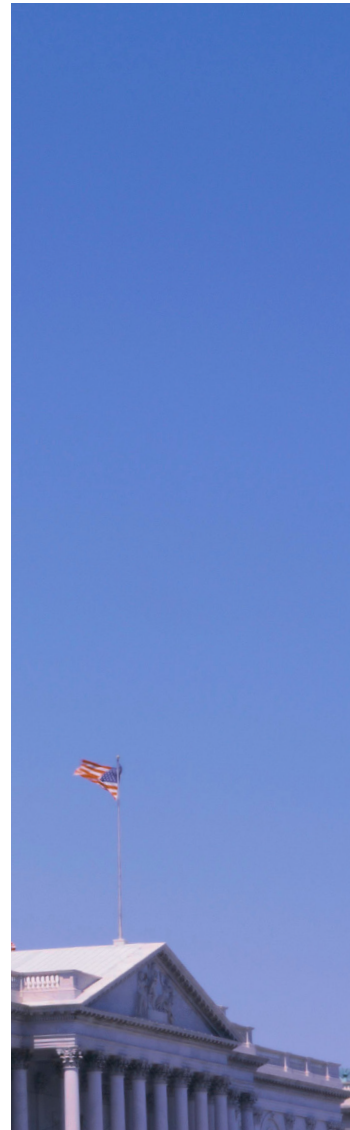


FDIC Office of Inspector General **Semiannual Report to the Congress**

October 1, 2024 - March 31, 2025



Integrity • Independence • Accuracy • Fairness • Objectivity • Accountability • Transparency • Professionalism • Judgment

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

The FDIC is an independent agency created by the Congress to maintain stability and confidence in the Nation's banking system. The FDIC insures deposits; examines and supervises financial institutions for safety and soundness and consumer protection; makes large, complex financial institutions resolvable; and manages receiverships. Approximately 6,404 individuals carried out the FDIC mission throughout the country as of December 31, 2024.

According to most current FDIC data (December 31, 2024), the FDIC insured \$10.7 trillion in domestic deposits in 4,496 institutions, of which the FDIC supervised 2,848. The Deposit Insurance Fund balance totaled \$137.1 billion as of December 31, 2024. Active receiverships as of March 31, 2025, totaled 48, with assets in liquidation of about \$27.18 billion.





Semiannual Report to the Congress

October 1, 2024 - March 31, 2025



Office of Inspector General



Federal Deposit Insurance Corporation



Inspector General's Statement



On behalf of the Office of Inspector General (OIG) at the Federal Deposit Insurance Corporation (FDIC), I am pleased to present our Semiannual Report for the period October 1, 2024, to March 31, 2025. During the past 6 months, we have conducted important oversight work on behalf of the American people, a sampling of which is presented in this report. Our impact is strongly felt both in the internal operations of the FDIC and in the financial services industry at large. With the pace of change throughout the Federal government, the past several months have introduced challenges for our workforce. Still, results from this semiannual reporting period attest to the significant contributions and positive impact we continue to make.

We issued 4 audit and evaluation products with 21 recommendations to the FDIC designed to strengthen controls to address identified risks. Among the most important was Part 1 of our Special Inquiry report on the FDIC's Workplace Culture where we made six recommendations regarding the FDIC's efforts to improve its workplace culture by setting a tone at the top where all FDIC executives model the FDIC's core ethical values. We also issued a Material Loss Review on the failure of Republic First Bank, which failed in April 2024, causing an estimated loss to the Deposit Insurance Fund (DIF) of \$667 million. That report contained four recommendations to improve the FDIC's supervision process and help prevent future losses to the DIF. With regard to resolutions, we made recommendations to improve operational readiness in a third report that covered the FDIC's readiness to resolve large regional banks prior to the unanticipated failures in Spring 2023 of Silicon Valley Bank, Signature Bank of New York, and First Republic Bank—three of the largest failures in FDIC history. And in March we issued our assessment of the Top Management and Performance Challenges facing the FDIC, highlighting the need to enhance the FDIC governance structure to address the challenges we identified.

As for Investigations, we are helping to maintain and preserve the integrity of the banking sector and to detect and deter financial fraud. Of note, we present results of three complex and varied cases from this reporting period involving Par Funding, American Express, and TD Bank, along with other successful outcomes. In brief, the former CEO of Par Funding was sentenced to 186 months for RICO conspiracy, securities fraud, obstruction of justice, tax violations, and related charges. In the case of American Express, it agreed to pay \$108.7 million to settle allegations of deceptive marketing and "dummy" account information. TD Bank was sentenced for Bank Secrecy Act and money laundering conspiracy violations and agreed to a \$1.8 billion resolution.

Overall, FDIC OIG investigations during the reporting period resulted in 64 indictments, 48 convictions, 62 arrests, and more than \$2.76 billion in fines, restitution ordered, and other monetary recoveries. These results include the FDIC OIG's efforts combatting fraud in the Federal government's COVID-19 pandemic response, which resulted in 13 indictments and informations, 11 arrests, and 20 convictions. Monetary benefits resulting from these types of cases alone this period totaled nearly \$44.9 million.

Importantly, our Office has also seen an increase in fraudulent scammers who prey on the public. We include a special feature in this report to alert readers about the nature and consequences of such scams, some of which have been perpetrated falsely using the names of FDIC and FDIC OIG officials or misrepresenting the FDIC name and logo. We reiterate that if consumers believe they have been victimized, they should contact our OIG Hotline.

Other priority areas of focus for our office during the reporting period include strengthening relations with partners and stakeholders, efficiently and effectively administering the OIG's IT and human resources, and promoting leadership and teamwork. We have also contributed substantially to the IG community and law enforcement partners, through engagement on Council of the Inspectors General on Integrity and Efficiency (CIGIE) Committees and Working Groups, and participation on financial crime task forces and law enforcement working groups throughout the country.

The OIG has undergone significant organizational change during the reporting period. We resumed full-time, in-office presence on February 24, 2025. Fourteen members of our office accepted the Deferred Resignation Program and 3 staff retired or took other positions, resulting in a 17-full time equivalent staff reduction overall. This has led to organizational restructuring and reassignment of certain key responsibilities.

At the same time and notwithstanding such organizational changes, we have continued to pursue our mission and to ensure we are prepared to effectively meet our oversight responsibilities. The OIG is firmly committed to sustained delivery of credible results that drive meaningful change, enhance integrity and accountability, and foster public trust in the FDIC.

In closing, I sincerely thank those who departed the OIG as of the writing of this report for their many years of dedicated and unwavering Federal service as well as their contributions to the success of our office. I am also grateful for the support of the Congress, the FDIC Board and management, and colleagues in the IG and law enforcement communities. I am especially proud of the accomplishments of our dedicated and resilient staff who tirelessly and passionately serve the American people.

/S/

Jennifer L. Fain
Inspector General
April 2025



Table of Contents

Inspector General's Statement	i
Acronyms and Abbreviations	2
Introduction and Overall Results	3
Audits, Evaluations, and Other Reviews	4
Investigations	16
Other Key Priorities	34
Cumulative Results	41
Reporting Requirements	42
Appendix 1 Information in Response to Reporting Requirements	44
Appendix 2 Information on Failure Review Activity	66
Appendix 3 Peer Review Activity	67
Congratulations	70

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



Acronyms and Abbreviations

AML	Anti-Money Laundering
ATO	Account Takeover
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
COVID-19	Coronavirus Disease 2019
DIF	Deposit Insurance Fund
DOJ	Department of Justice
ECU	Electronic Crimes Unit
EIN	Employer Identification Number
FBI	Federal Bureau of Investigation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FinCEN	Financial Crimes Enforcement Network
FRB	Federal Reserve Board
IG	Inspector General
IRS-CI	Internal Revenue Service-Criminal Investigation
IT	Information Technology
MLR	Material Loss Review
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
ORMIC	Office of Risk Management and Internal Control
PA DoBS	Pennsylvania Department of Banking and Securities
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
SBA	Small Business Administration
USAO	United States Attorney's Office
USSS	United States Secret Service



Introduction and Overall Results

The mission of the Office of Inspector General (OIG) at the Federal Deposit Insurance Corporation (FDIC) is to prevent, deter, and detect fraud, waste, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the Agency. Our vision is to serve the American people as a recognized leader in the Inspector General (IG) community: driving change and making a difference by prompting and encouraging improvements and efficiencies at the FDIC; and helping to preserve the integrity of the Agency and the banking system and protect depositors and financial consumers.

Our Office conducts its work in line with 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, 2024–March 31, 2025)	
Audit, Evaluation, and Other Products Issued	4
Recommendations	21
Investigations Opened	67
Investigations Closed	81
Judicial Actions:	
Indictments/Informations	64
Convictions	48
Arrests	62
OIG Investigations Resulted in:	
Special Assessments	\$14,800.00
Fines	\$1,435,434,478.40
Restitution	\$504,208,524.75
Asset Forfeitures	\$640,113,149.23
Criminal Penalty	\$77,696,000.00
Civil Penalty	\$108,700,000.00
Total	\$2,766,166,952.38
Referrals to the Department of Justice (U.S. Attorney and DOJ Antitrust)	63
Investigative Reports Referred to FDIC Management	15
Responses to Requests Under the Freedom of Information/Privacy Act	20
Subpoenas Issued	3



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 addressing control improvements needed in workplace culture, supervision, and resolutions. We made a total of 21 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. We issued one such material loss review (MLR) report this period.

If the losses to the DIF as a result of a failure are less than the material loss threshold, the FDI Act requires the Inspector General of the appropriate Federal banking agency to determine the grounds upon which the state or Federal banking agency appointed the FDIC as receiver and whether any unusual circumstances exist that might warrant an In-Depth Review of the loss. As of the end of the reporting period, we had one failed bank review ongoing, that of Pulaski Savings Bank, Chicago, Illinois. This bank failed on January 17, 2025, with losses to the DIF estimated at \$28.5 million.

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

Audits, Evaluations, and Other Reviews

Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct – Part 1

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.

Of significance, we issued our report on the results of the first three of four objectives in our Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct. The objectives were to determine (1) employee perceptions of the FDIC workplace culture with respect to harassment, or related misconduct, and management actions; (2) FDIC management's actions to review, process, and address complaints of harassment and related misconduct, including the management of related litigation; (3) FDIC executives' knowledge of harassment and related misconduct and what actions (if any) were taken in response; and (4) factual findings regarding selected allegations that senior officials personally engaged in harassment or related misconduct.

We found that a majority of FDIC employees who responded to a workplace culture survey that we administered 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 does 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 does not have clear policy, standards, and procedures for documenting the process that it followed to make disciplinary decisions.

FDIC executives have varying levels of knowledge regarding harassment and related misconduct complaints across the FDIC. Also, FDIC policies do not require allegations of harassment or related misconduct involving FDIC employees to be reported to the appropriate FDIC stakeholders.

We made six recommendations regarding the FDIC's efforts to improve its workplace culture by setting a tone at the top where all FDIC executives model the FDIC's core ethical values; including a mechanism to provide support and protection for employees who fear or experience retaliation; establishing an agreement with a third party to conduct investigations of complaints against senior FDIC officials; developing a process to periodically report complaints of harassment and related misconduct to appropriate FDIC stakeholders; restating FDIC employees' obligation to report allegations of misconduct; and including the OIG Hotline as an option for reporting misconduct.

