to report ownership interests in businesses outside of the United States while working at the FDIC. This case was presented to DOJ for criminal prosecution but was ultimately declined.

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 October 1, 2025 through March 31, 2026 (for failures that occur on or after January 1, 2014 causing losses to the Deposit Insurance Fund of less than $50 million)

When the Deposit Insurance Fund (DIF) incurs a loss under $50 million, 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 undertook a Failed Bank Review of the failure of Metropolitan Capital Bank & Trust, Chicago, Illinois, which failed on January 30, 2026. The FDIC preliminarily estimated that the failure would cost the DIF about $19.7 million. Our Failed Bank Review was in progress as of March 31, 2026.

Appendix 3

Peer Review Activity

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

Definition of Audit Peer Review Ratings

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

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

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

Audit Peer Reviews

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

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

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

This peer review report is posted on our Website.

Inspection and Evaluation Peer Reviews

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

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

As conveyed on March 26, 2026, in the Department of Education OIG's opinion, the system of quality control for the FDIC OIG in effect for the year ended September 30, 2025, had been suitably designed and complied with to provide the FDIC OIG with reasonable assurance of performing and reporting in conformity with the Blue Book. Inspection and Evaluation (I&E) organizations can receive a rating of pass, pass with deficiencies, or fail. The FDIC OIG received an External Peer Review rating of **Pass**. The Department of Education OIG also issued a letter of comment that set forth findings that were not considered to be of sufficient significance to affect its opinion on the peer review.

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 Office of Inspectors General with Statutory Law Enforcement Authority and Section 6(e) of the Inspector General Act of 1978, as amended. Those documents authorize law enforcement powers for eligible personnel of each of the various Offices of Inspector 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 prior reporting period, we issued the results of our review of the system of internal safeguards and management procedures for the investigative operations of the Office of Inspector General (OIG) for the U.S. General Services Administration (GSA) for the 12 months ending September 2024. Our review was conducted in conformity with the *Quality Standards for Investigations* and the *Qualitative Assessment Review Guidelines for Investigative Operations of Federal Offices of Inspector General* established by CIGIE, as applicable.

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

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

Our review found that the system of internal safeguards and management procedures for the investigative operations of the GSA OIG for the period ending September 2024 complied with the quality standards established by CIGIE and other applicable guidelines and statutes cited above. These safeguards and procedures provided reasonable assurance of conforming to professional standards in the planning, execution, and reporting of GSA OIG investigations and in the use of law enforcement powers.

OIG 250th

We are working as an OIG in a tradition going back almost 250 years….

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

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

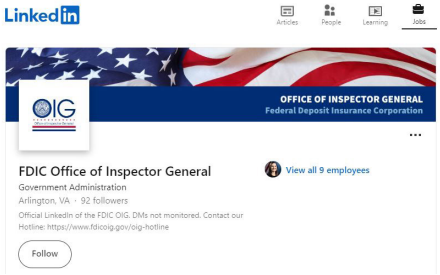
The basic tenets of the IG Act have remained constant and strong over the past nearly half century. Although amended several times, for example, to add new IGs, increase authorities, clarify reporting requirements, and create a governing Council, the Act has given IGs the authority and responsibility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

The FDIC OIG is proud to be part of the historical evolution of the IG concept, and we look forward to continuing to serve the best interests of our Nation as we prepare to celebrate America's 250th.

★**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

Office of Inspector General

Federal Deposit Insurance Corporation

HOTLINE

Do you suspect fraud, waste, abuse, mismanagement, or misconduct in FDIC programs or operations, or at FDIC banks?

For example:

- **Fraud by bank officials or against a bank**
- **Cybercrimes involving banks**
- **Organizations laundering proceeds through banks**
- **Wrongdoing by FDIC employees or contractors**

Make a Difference and Contact Us:

www.fdicoig.gov/oig-hotline **1-800-964-FDIC**

3501 Fairfax Drive • Room VS-D-9069 • Arlington, VA 22226

The OIG reviews all allegations and will contact you if more information is needed.

Individuals contacting the Hotline via the website can report information openly, confidentially, or anonymously.

OIG
Office of Inspector General

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-005-2026