The FDIC agreed with the recommendations and will take corrective action by June 30, 2025.

Our investigative work on objective four—that is specific allegations and complaints of harassment and related misconduct against several senior FDIC officials—remains ongoing.

Material Loss Review of Republic First Bank

On April 26, 2024, the Pennsylvania Department of Banking and Securities (PA DoBS) closed Republic First Bank and appointed the FDIC as receiver. On May 21, 2024 the FDIC estimated the final loss to the DIF to be approximately \$667.1 million.

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

Sikich found that the direct cause of Republic First Bank's failure was its determination that it could no longer hold its "held-to-maturity" debt securities to maturity, requiring the Bank to reclassify them as "available-for-sale" securities. Because of insufficient liquidity, the Bank then further determined it was "more-likely-than-not" that it would have to sell these securities before the recovery of the amortized cost, thereby requiring the Bank to recognize significant fair value losses in its net income. Once this occurred, the Bank became critically undercapitalized for PCA purposes and was closed by the PA DoBS. Sikich also found that the dysfunctional Board and management team was a significant contributing factor to the Bank's troubled condition, its inability to adjust strategies and address increasing risk, and its eventual failure.

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

- The FDIC's November 2023 visitation for Republic First Bank lacked documented support for its conclusions related to changes to the Management rating and a proposed FDIC enforcement action; and
- The FDIC's approval of the Bank's use of brokered deposits contributed to an increase in insured deposits of approximately \$300 million and that improvements to the FDIC's brokered deposit waiver process are needed to adequately assess risks to the DIF.

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

FDIC Readiness to Resolve Large Regional Banks

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

The objective of this evaluation was to assess the FDIC's readiness to resolve large regional bank failures under the FDI Act, prior to the failures of SVB, Signature, and First Republic.

We determined the FDIC's readiness to resolve large regional banks under the FDI Act was not sufficiently mature to facilitate consistently efficient response efforts in a potential crisis failure environment. We found that at the time of the Spring 2023 failures, the FDIC had not ensured that it fully met its human and technology resource needs or that it sufficiently coordinated resources among its divisions and offices. As a result, the FDIC did not satisfy the readiness activities for planning, training, exercises, evaluation, and monitoring consistent with best practices. The FDIC could have been more effective in demonstrating its readiness to resolve large regional bank failures by:

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

Improving operational readiness will enhance the FDIC's ability to conduct resolutions in the most efficient and effective manner, reduce strain on staff, and strengthen interdivisional relationships.

We made 11 recommendations to the FDIC to address the findings in our report. We recommended the FDIC take actions to: improve interdivisional coordination of human and information technology resources; complete or revise resolution guidance, plans, and agreements to address significant gaps; increase interdivisional coordination over planning and exercises; ensure regular training of key resolution staff; identify, prioritize, and track significant after-action review recommendations; conduct regular internal reviews of resolution planning activities; and implement a process to periodically assess its resolution readiness. The FDIC concurred with all of our recommendations and plans to complete corrective actions by June 30, 2026.

Top Management and Performance Challenges

Our Top Management and Performance Challenges document summarizes the most serious challenges facing the FDIC and briefly assesses the Agency's progress to address them, in accordance with the Reports Consolidation Act of 2000 and Office of Management and Budget Circular A-136 (revised August 10, 2021). The Top Challenges document that we issued in March 2025 was based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities. By statute, the FDIC OIG is required to include this assessment in the FDIC's Annual Report, which was issued on March 20, 2025.

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

We identified the following eight Top Challenges facing the FDIC.

1. Enhancing Governance

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

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

2. Establishing Effective Human Capital Management

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

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

3. Ensuring Readiness to Execute Resolution and Receivership Responsibilities

- Improving Planning for Large Regional Bank Resolutions and Orderly Liquidations

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

4. Identifying and Addressing Emerging Financial Sector Risks

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

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

5. Assessing Operational Resilience in the Financial Sector

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

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

6. Improving Contract Management

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

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

7. Ensuring Information Technology (IT) Security and Scalability

- Fostering IT Systems Security
- Providing IT Scalability During Crises

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

8. Guarding Against Harmful Schemes

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

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

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

Ongoing Work

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

- **Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct:** Work is ongoing on the fourth sub-objective of this assignment: (4) factual findings regarding selected allegations that senior officials personally engaged in harassment or related misconduct. (Note: As reported earlier, we have issued the results of the first three sub-objectives.)
- **The FDIC's Procurement of Resolution and Receivership Services:** Our objective is to determine whether the FDIC awarded certain resolution and receivership contracts in accordance with FDIC requirements, contract terms and conditions, and best practices for government contracting.
- **Significant Service Provider Examination Program:** Our objective is to determine the effectiveness of the FDIC's Significant Service Provider Examination Program in evaluating the risk exposure and risk management performance of Significant Service Providers and determining the degree of supervisory attention needed to ensure weaknesses are addressed and risks are properly managed.
- **Oversight of the Infrastructure Support Services Contract:** Our objective is to determine whether the FDIC provided effective oversight of the Infrastructure Support Services contract to ensure compliance with service level metrics, invoice review and approval procedures, and data protection and security controls.

- **Failed Bank Review of Pulaski Savings Bank, Chicago, Illinois:** Our 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.
- **Audit of Security Controls for a Cloud Platform and Application:** Our objective is to assess the effectiveness of security controls for a cloud platform and application.
- **Federal Information Security Modernization Act:** Our objective is to evaluate the effectiveness of the FDIC's information security program and practices.
- **FDIC's Student Residence Center:** Our objective is to assess the FDIC's efforts to determine the cost benefits of, and organizational risks associated with, operating the Student Residence Center.
- **Succession Management:** Our preliminary objective is to determine to what extent the FDIC has taken and sustained actions to address the risks related to succession management for key positions and roles and employee retention.

Peer Review of Amtrak OIG's Audit Function

Our Office of Audits reviewed the system of quality control for the audit organization of the National Railroad Passenger Corporation (Amtrak) OIG in effect for the year ended September 30, 2024.

A system of quality control encompasses Amtrak OIG's organizational structure, and the policies adopted, and procedures established to provide it with reasonable assurance of conforming in all material respects with Government Auditing Standards and applicable legal and regulatory requirements. The elements of quality control are described in Government Auditing Standards.

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.

Update on Issue Related to OIG Email Security

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

We noted that 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. This includes implementing effective processes for ensuring the confidentiality and timely receipt of OIG email from complainants, whistleblowers, and law enforcement partners to meet the OIG's mission and maintain its independence. The response included intended changes in technical and policy controls and IT infrastructure to mitigate the risks that we identified. We reported that the FDIC OIG was working with FDIC IT personnel to address our concerns.

On February 16, 2023, we received a written plan for modernizing the OIG's email infrastructure. Based on the OIG's feedback, an updated plan was provided to the OIG on March 31, 2023. The revised plan, broken into two phases, outlined the challenges, solutions, and milestones planned for 2023 and 2024 to modernize the FDIC and OIG email infrastructure. Phase 1 was planned to begin in the second quarter of 2023 and end in the fourth quarter of 2023. Phase 2 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 is on track for completion in 2024. Throughout the duration of this project, the OIG has requested updates concerning the completion of previously committed Phase 1 and Phase 2. We learned Phase 1 was mostly implemented. For Phase 2, the completion of the project could extend to 2025.

Timely implementation of both phases is critical to meet the OIG's mission and ensure the confidentiality and timely receipt of OIG email from complainants, whistleblowers, and law enforcement partners. We will continue to coordinate with the CIO on this matter and have a meeting planned for April 30, 2025 to further discuss the issues.

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 29 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 Control (ORMIC) to determine whether the OIG's recommended and agreed-upon corrective actions have been completed. In reviewing the status of these open recommendations, the OIG believes that 12 of the 29 should have been closed in a timelier manner. Eleven of the 12 are currently being worked on by the FDIC, and the closure form for the remaining recommendation is under review by the OIG. ORMIC had also indicated, as reported in our last semiannual report, that going forward, it would take steps to better ensure timely completion of outstanding OIG and Government Accountability Office recommendations.

To that end, ORMIC's newly created Power BI dashboard provides Senior Executives with greater insight into the status of all open recommendations (e.g., on-time, extension likely, past due). Additionally, ORMIC has worked with Divisions and Offices to establish interim milestones to track and monitor progress in closing recommendations that remain open beyond one year. According to ORMIC, these efforts are designed to better manage the FDIC's progress in completing corrective actions in a timely manner and reduce the likelihood that recommendations remain open beyond one year. The reduction from 44 reported in the previous semiannual report to 29 is a positive trend.

A listing of the 12 recommendations follows. The OIG will continue its efforts to ensure the timely implementation of all open recommendations.

With FDIC Management for Action

AUD-23-002, *FDIC's Security Controls Over Microsoft Windows Active Directory* (March 15, 2023)

Recommendation #12: Update and implement procedures to proactively update or replace operating systems before vendor support ends.

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.

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

Recommendation #7: Develop and implement a feedback process for external threat sharing activities.

Recommendation #8: Develop performance measures to assess the effectiveness of the FDIC's external threat and vulnerability information sharing activities.

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

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

Recommendation #1: Emphasize to examiners in the form of training and other internal communications the requirements around timely escalation of supervisory concerns in line with the FDIC's forward-looking approach to supervision.

Recommendation #2: Reiterate to examiners requirements around prompt communication of risk and supervisory results to bank management, emphasizing the significance of prompt communication over linear or chronological issuance of supervisory products.

Recommendation #5: Implement target metrics and monitor variances for key supervisory outputs consistent with requirements contained in Continuous Examination Process procedures, such as:

- a. Supervisory Plan percentage completed to actual percentage completed to identify and take timely corrective action when examination teams are not on track to achieve objectives detailed in annual supervisory plans.
- b. Target review start date to actual review start date to identify and take timely corrective action when examination teams are not on track to achieve objectives detailed in annual supervisory plans.
- c. Number of days elapsed between target review start date and exit meeting to expectation to identify and take corrective action when reviews are not being completed and informal results communicated to the bank timely.
- d. Number of days elapsed between target review start date and issuance of Supervisory Letter to expectation to identify and take corrective action when the results of reviews are not being completed and results communicated to the bank timely.
- e. Number of days elapsed between year-end and Report of Examination (ROE) issuance to expectation to identify and take corrective action when ROEs are not being completed and results communicated to the bank timely.
- f. Number of days elapsed between quarter-end and issuance of Ongoing Monitoring Reports to expectations to identify and take corrective action when ongoing monitoring is not being completed timely.

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

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

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.

EVAL-23-003, *FDIC Efforts to Increase Consumer Participation in the Insured Banking System* (September 13, 2023)

Recommendation #13: Develop clear guidance on running business reports out of Community Affairs Reporting and Events System, including the use of filters.

With the OIG

AUD-22-004, *The FDIC's Information Security Program – 2022* (September 27, 2022)

Recommendation #1: Address the 31 Plans of Action and Milestones identified as of June 21, 2022, associated with NIST SP 800-53 Rev. 5 control SI-2 (Flaw Remediation).

Investigations

As reflected in our second Guiding Principle, the **FDIC OIG investigates significant matters of wrongdoing and misconduct relating to FDIC employees, contractors, and institutions.** We do so by:

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

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

FDIC OIG investigations during the reporting period resulted in 64 indictments/informations, 48 convictions, 62 arrests, and more than \$2.76 billion in fines, restitution ordered, and other monetary recoveries. We opened 67 cases and closed 81 during the reporting period. We referred 15 investigative reports to FDIC management for action.

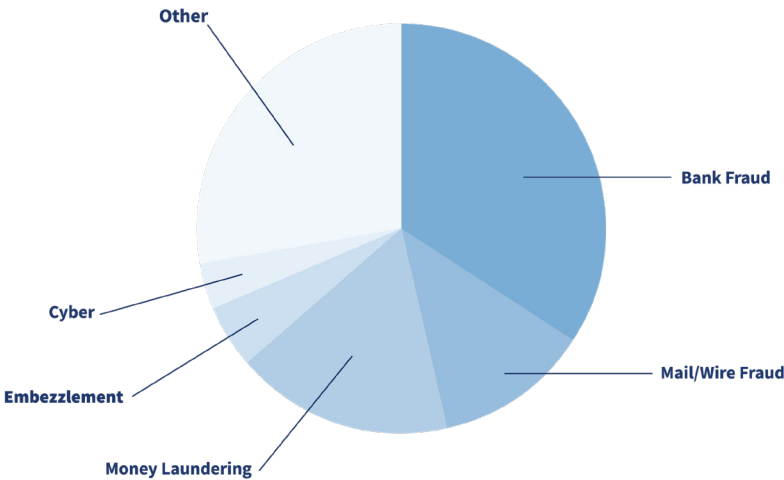


Office of Investigations engages in outreach regarding the OIG's mission and investigative impact.

Open Investigations

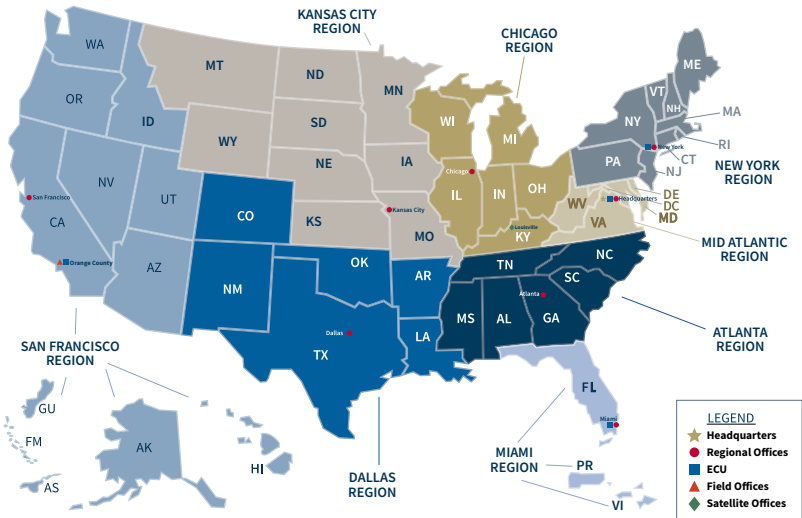
The FDIC OIG’s open investigations cover a wide range of allegations, as shown in the accompanying Figure.

Open Investigations – Allegations



Other includes the following: Abuse of Position, Conspiracy, Identity Theft, Elderly Fraud, Bank Secrecy Act Violations, Mortgage Fraud, Employee Cases, Ethics Violations, Conflicts of Interest, Misappropriation of Funds, Banking Client Fraud, Kickbacks, False Claims, Contract Fraud, False Personation, Bankruptcy Fraud, Misrepresentation of FDIC, False FDIC Affiliation, Theft of Government Property, Disclosure of Information, Drugs, Harassment, Anti-Trust Violations, Assault, and Foreign Corrupt Practices Act.

OIG Regional Map



Implementation of the OIG's Body Worn Camera Program

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

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 programs and operations. Investigative priorities include intrusions, cryptocurrency, impersonation, ransomware, Darkweb, business email compromises, and account takeovers targeting financial institutions. The ECU continues to focus on early-warning notifications to enable prompt and coordinated law enforcement responses to adversarial cyberattacks. (Learn more about the FDIC OIG ECU in a video on our website at www.fdicigoig.gov/oig-videos.)



IG recognizes the accomplishments of the OIG's ECU.

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 been working 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 201 such cases.

Notably, during the reporting period, the FDIC OIG's efforts related to the Federal government's COVID-19 pandemic response resulted in 13 charging actions (indictments, informations, and superseding indictments and informations), 11 arrests, and 20 convictions involving fraud in the CARES Act Programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases totaled \$44,858,009.

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 have hired in-house data science expertise – in order to marshal our resources and harness voluminous data.

During the reporting period, we migrated numerous mission critical data sets into the data lake to permit access to advanced analytical tools. In particular, the OIG has focused on access to data that assists in the prevention of commercial and residential real estate-related bank fraud. The OIG has finished deploying data management and query tools and is currently testing a suite of natural language processing tools--to be available in May--and generative artificial intelligence (AI) tools--to be available later this calendar year--to enhance our data analytic capabilities. Roughly one-third of the OIG completed dashboard and data visualization training over the last year. The OIG is also engaged in data analytics outreach and partnerships with CIGIE and recently presented a joint session at the 2025 FDIC Data Summit with the Financial Crimes Enforcement Network (FinCEN) from the Department of the Treasury. 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 (PRAC), the FDIC, FinCEN (as noted above), DOJ, FBI, and others. These efforts have resulted in expanded access to investigative data tools and capabilities for OIG investigations; identification of potential data sets relevant to OIG efforts; new opportunities for collaboration with external partners; identification of additional data analytics pilot projects; and information sharing agreements to help inform overall strategic planning within the OIG.

Case Highlights

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

As noted in our prior semiannual report, after conducting a peer review of OI, the Department of Veterans Affairs OIG reported that in its opinion, the system of internal safeguards and management procedures for the investigative function of 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.

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

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

On March 13, 2025, in the Eastern District of Pennsylvania, James LaForte, 48, of New York, New York, brother of Joseph LaForte, was sentenced to 137 months' imprisonment, followed by 3 years of supervised release to include 12 months' home confinement. In addition, he was ordered to pay \$2,488,645 in restitution, representing the portion of investor proceeds that he illegally diverted from Par Funding's numerous investors. James LaForte pleaded guilty in September 2024 to racketeering conspiracy, securities fraud, and extortionate collection of debt, as well as obstruction of justice, for his violent assault on one of the Par Funding receivership's Philadelphia attorneys, and retaliation, for threatening several government witnesses. In January 2025, the Court found the Par Funding fraud scheme caused an actual fraud loss of approximately \$404,000,000, which it reduced to \$288,395,088 after factoring in credit for collateral seized from Par Funding by federal authorities when the investigation became public in July 2020 when the Securities and Exchange Commission placed Par Funding in receivership.

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

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

Per the indictment, as part of their fundraising efforts, these defendants and their conspirators caused false and misleading information to be conveyed to investors regarding various issues, including, for example Joseph LaForte's true name, his role at Par Funding, and his criminal history; Par Funding's underwriting process; Par Funding's default rate; and Par Funding's financial success and profitability.

Although Joseph LaForte operated Par Funding and referred to it as his business, he concealed this ownership and control by using his wife as his nominee. Joseph LaForte also used several aliases while working at the company. It is alleged that Joseph LaForte, James LaForte, and their conspirators engaged in this deception to conceal Joseph LaForte's true role as the person operating the company and his significant criminal history from investors.

The indictment also alleged that Par Funding's principal means of generating income was to "advance" money to businesses that were in need of short-term financing at high rates of return. The indictment further alleged that the enterprise, including James LaForte, used threats of violence to collect money from customers whose payments were overdue. James LaForte, who was previously sentenced to 137 months imprisonment for his role in the scheme, threatened one particular Par Funding customer, telling him that he must repay the company immediately because James LaForte was not to be messed with and had previously torched people's cars and kicked people's teeth in.

Joseph LaForte and James LaForte also allegedly engaged in obstruction of justice in late February 2023 in connection with James LaForte's physical assault of one of the Par Funding receivership's attorneys outside of the attorney's office in Center City Philadelphia, sending the attorney to the hospital and causing serious bodily injury. Several days later, defendant James LaForte is alleged to have made threatening phone calls to several government witnesses and their family members, including Perry Abbonizio, who James LaForte knew had recently pleaded guilty to conspiring with Joseph LaForte in connection with the fraudulent operation of Par Funding.

Finally, Joseph LaForte and others were also previously charged with committing a variety of tax crimes involving the proceeds he received from Par Funding, including hiding tens of millions of taxable income via false entries on business and personal federal tax returns and pretending to live in Florida to avoid paying Pennsylvania income tax. In April 2024, Joseph LaForte's wife, Lisa McElhone, pleaded guilty in connection with the Florida residency scheme. It was further alleged that Joseph LaForte failed to report millions of dollars in cash kickbacks that he personally received from a Par Funding merchant customer, and by regularly paying cash wages to Par Funding employees but failing to withhold taxes from these wages or report them to the Internal Revenue Service (IRS).

Source: USAO, Eastern District of Pennsylvania

Responsible Agencies: FDIC OIG, FBI, and IRS-Criminal Investigation (IRS-CI).

Prosecuted by the USAO, Eastern District of Pennsylvania.

American Express Agrees to Pay \$108.7M to Settle Allegations of Deceptive Marketing and "Dummy" Account Information

On January 16, 2025, the American Express Company (American Express), agreed to pay a \$108.7 million civil penalty to resolve allegations that it violated the Financial Institutions Reform, Recovery, and Enforcement Act by deceptively marketing credit card and wire transfer products and by entering "dummy" Employer Identification Numbers (EINs) in the credit card accounts of its affiliate bank. Contemporaneous with the civil resolution, American Express entered into a Non-Prosecution Agreement (NPA) with the U.S. Attorney's Office for the Eastern District of New York and agreed to pay a criminal fine and forfeiture. Under the terms of the NPA, American Express will pay a criminal fine of \$77,696,000 and forfeit a total of \$60,700,000.

The U.S. alleged that, from 2014 through 2017, American Express deceptively marketed credit cards through the conduct of an affiliated entity that initiated sales calls to small businesses. Alleged deceptions included misrepresenting the card rewards or fees and whether credit checks would be done without a customer's consent and submitting falsified financial information for prospective customers, such as overstating a business's income.

The U.S. also alleged that American Express engaged in practices to deceive its federally insured financial institution (American Express National Bank) into allowing certain small business customers to acquire American Express credit cards without the required EINs. EINs are required by law if the card recipient is a business entity such as a corporation or partnership; the requirement does not apply to sole proprietors. The U.S. alleged that American Express employees used "dummy" EINs such as "123456788" in opening small business credit cards in 2015 and the first half of 2016. These cards were sold to replace an American Express co-branded credit card that was being discontinued during that time period. American Express allegedly allowed these "dummy" EINs to remain on the credit card accounts for up to 2 years before remediating the problem. American Express allegedly knew that many of the small business applicants had previously acquired American Express-issued co-brand cards where the card application stated that EINs were required for corporations or partnerships, but if the applicants left the EIN line blank, American Express would assume they were sole proprietors. That practice exacerbated the effects of American Express's failure to enter proper EINs when it sold these customers replacement cards.

Finally, the U.S. further contended that American Express employees deceptively marketed wire transfer products known as Payroll Rewards and Premium Wire to its small business customers from 2018 through 2021, making false assertions regarding these products' tax benefits. As to both products, American Express allegedly would wire money for an above-market fee that was far in excess of that offered by competitors in the marketplace and award the businesses or the business owners credit card membership reward points. American Express sales employees allegedly told customers that the wire transfer fees were tax deductible as business expenses, while the reward points earned on the transaction were not taxable, and thereby afforded the customer tax-free benefits. The U.S. contended, however, that the above-market wiring fee was not deductible as an ordinary or necessary business expense insofar as it was incurred by a customer solely for the purpose of generating a personal benefit.

Source: DOJ, Civil Division.

Responsible Agencies: FDIC OIG, Treasury OIG, and the Board of Governors of the Federal Reserve System and Consumer Financial Protection Bureau OIG. Handled by DOJ's Civil Division, Commercial Litigation Branch, Fraud Section.

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

On November 7, 2024, TD Bank N.A. (TDBNA), the 10th largest bank in the U.S., and its parent company TD Bank US Holding Company (TDBUSH) (together with TDBNA, TD Bank) were sentenced to 5 years of probation. The judge accepted all the terms of the plea agreement and TDBNA was ordered to pay a \$500,000 fine and \$400 special assessment. TD BUSH was ordered to pay a special assessment of \$800 and was given a credit to the criminal fine in the amount of \$500,000 for the special assessment of TDBNA and \$5.5 million claw back credit. As part of the plea agreement, TD Bank has agreed to forfeit \$452,432,302.00 and pay a criminal fine of \$1,434,513,478.40, for a total financial penalty of \$1,886,945,780.40. TD Bank has also agreed to retain an independent compliance monitor for three years and to remediate and enhance its Anti-Money Laundering (AML) compliance program. TD Bank has separately reached agreements with the Federal Reserve Board (FRB), Office of the Comptroller of the Currency, and FinCEN, and the DOJ will credit \$123.5 million of the forfeiture toward the FRB's resolution.

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

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

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

TD Bank's AML failures made it "convenient" for criminals, in the words of its employees. These failures enabled three money laundering networks to collectively transfer more than \$670 million through TD Bank accounts between 2019 and 2023. Between January 2018 and February 2021, one money laundering network processed more than \$470 million through the bank via large cash deposits into nominee accounts. The operators of this scheme provided TD Bank employees gift cards worth more than \$57,000 to ensure employees would continue to process their transactions. And even though the operators of this scheme were clearly depositing cash well over \$10,000 in suspicious transactions, TD Bank employees did not identify the conductor of the transaction in required reports. In a second scheme between March 2021 and March 2023, a high-risk jewelry business moved nearly \$120 million through shell accounts before TD Bank reported the activity. In a third scheme, money laundering networks deposited funds in the U.S. and quickly withdrew those funds using ATMs in Colombia. Five TD Bank employees conspired with this network and issued dozens of ATM cards for the money launderers, ultimately conspiring in the laundering of approximately \$39 million. The DOJ has charged over two dozen individuals across these schemes, including two bank insiders. TD Bank's plea agreement requires continued cooperation in ongoing investigations of individuals.

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

Source: Request for assistance from the USAO, District of New Jersey, and IRS-CI.

Responsible Agencies: FDIC OIG, IRS-CI, and Drug Enforcement Administration.

Prosecuted by the USAO, District of New Jersey, and the Money Laundering and Asset Recovery Section (MLARS) of the DOJ.

California Couple Sentenced for Defrauding Paycheck Protection Program

On January 9, 2025, Christopher A. Mazzei and Erin V. Mazzei both of Arroyo Grande, California, were sentenced to 36 months and 27 months of imprisonment, respectively, for conspiracy to commit wire fraud and conspiracy to commit money laundering in connection with a scheme to defraud the government of forgivable Paycheck Protection Program (PPP) loan funds intended for Coronavirus-related relief. The Mazzeis pleaded guilty to two counts of the Indictment on August 28, 2024.

The two fraudulently obtained COVID-19 benefits from the PPP by submitting false and fraudulent loan applications and supporting documents on behalf of three companies they owned (Better Half Productions, Inc., Better Half Entertainment, LLC, and Gusto on the Go, LLC). The Mazzei's also concealed the fact that they were submitting multiple PPP loan applications. As a result of the scheme, they fraudulently obtained approximately \$1,365,000 in PPP funds to which they were not entitled. They used the fraud proceeds to pay personal expenses and investment in an unallowable business venture.

The Mazzeis also consented to a forfeiture money judgment in the amount of \$1,365,332 and agreed to the forfeiture of a property in Kapolei, HI, a property in Arroyo Grande, CA, \$583,993.60 in cash previously seized from two bank accounts, and \$42,000 representing the proceeds of the sale of a 2019 Ford Expedition registered to Erin Mazzei. The seizures resulting from the investigation total \$2,421,374.37. The seized funds exceed the value of the fraudulent PPP loans received by the Mazzeis because the Mazzeis also engaged in bank/mortgage fraud activity as part of their scheme. The Mazzeis were not charged with bank/mortgage fraud, but the plea agreement stipulated that the Court could consider the events underlying those potential charges for sentencing purposes.

Source: USAO, District of Hawaii.

Responsible Agencies: This is a joint investigation with FDIC OIG, FRB OIG, Treasury Inspector General for Tax Administration, and IRS-CI.
Prosecuted by the USAO, District of Hawaii.

California Man Sentenced in Fraud Scheme

On November 25, 2024, Brett Bartlett was sentenced to 188 months in prison, ordered to pay \$22,502,093 in restitution, and serve 3 years of supervised release for his investment fraud scheme which defrauded over 1,000 victims.

From May 2015 to August 2020, Bartlett used his businesses, 7M-E Group Corporation (7M-E) and Dynasty Toys, Inc. (Dynasty), to purchase items at liquidation sales, which he then sold online for profit. Bartlett solicited individuals to invest in these companies by promising annual returns of 20 percent to 40 percent. Notably, Bartlett marketed his businesses as a faith-based family business and, consequently, recruited dozens of investors through his connections with a church in central Illinois. In order to execute his scheme, Bartlett made false claims to investors regarding the past, current, and future financial success of the companies; inflated the annual returns in his financial reporting to the investors; and claimed that Dynasty had millions of dollars in gold assets. In total, Bartlett recruited approximately 1,000 investors who invested over \$20 million in these businesses, a portion of which was used on personal expenses. In May 2020, while Bartlett's businesses were failing, he mailed payout checks drawn on a Bank of America account to investors totaling millions of dollars, even though there was less than \$10,000 in the account.

On May 2, 2023, Bartlett, along with his businesses, 7M-E and Dynasty, were indicted on three counts of wire fraud, one count of mail fraud, one count of securities fraud, and one count of money laundering. On the same date, the Securities and Exchange Commission filed a complaint regarding the same conduct. On April 29, 2024, Bartlett pleaded guilty to all six counts in the Indictment.

Source: USAO, Central District of Illinois.

Responsible Agencies: FDIC OIG and the FBI.

Prosecuted by the USAO, Central District of Illinois.

Bank Customer Sentenced for Fraud Related to Pandemic Relief, Cattle Theft, and Bankruptcy Fraud

On October 10, 2024, Michael Butikofer was sentenced in the Northern District of Iowa to 188 months imprisonment, 3 years supervised release, and ordered to pay restitution in the amount of \$5,765,594.85. Butikofer previously pleaded guilty to one count of theft of livestock, one count of wire fraud, and one count of providing a false bankruptcy declaration. This investigation involved other allegations of fraud, to include bank fraud, that were ultimately not charged as part of Butikofer's guilty plea.

Butikofer operated a large farming operation in Northeastern Iowa. Between July 2020 and February 2022, he misappropriated the proceeds from the sale of cattle owned by six cattle investors for his personal use. Butikofer previously convinced the cattle investors to allow him to sell the cattle in his own name. When Butikofer sold the cattle, he falsely represented to the slaughterhouse that he owned the cattle outright, when in fact he did not.

Between July 2020 and August 2020, Butikofer also defrauded the U.S. Department of Agriculture of more than \$1.2 million in emergency assistance funds designed to assist livestock producers during the COVID-19 pandemic. Specifically, fraudulent applications were made to the Coronavirus Food Assistance Program in another person's name. Butikofer used the fraudulently obtained funds for his personal use.

In February 2022, Butikofer received over \$1.5 million from the Small Business Administration (SBA) for an Economic Injury Disaster Loan. Butikofer falsely stated to the SBA that he would use the proceeds as working capital to alleviate economic injury caused by the COVID-19 pandemic. However, upon receiving the \$1.5 million from the SBA, Butikofer again used the funds for his personal use.

In March 2022, Butikofer submitted a false and fraudulent statement of financial affairs in his bankruptcy case. In April 2022, Butikofer falsely testified under oath at a meeting of creditors and, in November 2022, repeatedly committed perjury before the bankruptcy court when asked questions about his cattle operation.

Source: SBA.

Responsible Agencies: FDIC OIG, SBA OIG, Department of Labor OIG, Homeland Security Investigations and USDA OIG.

Prosecuted by the USAO, Northern District of Iowa.

Miami Subject Sentenced for Role in \$65 Million International Account Takeover Scheme

On November 8, 2024, Collins Chike Oleh was sentenced in the Southern District of Florida to 84 months in prison, to be followed by 3 years of supervised release, for his role in a \$65 million international Account Takeover (ATO) scheme involving over 200 victims and at least six FDIC insured institutions. In addition, Oleh was ordered to pay \$2.2 million in restitution. Oleh previously pleaded guilty on August 18, 2024, to one count of conspiracy to commit money laundering.

Oleh was a co-conspirator in an approximate \$65 million international ATO scheme. He coordinated the recruitment of money mules who were instructed to open, and/or provide, bank accounts for the purpose of receiving victim funds which were stolen during the course of a \$65 million international ATO that spanned approximately 3 years. Upon receipt of stolen victim funds into the mule bank accounts via wire transfer, Oleh would physically escort mules to their respective financial institutions and instruct them to enter the bank, withdraw the stolen funds, and give the funds to Oleh and/or one of his co-conspirators. In return, the mules were promised a small percentage of the funds withdrawn. Oleh is one of multiple defendants in this investigation.

Source: The United States Secret Service (USSS).

Responsible Agencies: FDIC OIG and USSS.

Prosecuted by the USAO, Southern District of Florida.

Former Bank Senior VP and Commercial Loan Officer Sentenced

On December 13, 2024, in the Western District of Oklahoma, John Padilla, a former senior vice president and commercial loan officer at BancFirst in Lawton, Oklahoma, was sentenced to 16 months in prison, followed by 3 years of supervised release, and ordered to pay restitution of \$1,092,135.50. Padilla previously pleaded guilty to one count of bank fraud.

In carrying out the alleged scheme, Padilla recruited borrowers to apply for loans from BancFirst that were under his delegated loan authority of \$350,000. Most of these borrowers were not creditworthy and would not have been approved for the loans, but for Padilla approving them. Many of these borrowers were Padilla's friends and associates. Padilla explained to them he would use the loan proceeds to invest in his real estate venture and then pay the borrowers a percentage of the profit. Padilla also assured these borrowers he would make all the payments toward the outstanding balance on each loan and listed collateral on these loan applications that did not exist. Additionally, in the event the borrower did own certain collateral, Padilla would often list this collateral on the loan applications without disclosing to the borrower that the loan was being secured with that collateral.

Padilla often waived the credit report for these borrowers, misrepresented the purpose of the loan, and used most of the loan proceeds to support his personal gambling habit. The loan disbursements were mostly issued via cashier's checks to the borrowers. Subsequently, the borrowers were instructed to obtain additional cashier's checks and to make the checks payable to another individual Padilla knew. Padilla opened a joint bank account with that other individual so Padilla could have the loan proceeds deposited into a bank account he controlled. Padilla also used loan proceeds from unauthorized loans he approved to make payments toward earlier unauthorized loans he approved, thus enabling the scheme to continue undetected. Padilla's scheme caused a loss to BancFirst of approximately \$1,092,135.50.

Source: FDIC's Division of Risk Management Supervision.

Responsible Agencies: FDIC OIG and Federal Housing Finance Agency OIG.

Prosecuted by the USAO, Western District of Oklahoma.

Former CEO of Mariner's Bank Sentenced

On March 7, 2025, Fred Daibes was sentenced to 37 months imprisonment to be followed by 2 years of supervised release. Additionally, Daibes was ordered to pay a fine of \$300,000. Daibes previously pleaded guilty to making false entries (18 U.S.C. § 1005) stemming from a nominee loan scheme to obtain a \$1.8 million loan from Mariner's Bank for his benefit.

Daibes is the Former CEO and Chairman of the Board of Directors at Mariner's Bank. He falsely stated that a \$1.8 million line of credit was for the benefit of a nominee borrower on a Mariner's Bank loan memorandum dated June 11, 2008 when in fact the line of credit was for his own benefit. Further, the memorandum falsely stated that the source of repayment would be the personal cash flow of the nominee borrower even though Daibes would and did fund the payments on the line of credit.

Source: Based on a referral from a financial institution.

Responsible Agencies: FDIC OIG, FBI, and agents from the USAO, New Jersey.

Prosecuted by the USAO, District of New Jersey.

Special Feature

Beware of Scams

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

Common Schemes

The four most common types of schemes that have been reported to the OIG have included relationship scams, investment scams, government impersonation scams, and business email compromise scams. In a relationship scam, a scammer adopts a fake online identity to gain a victim's affection and trust and then uses the illusion of a romantic or close relationship to manipulate the victim. In an investment scam, a scammer offers low- or no-risk investments, guaranteed returns, and complex strategies to manipulate or steal from the victim. These two scams are often associated with "Pig Butchering" schemes—a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally in the form of cryptocurrency, to a seemingly sound investment before the scammer disappears with the contributed monies.

Recent OIG investigations have also revealed that government impersonation scams to manipulate or steal from consumers are increasingly common and often take the form of unsolicited phone calls, text messages, or e-mails that claim to be from the FDIC or FDIC OIG. Fraudsters may use the FDIC or OIG's seal or logo, and even names of actual employees, to make their demand for funds seem legitimate.

- In cases of FDIC impersonation, scammers may contact an individual and claim that the individual has been awarded a grant or a sum of money, and the scammers may request personal information, such as bank account or credit card details, or ask for money or gift cards. These schemes often require an advance payment, which is a warning sign.
- For FDIC OIG impersonations, scammers may contact an individual pretending to be OIG personnel, sometimes using the names of Special Agents to lend credibility to their claims. They might inform the recipient that they are under investigation and must pay a fee or fine to avoid arrest. The fee or fine is frequently requested to be paid through gift cards or other forms of payment.

Yet another type of payment scam is known as a business email compromise scam. The scammer targets a business or individual and takes over an official account, or uses email spoofing, to attempt to redirect legitimate payments to an illicit account controlled by the scammer to steal from the victim.

Special Feature

Addressing Misuse of the FDIC Name and Logo

Section 18(a)(4) of the FDI Act specifically prohibits any person from harming consumers by misusing the FDIC name or logo or making misrepresentations about deposit insurance. The FDIC may investigate any claims under this section and may issue administrative enforcement actions, including cease and desist orders, and impose civil money penalties against perpetrators. As of December 31, 2024, the FDIC had received 1,200 misrepresentation allegations through its portals, which is a 60-percent increase from the 750 allegations received in 2023. The FDIC has issued public cease and desist orders for some of these violations, and the FDIC's Legal Division, working with other stakeholders, including the OIG, has initiated the take-down of websites determined to be fraudulent and made referrals to appropriate agencies.

Efforts to protect consumers from fraudulent schemes and misrepresentations can help protect taxpayer savings, provide them with trusted financial products and services, and foster public confidence in the FDIC.

If you believe you have been the victim of such schemes, contact the [OIG Hotline](#).

SCAM ALERT: "PIG BUTCHERING"

HAVE YOU EVER RECEIVED AN UNEXPECTED TEXT OR DIRECT MESSAGE FROM A STRANGER?



DON'T RESPOND!

It might be the first step in a Pig Butchering Scam. Don't be the next victim.

What You Need to Know About a Fast-Growing Scam Known as "Pig Butchering"

This scam is named in reference to the practice of fattening a pig before slaughter. It is a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally in the form of cryptocurrency, to a seemingly sound investment before the scammer disappears with the contributed monies.

Beware!!! This is how it works:

- Perpetrators will contact you out of nowhere via text messages, dating apps, social media platforms, and later switch to VOIP chat applications.
- Perpetrators will try to develop meaningful relationships with you, gain your trust, and offer you high-yield investment opportunities in virtual assets, such as cryptocurrency.
- Perpetrators will tell you to open accounts on online investment websites and instruct you to deposit money via wire transfer to shell companies, or direct transfers on legitimate virtual asset service providers (VASPs) or cryptocurrency exchanges.
- Perpetrators will pressure you to invest more money, or your relationship with them will end.
- You can be duped and the fraud will end: When you attempt to withdraw money, websites may demand that you pay additional fees to do so, or you may be locked out of the account and never hear back from the perpetrator. Perpetrators disappear with all of your funds.

REPORT: If you suspect you are a victim of a Pig Butchering Scam, notify your bank immediately. Contact your local police department and file a police report. File a complaint on the FBI's Internet Crime Complaint Center (IC3): <https://www.ic3.gov>.



SCAM ALERT: "PIG BUTCHERING"

Beware. THIS SCAM CAN CAUSE SERIOUS HARM TO YOUR BANK AND YOUR CUSTOMERS!

This scam is named in reference to the practice of fattening a pig before slaughter. It is a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally in the form of cryptocurrency, to a seemingly sound investment before the scammer disappears with the contributed monies.



How the Scam Works:

- Perpetrators contact victims at random via text messages, dating apps, social media platforms, and later switch to VOIP chat applications.
- Perpetrators develop meaningful relationships with victims, gain their trust, and offer them high-yield investment opportunities in virtual assets, such as cryptocurrency.
- Perpetrators tell victims to open accounts on online investment websites and instruct them to deposit money via wire transfer to shell companies, or direct transfers on legitimate virtual asset service providers (VASPs) or cryptocurrency exchanges.
- Perpetrators pressure victims to invest more money, or the relationship will end.
- Victims are duped and the fraud ends: When a victim attempts to withdraw money, websites may demand that victims pay additional fees to do so; other victims are locked out of the account and never hear back from the perpetrator. Perpetrators disappear with all of the victim's funds.

What to Watch For: "Red Flags"

- A customer with no prior interactions with virtual exchanges suddenly exchanges large sums of fiat currency from their bank account for virtual currency or transfers money to VASPs.
- A customer's account shows frequent and large withdrawals of money or multiple wire transfers to a VASP when in the past, there was limited or no activity in the account.
- A customer appears distressed or anxious to access funds immediately to meet the timeline of a virtual currency investment opportunity or a bank receives calls from a victim requesting the cancellation of a transfer.

What to Do: Mitigate Your Risk!

- Focus on "Know Your Customer" (KYC) requirements: Do the businesses and individuals have websites? Are they registered with the appropriate state and federal compliance office?
- Immediately freeze accounts and conduct compliance checks: Follow up with account owners who you suspect to be victims. Justify the origin of the money. Request supporting documentation, such as invoices for services provided.
- Contact recipients of outbound transactions: Ensure transfers are for legitimate purposes.

REPORT: File a Suspicious Activity Report (SAR) and 314(b) filings. Financial institutions are encouraged to refer their customers who may be victims of Pig Butchering Scams to their local police department to file a police report and to file a complaint on the FBI's Internet Crime Complaint Center (IC3): <https://www.ic3.gov>.



Office of Inspector General ALERT

Federal Deposit Insurance Corporation



Beware of Impersonation Scams Claiming to be from the FDIC or FDIC OIG

Unsolicited phone calls, text messages, or e-mails purporting to be from the Federal Deposit Insurance Corporation (FDIC) or the FDIC Office of Inspector General (OIG) may be fraudulent.

Types of Impersonation Scams

FDIC Impersonation

Scammers may contact an individual and assert that the individual has been awarded a grant or a sum of money, and the scammers may then request personal information (such as bank account or credit card information), money, or gift cards. We urge recipients of such calls or e-mails that demand a fee for release of funds to be especially wary of any such scheme requiring an advanced payment.

FDIC OIG Impersonation

Scammers may contact an individual claiming to be FDIC OIG personnel, sometimes utilizing the names of Special Agents to add an appearance of legitimacy to the scam. They may also indicate that the recipient of the call or message is under investigation and must pay a fee or fine in order to avoid being arrested. The fee or fine is often requested to be paid in the form of gift cards or other forms of payment.

Scammers purporting to be from the FDIC or FDIC OIG may use the FDIC or FDIC OIG's seal or logo to make their demand for funds appear to look legitimate. **The FDIC and FDIC OIG will not send unsolicited correspondence asking for sensitive personal information or demanding payment through gift cards, wire transfers, or digital currency.**

Contact the OIG Hotline

If you have been a victim of such scams or have questions about any unsolicited correspondence, please contact the FDIC OIG Hotline.

www.fdicig.gov/oig/hotline

1-800-964-FDIC

3503 Fairfax Drive - Room VS-0-909 - Arlington, VA 22226

The OIG reviews all allegations and will investigate a matter in appropriate circumstances. Individuals contacting the Hotline via the website can report information openly, confidentially, or anonymously.



Alerts posted at fdicoig.gov warn the public of fraudulent scams.

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 38 locations in the U.S.

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

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



Keeping Current with Criminal Activities Nationwide

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

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



Other Key Priorities

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

Strengthening relations with partners and stakeholders.

- Communicated with the FDIC Chairman, other FDIC Board Members, Chief Operating Officer, Chief Financial Officer, and other senior FDIC officials through the IG's and senior OIG leadership's 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 Vice Chairman, in his capacity as Chairman of the FDIC Audit Committee, to provide status briefings and present the results of completed audits, evaluations, and related matters for the Audit Committee Chairman's and other Committee members' consideration. Presented the results of OIG audits, evaluations, and other reviews at two scheduled Audit Committee meetings. Apprised the Chairman and other internal Board Member accordingly.
- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them informed of ongoing OIG reviews, results, and planned work.
- Continued to enhance our external website and other social media presence to provide stakeholders better opportunities to learn about the work of the OIG, the findings and recommendations our auditors and evaluators have made to improve FDIC programs and operations, the results of our investigations into financial fraud, and helpful information to guard against ever-evolving scams.
- 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 any Congressional correspondence pertaining to the OIG.
- Briefed Senate Majority staff regarding the steps the FDIC OIG is taking "to ensure all current and former FDIC employees responsible for creating the extremely toxic workplace culture at the agency are fully investigated," as requested by several Senators in a November 14 letter to our office.
- Briefed House Oversight and Government Reform Minority staff on the FDIC OIG's Special Inquiry Report.
- Held an introductory meeting with Majority staff from the House Financial Services Subcommittee on Financial Institutions and Monetary Policy regarding the OIG, our mission, and the overall nature of our work.
- 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.fdicioig.gov/oig-hotline> integrates seamlessly with our electronic investigative management system and 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 432 Hotline inquiries, 24 of which led to our opening investigations. Our on-line form, email, telephone, and regular mail were the most common vehicles for inquiries.
- Posted a Scam Alert and accompanying visual on our website highlighting impersonation schemes whereby imposters claim to be FDIC or FDIC OIG employees to gain personal information from unsuspecting victims. Also reiterated warnings about "pig butchering" as part of National Consumer Protection week. This scam is named in reference to the practice of fattening a pig before slaughter. It is a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally in the form of cryptocurrency, to a seemingly sound investment before the scammer disappears with the contributed monies. Supported efforts of the Social Security OIG in National Slam the Scam Day in March as well.
- Participated on the PRAC's Law Enforcement Coordination Subcommittee. The Subcommittee assists OIGs in the investigation of pandemic fraud; serves as a coordinating body with DOJ prosecutors, the FBI, and other Federal law enforcement agencies; and enables OIGs to tap into criminal investigators and analysts from across the OIG community to help handle pandemic fraud cases.

- Supported the broader IG community by attending monthly CIGIE meetings and other meetings, such as those of the CIGIE Legislation Committee; Audit Committee; Inspection and Evaluation Committee, Technology Committee; Investigations Committee; Professional Development Committee; Assistant IGs for Investigations; and Council of Counsels to the IGs; responding to multiple requests for information on IG community issues of common concern; and monitoring various legislative matters through CIGIE's Legislation Committee.
- 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, 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.
- 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, including the OIG's March issuance of the Top Management and Performance Challenges document.
- Coordinated with the Office of Management and Budget to address matters of interest related to our FY 2025 budget and proposed budget for FY 2026.
- 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.)
- Promoted transparency to keep the American public informed through four main 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, and 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.
- Took action in response to the OIG's internal stakeholders—our staff—based on a survey administered by our Office of Management. Provided the feedback received from the survey and the responsive steps OM would take in the interest of delivering high-quality services to meet the needs of the OIG and support its mission.

Administering resources prudently, safely, securely, and efficiently.

- Proposed a budget of \$55.4 million for FY 2026 – approximately 5.3 percent above the OIG's budget request for FY 2025 of \$52.6 million. This amount would help sustain prior investments in information technology and data analysis and support critical OIG contractual audit services focused on cyber security and statutorily mandated reviews of failed banks. With the requested amount of \$55.4 million, the OIG can maintain its current level of oversight, while enhancing and advancing its mission to improve the FDIC's programs and operations through independent and objective audits, evaluations, and investigations.
- Held an informative session for OIG staff upon our return to office full-time, discussing our emergency preparedness posture, shelter-in-place guidance, and communications and procedures in the event of an emergency at the OIG's Virginia Square headquarters.
- Made progress in building a dashboard to display key metrics and performance indicators for OIG leadership. The data in the dashboard will help inform the OIG's strategic plan, staffing plans, and the effective management of our budget and human capital resources.
- Carried out a number of IT initiatives, including the following: developed dashboards to better track resource onboarding and offboarding; completed Windows 11 laptop deployment and training; took ownership and started restructuring eDiscovery processes within the OIG; developed three applications on the Power Apps platform to automate OIG processes for document approvals, procurement card requests, and training requests; enhanced the OIG's security posture by modernizing authentication and facilitating improvements to the FDIC identity management platform; integrated case management data into dashboards for investigators' and auditors/evaluators' use and included key metrics to improve decision-making; established a modernization strategic plan for OI's ECU Forensic Lab environment; and revised security policy and log aggregation queries to better align with current circumstances and started implementing proactive approaches to identifying threats and vulnerabilities.

- Leveraged the OIG ECU's forensic laboratory. The laboratory allows 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. The build-out of the ECU has also facilitated financial fraud investigations, including cybercrimes at banks.
- Continued to pursue OIG data management strategies and solutions. Auditors, criminal investigators, and information technology professionals are seeking to ensure that we are leveraging the power of data analytics to inform organizational decision making and ensure we are conducting the most impactful audits, evaluations, reviews and investigations. The OIG continues to migrate mission critical datasets into the data lake, supporting both audits and investigations. In particular, the OIG has focused most recently on access to data that assists in the prevention of commercial and residential real estate-related bank fraud. Currently, all OIG employees can access cloud-based data management software, and we are currently testing generative AI tools that will be available later this calendar year. Roughly one-third of the OIG completed dashboard and data visualization training over the past six months. 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 PPP fraud through collaboration with the PRAC, the FDIC, FinCEN, DOJ, the FBI, and private-sector entities. Additionally, the OIG is expanding our use of commercially available data to detect bank fraud and threats to the integrity of the banking system.
- Updated the OIG's intranet site and explored additional options to enhance the site's usability and increase collaboration, and to provide component offices more control over and access to information, guidance, and procedures, to better conduct their work in the current operating environment.
- Relied on the OIG's General Counsel's Office to ensure the Office complied with legal and ethical standards, rules, principles, and guidelines; provide legal advice and counsel to teams conducting audits, evaluations and other reviews; and support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.
- Continued to review and update a number of OIG internal policies related to audit, evaluation, investigation, operations, and administrative processes of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the Office. We reviewed or updated several OIG-specific internal operating procedures, including those for Professional Liability Insurance, a Drug Free Workplace, Telework, and Distinguished Achievement Awards.
- Refined the OIG's personnel policy on hiring authorities, procedures, and staffing plans, to ensure controls and efficiencies throughout the process.

- Held a number of information sessions sponsored by our Office of Management and the OIG's Human Resources staff to keep staff informed of important topics such as procurements, the OIG budget process and updates, personnel benefits, open season selections, data analytics, training, facilities issues, and IT matters.
- 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.
- Continued to integrate and leverage the use of MS Teams throughout our Office to promote virtual collaboration and communication.

Exercising leadership skills and promoting teamwork.

- Held a Town Hall meeting in October, during which updates from each component office were shared, and the IG presented her thoughts on the OIG's role in serving the public, and the mission, vision, and values of our office.
- Represented the FDIC OIG on the Council of Inspectors General on Integrity and Efficiency. The FDIC IG is currently Chair of the Audit Committee. Related to the Committee, our former Assistant Inspector General for Audits, Evaluations, and Cyber served as the Federal Audit Executive Council's Chair up until her departure from our office, and we continue to support the efforts of that Council.
- Held a learning forum for the OIG's auditors and evaluators, the theme of which was "Acknowledging, Empowering, Connecting." Staff heard from the IG and certain FDIC Division Directors. The Division of Administration presented on employee life and career development. The OIG's Training Officer facilitated a session on organizational systems. Another session called, "Working by Design," was intended to build common ground in working together. Audit and evaluation managers and project leads attended a workshop, "Building Common Ground," to foster open communication, trust, resilience, and collaborative problem-solving. The goal was to build a high-performing team capable of navigating difficult conversations, ensuring accountability, and creating an engaged and synergistic work environment.
- 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.
- 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.

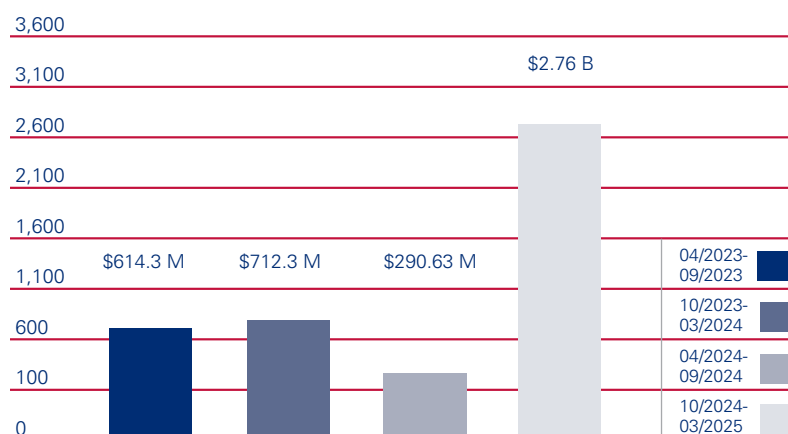
- Kept OIG staff engaged and informed of Office priorities and key activities through regular meetings among staff and management; updates from senior management and IG community meetings; issuance of OIG Connection newsletters, and other communications.
- Enrolled OIG staff in several different FDIC, CIGIE, and other Leadership Development Programs to enhance their leadership capabilities.
- Supported OIG staff pursuing professional training and certifications to enhance their expertise and knowledge.
- Organized several activities to promote community, teamwork, and collegiality among OIG staff.
- Represented the FDIC OIG in the CIGIE Connect, Collaborate & Learn (CCL) and Upon Further Inspection: Monetary Impact Training. We presented on monetary impact requirements, identification and calculation, presentation, and reporting. We also participated in a panel discussion on coordinating monetary impact recommendations with management officials. Several staff have supported various CIGIE subcommittees and working groups throughout the reporting period.
- Shared information from our Training Officer throughout the OIG to promote employee engagement, training, and career development.
- Established a mechanism for OIG staff to pose questions related to issues of concern to them—for example with respect to the Deferred Resignation Program, Return to Office guidelines, and other changes brought about in light of the new Administration’s Executive Orders and related guidance.

Cumulative Results (2-year period)

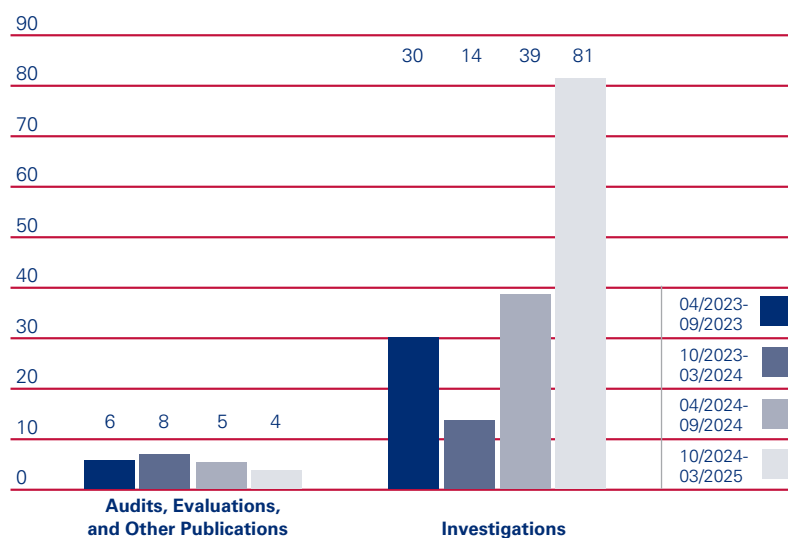
Recommendations

April 2023 – September 2023	71
October 2023 – March 2024	31
April 2024 – September 2024	42
October 2024 – March 2025	21

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



Products Issued and Investigations Closed





Reporting Requirements

Index of Reporting Requirements

The following listing reflects IG reporting requirements based on certain changes in Section 5 of the IG Act, pursuant to Section 5273 of the National Defense Authorization Act for Fiscal Year 2023.

Reporting Requirements	Page
Section 4(a)(2): Review of legislation and regulations.	44
Section 5(a)(1): A description of significant problems, abuses, and deficiencies relating to the administration of programs and operations of the establishment and associated reports and recommendations for corrective action made by the Office.	4-7
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 costs savings associated with the recommendation. (Recommendations open for more than one year are noted.)	45-62
Section 5(a)(3): A summary of significant investigations closed during the reporting period.	20-29
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.	63
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.	64
Section 5(a)(7): The information described under section 804(b) of the Federal Financial Management Improvement Act of 1996.	64
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.	67-69
Section 5(a)(9): A list of any outstanding recommendations from any peer review conducted by another Office of Inspector General that have not been fully implemented, including a statement describing the status of the implementation and why implementation is not complete.	67-69

Reporting Requirements (continued)

Page

Section 5(a)(10): A list of any peer reviews conducted by the Inspector General of another Office of Inspector General during the reporting period, including a list of any outstanding recommendations made from any previous peer review (including any peer review conducted before the reporting period) that remain outstanding or have not been fully implemented.

67-69

Section 5(a)(11): Statistical tables showing, for the reporting period:

- number of investigative reports issued during the reporting period;
- the total number of persons referred to the Department of Justice for criminal prosecution during the reporting period;
- the total number of persons referred to State and local prosecuting authorities for criminal prosecution during the reporting period; and
- the total number of indictments and criminal informations during the reporting period that resulted from any prior referral to prosecuting authorities.

64

Section 5(a)(12): A description of metrics used for Section 5(a)(11) information.

64

Section 5(a)(13): A report on each investigation conducted by the Office where allegations of misconduct were substantiated involving a senior Government employee or senior official (as defined by the Office) if the establishment does not have senior Government employees.

64

Section 5(a)(14):

- (A) A detailed description of any instance of whistleblower retaliation, including information about the official found to have engaged in retaliation; and
- (B) what, if any, consequences the establishment actually imposed to hold the official described in subparagraph (A) accountable.

65

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.

65

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.

65



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 CIGIE's 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 the IG community as it works with Congress on these priorities and other government reform issues.

Listed below are legislative proposals that CIGIE considers of high priority to the IG community. According to CIGIE, if enacted, the legislative priorities and initiatives supported by CIGIE's 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.
- **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.

Table I: Unimplemented Recommendations from Previous Semiannual Periods

Notes:

1. A current listing of each of the unimplemented recommendations is available at <https://www.fdicigoig.gov/unimplemented-recommendations>. The listing is updated monthly.
2. Recommendations open for more than one year are marked **. These total 29 recommendations as of March 31, 2025.

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-22-004 <u>The FDIC's Information Security Program - 2022</u> September 27, 2022	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 conducted an audit to evaluate the effectiveness of the FDIC's information security program and practices. The audit found that the FDIC had established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and National Institute of Standards and Technology security standards and guidelines. In addition, the FDIC had completed certain actions to continue to strengthen its security controls since the prior year, such as prioritizing the remediation of Plans of Action and Milestones; remediating outdated baseline configurations; and finalizing an Identity, Credential, and Access Management Roadmap. However, the audit found security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. These control weaknesses could be improved to reduce the impact on the confidentiality, integrity, and availability of the FDIC's information systems and data. The report contained one recommendation for the FDIC to address the 31 flaw remediation Plans of Action and Milestones. Recommendation 1 is unimplemented.	1	1 **	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
REV-23-001 <u>Security Controls Over the FDIC's Wireless Networks</u> December 13, 2022	Wi-Fi technology offers benefits to organizations, such as ease of deployment and installation and expanded network accessibility. However, Wi-Fi technology also presents security risks to the confidentiality, availability, and integrity of FDIC data and systems because it is not bound by wires or walls, and if not properly configured, is susceptible to signal interception and attack. We conducted an evaluation to determine whether the FDIC had implemented effective security controls to protect its wireless networks. We engaged the professional services firm of TWM Associates, Inc. to conduct the technical aspects of this review. We found that the FDIC did not comply or partially complied with several practices recommended by the National Institute of Standards and Technology and Federal and FDIC guidance in the following five areas: 1. Configuration of Wireless Networks 2. Wireless Signal Strength 3. Security Assessments and Authorizations 4. Vulnerability Scanning 5. Wireless Policies, Procedures, and Guidance The report contained eight recommendations intended to strengthen the security controls over the FDIC's wireless networks. Recommendation 2 is unimplemented.	8	1**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-23-002 <u>The FDIC's Security Controls Over Microsoft Windows Active Directory</u> March 15, 2023	The FDIC relies heavily on information systems containing sensitive data to carry out its responsibilities. To ensure that only individuals with a business need are allowed access, the FDIC uses Active Directory to centrally manage user identification, authentication, and authorization. Active Directory infrastructure is an attractive target for attackers because the same functionality that grants legitimate users access to systems and data can be hijacked by malicious actors for nefarious purposes. Therefore, it is paramount for the FDIC to ensure that it is adequately protecting its Active Directory infrastructure. We conducted an audit to assess the effectiveness of controls for securing and managing the Windows Active Directory to protect the FDIC's network, systems, and data. We engaged the professional services firm of Cotton & Company Assurance and Advisory, LLC (Cotton) to conduct this audit. Cotton determined that the FDIC had not fully established and implemented effective controls for securing and managing the Windows Active Directory to protect the FDIC's network, systems, and data in 7 of the 12 areas we assessed. The report contained 15 recommendations to improve Active Directory security controls. Recommendation 12 is unimplemented.	15	1**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
REV-23-002 <u>FDIC's Oversight of a Telecommunications Contract</u> March 31, 2023	In February 2014, the FDIC awarded a telecommunications service contract to AT&T Corp. (AT&T) in the amount of \$12 million for telecommunication services. In May 2019, the FDIC Chief Information Officer Organization (CIOO) approved a strategy to upgrade the bandwidth of AT&T's telecommunication services within the FDIC Field Offices. In March 2021, the FDIC CIOO notified the OIG of major internal control failures with the telecommunications contract. We conducted a review to determine if the FDIC authorized and paid AT&T for services to upgrade bandwidth in FDIC Field Offices in accordance with its policies and procedures and existing telecommunications contract. We determined that the FDIC did not authorize and pay AT&T for services to upgrade bandwidth in the FDIC Field Offices in accordance with its policies and procedures and existing telecommunications contract. The FDIC did not adhere to its acquisition policies and procedures because FDIC CIOO Executive Managers did not establish an accountable organizational culture or "tone at the top" for compliance with FDIC acquisition policies and procedures. FDIC CIOO Executive and Corporate Managers also did not implement proper internal controls for the AT&T contract. In addition, risks related to the FDIC CIOO's reliance on contractor services and the need to maintain an effective internal control environment for its contract oversight management activities were not included in the FDIC's Enterprise Risk Management Risk Inventory. Lastly, FDIC CIOO personnel failed to fulfill their roles and responsibilities with regard to the AT&T contract. The report contained 14 recommendations to enhance contracting controls. Recommendation 9 is unimplemented.	14	1**	\$1,500,000

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-23-002 Sharing of Threat and Vulnerability Information with Financial Institutions August 29, 2023	Financial institutions face a wide range of significant and persistent threats to their operations. Such threats include cyberattacks, money laundering, terrorist financing, pandemics, and natural disasters such as hurricanes, tornadoes, and floods. Whether man-made or natural, these threats can disrupt the delivery of financial services and inflict financial harm on consumers and businesses. The interconnected nature of the financial services industry further elevates the potential impact that threats can have on financial institutions. For example, many insured financial institutions rely on third-party service providers to provide critical banking services. An incident at a large service provider could have a cascading impact on a large number of financial institutions. If widespread, the impact could ultimately diminish public confidence and threaten the stability of the U.S. financial system. We conducted an evaluation to determine whether the FDIC had implemented effective processes to ensure that financial institutions receive actionable and relevant threat and vulnerability information. The FDIC had implemented processes for the sharing of threat and vulnerability information with financial institutions. For example, the FDIC established formal procedures to communicate cyber threat and vulnerability information. However, we reported that the FDIC could improve the effectiveness of its processes to ensure financial institutions receive actionable and relevant threat and vulnerability information. The report contained 10 recommendations to improve the FDIC's processes in order to ensure that financial institutions receive actionable and relevant threat and vulnerability information. Recommendations 7, 8, and 10 are unimplemented.	10	3**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-23-004 <u>The Federal Deposit Insurance Corporation's Information Security Program – 2023</u> 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**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-23-003 FDIC Efforts to Increase Consumer Participation in the Insured Banking System September 13, 2023	In October 2022, the FDIC issued results from the 2021 FDIC National Survey of Unbanked and Underbanked Households (2021 Household Survey). The 2021 Household Survey found that an estimated 4.5 percent of U.S. households were unbanked. The FDIC defines economic inclusion as the general population's ability to participate in all aspects of a nation's economy, to include access to safe, affordable financial products and services. The FDIC's Division of Depositor and Consumer Protection leads the FDIC's economic inclusion efforts. We conducted an evaluation to determine whether the FDIC developed and implemented an effective strategic plan to increase the participation of unbanked and underbanked consumers in the insured banking system. The FDIC developed an Economic Inclusion Strategic Plan with the stated goal to "promote the widespread availability and effective use of affordable, and sustainable products and services from insured depository institutions that help consumers and entrepreneurs meet their financial goals." However, opportunities exist to strengthen the effectiveness of future Economic Inclusion Strategic Plans by incorporating additional strategic planning best practices into the strategic planning process. The report contained 14 recommendations intended to improve the development and implementation of future FDIC Economic Inclusion Strategic Plans. Recommendation 13 is unimplemented.	14	1**	NA

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. Recommendations 2, 3, 4, 6, 7, 8, 9, 11, and 17 are unimplemented.	17	9**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-24-01 FDIC Strategies Related to Crypto- Asset Risks October 17, 2023	In recent years, the crypto-asset sector has experienced significant volatility. The total market capitalization of crypto assets fluctuated from about \$132 billion in January 2019 to \$3 trillion in November 2021. More concerning, the market capitalization fell by 60 percent to \$1.2 trillion as of April 2023. These events highlight various risks that the crypto-asset sector could pose to financial institutions, including liquidity, market, pricing, and consumer protection risks. We conducted a review to determine whether the FDIC has developed and implemented strategies that address the risks posed by crypto assets. The FDIC had started to develop and implement strategies that address the risks posed by crypto assets. However, the Agency had not assessed the significance and potential impact of the risks. Specifically, the FDIC had not yet completed a risk assessment to determine whether the Agency could sufficiently address crypto-asset related risks through actions such as issuing guidance to supervised institutions. In addition, the FDIC's process for providing supervisory feedback on FDIC-supervised institutions' crypto-related activities was unclear. As part of its process, the FDIC requested that financial institutions provide information pertaining to their crypto related activities. Additionally, the FDIC issued letters (pause letters), between March 2022 and May 2023, to certain FDIC-supervised financial institutions asking them to pause, or not expand, planned or ongoing crypto-related activities, and provide additional information. However, the FDIC did not (1) establish an expected timeframe for reviewing information and responding to the supervised institutions that received pause letters and (2) describe what constituted the end of the review process for supervised institutions that received a pause letter. We made two recommendations for the FDIC to: (1) establish a plan with timeframes for assessing risks pertaining to crypto-related activities and (2) update and clarify the supervisory feedback process related to its review of supervised institutions' crypto-related activities. Recommendation 1 is unimplemented.	2	1**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-24-02 <u>Material Loss Review of Signature Bank of New York</u> October 23, 2023	On March 12, 2023, the New York State Department of Financial Services closed Signature Bank of New York (SBNY) and appointed the FDIC as receiver. On April 28, 2023, the FDIC estimated the loss to the Deposit Insurance Fund (DIF) to be approximately \$2.4 billion. We engaged Cotton & Company Assurance and Advisory, LLC (Cotton) to perform a Material Loss Review. The objectives were to (1) determine why the bank's problems resulted in a material loss to the DIF, and (2) evaluate the FDIC's supervision of the bank, including the FDIC's implementation of the Prompt Corrective Action (PCA) requirements of section 38 of the Federal Deposit Insurance Act, and make recommendations for preventing any such loss in the future. SBNY's failure was caused by insufficient liquidity and contingency funding mechanisms, which impeded the bank's ability to withstand a run on deposits. In addition, SBNY management prioritized aggressive growth over the implementation of sound risk management practices needed to counterbalance the liquidity risk associated with concentrations in uninsured deposits. Cotton found that the FDIC: • Missed opportunities to downgrade SBNY's Management component rating and further escalate supervisory concerns; • Did not consistently perform supervisory activities in a timely manner and was repeatedly delayed in issuing supervisory products; • Appropriately downgraded SBNY's Liquidity component rating, but changing market conditions warrant the FDIC's review and potential revision of examination guidance; and • Determined that SBNY was well capitalized throughout each examination cycle prior to its failure based on defined capital measures. Cotton made six recommendations intended to improve the FDIC's supervision processes and its ability to apply effective forward-looking supervision in a changing banking environment. Recommendations 1, 2, 4, and 5 are unimplemented.	6	4**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-24-03 Material Loss Review of First Republic Bank November 28, 2023	On May 1, 2023, the California Department of Financial Protection and Innovation closed First Republic Bank and appointed the FDIC as receiver. On June 5, 2023, the FDIC recorded a final estimated loss to the Deposit Insurance Fund (DIF) of \$15.6 billion. We engaged Cotton & Company Assurance and Advisory, LLC (Cotton) to perform a Material Loss Review. The objectives were to (1) determine why the bank's problems resulted in a material loss to the DIF, and (2) evaluate the FDIC's supervision of the bank, including the FDIC's implementation of the Prompt Corrective Action requirements of Section 38 of the Federal Deposit Insurance Act, and make recommendations for preventing any such loss in the future. First Republic Bank's failure was caused by contagion effects stemming from the failure of other prominent financial institutions, which led to a run on deposits, significantly reducing its liquidity and exposing vulnerabilities in its business strategy. Specifically, First Republic Bank's strategy of attracting high net-worth customers with competitive loan terms, and funding growth through low-cost deposits, resulted in a concentration of uninsured deposits while increasing the bank's sensitivity to interest rate risk. This strategy ultimately led to a significant asset/liability mismatch for the bank, and fair value declines on its portfolio of low-yielding, long-duration loans, which limited its ability to obtain sufficient liquidity and prevented its recovery. Cotton determined that: • The FDIC missed opportunities to take earlier supervisory actions and downgrade the bank's component ratings consistent with the FDIC's forward-looking supervisory approach; • The FDIC assessed the bank's uninsured deposits consistent with FDIC policies, but the magnitude and velocity of uninsured deposit outflows warranted the FDIC's re-evaluation of assumptions and guidance pertaining to uninsured deposits; and • The bank was well-capitalized throughout each examination cycle based on defined capital measures, but that the bank's failure may warrant changes to the guidelines establishing standards for safety and soundness, including the adoption of noncapital triggers requiring regulatory actions. Cotton made 11 recommendations intended to improve the FDIC's supervision processes and its ability to apply effective forward-looking supervision in a changing banking environment. Recommendation 11 is unimplemented.	11	1**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AEC Memorandum-24-01 <u>The FDIC's Regional Service Provider Examination Program</u> December 20, 2023	Banks routinely rely on third parties for numerous activities, including information technology services, accounting, compliance, human resources, and loan servicing. Under the Bank Service Company Act, the FDIC has the statutory authority to examine third party entities (or "service providers") that provide technology services to its regulated financial institutions. The FDIC conducts examinations of service providers to evaluate their 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 the financial institutions using these service providers. The FDIC performs service provider examinations using two risk tiers: Significant Service Providers and Regional Service Providers (RSP). RSPs are smaller in size, less complex, and provide services to banks within a local region. We conducted an audit to assess the effectiveness of the FDIC's RSP examination program related to third-party risks to financial institutions. These examinations are typically performed jointly with the Federal Reserve Board and Office of the Comptroller of the Currency, and in compliance with interagency guidance established by the Federal Financial Institutions Examination Council. We found that the FDIC has not formally established performance goals, metrics, and indicators to measure overall program effectiveness and efficiency. As a result, we were unable to conclude on the program's effectiveness; however, we identified opportunities to improve the RSP examination program. Specifically: (1) monitoring reports of examination distribution timeliness; (2) complying with examination frequency guidelines; (3) providing additional guidance on how to use RSP examinations in support of the FDIC's InTReX program; and (4) establishing a comprehensive inventory of FDIC supervised bank service providers and the financial institutions serviced. We recommended that the FDIC conduct a formal assessment of the RSP examination program to establish program-level goals, metrics, and indicators and determine whether additional resources and controls are needed to improve the effectiveness of the program. Recommendation 1 is unimplemented.	1	1**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-24-04 The FDIC's Purchase and Deployment of the FDIC Acquisition Management System January 25, 2024	The FDIC procures goods and services from contractors in support of its mission. In December 2020, the FDIC entered into an agreement to purchase an enterprise-wide acquisition management system. In June 2022, the FDIC went live with the system. However, the FDIC was unsuccessful in deploying the new system and abandoned it within 5 months. As a result, the FDIC incurred contract and staff labor-hour costs of nearly \$10 million and had to revert to its legacy acquisition systems and manual reporting of some acquisition activities. We conducted an evaluation to review the primary factors that led to the FDIC's unsuccessful deployment of the FDIC Acquisition Management System and identify improvements for implementing future significant organizational changes. We determined that the FDIC's deployment of this new acquisition management system was unsuccessful because the FDIC did not employ an effective change management process as its policies and procedures did not require it. In addition, FDIC managers lacked awareness and training on when and how to implement a change management process. We made three recommendations for the FDIC to: (1) incorporate change management processes into the FDIC's policies and procedures and internal controls, (2) provide training on the change management process, and (3) implement a change management strategy and plan for the acquisition of a new acquisition management system. We also identified \$9.9 million of funds to be put to better use that we reported in our Semiannual Report for the period ending March 30, 2024. Recommendations 1 and 2 are unimplemented.	3	2**	\$9,900,000

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

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

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-24-05 The FDIC's Sexual Harassment Prevention Program July 31, 2024	Sexual harassment can have profound effects and serious consequences for the harassed individual, fellow colleagues, and the agency as a whole. It can undermine an agency's mission by creating a hostile work environment that lowers productivity and morale, affects the agency's reputation and credibility, and exposes the agency to judgments for monetary damages. Establishing an effective sexual harassment prevention program and addressing sexual harassment allegations in a prompt and effective manner can protect employees and the agency against the risk of such harm and costs. We conducted an evaluation to determine whether the FDIC implemented an effective sexual harassment prevention program to facilitate the reporting of sexual harassment allegations and address reported allegations in a prompt and effective manner. This was a follow-up to our 2020 evaluation, Preventing and Addressing Sexual Harassment (EVAL-20-006). The FDIC had not implemented an effective sexual harassment prevention program that facilitated the reporting of sexual harassment misconduct allegations and had not always investigated and addressed allegations of sexual harassment promptly and effectively. We found that FDIC leadership at several levels had not demonstrated sufficient commitment to, and accountability for, the 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 Anti-Harassment Program (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 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, and 24 are unimplemented.	24	23	NA

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 <u>Audit of Security Controls for the FDIC's Cloud Computing Environment</u> 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, 3, 4, 5, 6, and 7 are unimplemented.	7	7	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-24-06 <u>Conflicts of Interest in the Acquisition Process</u> September 23, 2024	Employees' adherence to principles of ethical conduct, to include not holding financial interests that conflict with duties and avoiding actions creating the appearance of violations of ethical standards, helps ensure public confidence and integrity of the Federal Government. Media reports in October and December 2022 regarding financial conflicts of interest of senior government officials included reference to three FDIC employees. Subsequently, the OIG received a Congressional request on February 28, 2023, to conduct a review of conflicts of interest at the FDIC and the effectiveness of existing rules and laws to prevent such conflicts. The objective of this evaluation was to determine the extent to which the FDIC has processes and procedures to identify, analyze, respond to, and monitor for conflicts of interest of FDIC employees engaged in the acquisition process. We found the FDIC has processes and procedures to identify, analyze, respond to, and monitor for conflicts of interest in the acquisition process. However, improvements are needed to strengthen internal controls for conflicts of interest in the acquisition planning and approval processes. We also found that the FDIC could strengthen employee knowledge of ethics laws and regulations through specialized acquisition-related training. Additionally, we determined the FDIC could enhance its approach to confidential financial disclosure reviews by updating guidance and training. We made eight recommendations intended to improve the FDIC's internal controls related to conflicts of interest in the acquisition process and enhance its financial disclosure review program. Recommendations 1, 2, 3, 4, 5, 7, and 8 are unimplemented.	8	7	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-24-07 The FDIC's Information Security Program – 2024 September 25, 2024	The Federal Information Security Modernization Act of 2014 (FISMA), Public Law No. 113-283, requires Federal agencies, including the FDIC, to conduct annual independent evaluations of their information security programs and practices and to report the results to the Office of Management and Budget (OMB). FISMA requires the independent evaluations to be performed by the Agency IG, or an independent external auditor as determined by the IG. We engaged KPMG to conduct this evaluation. The objective of the evaluation was to assess the effectiveness of the FDIC's information security program and practices. KPMG considered FISMA requirements, National Institute of Standards and Technology (NIST) security standards and guidelines, the NIST Cybersecurity Framework, Office of Management and Budget policy and guidance, FDIC policies and procedures, and Department of Homeland Security guidance and reporting requirements to plan and perform the work and to conclude on the objective. KPMG determined that the FDIC's overall information security program was operating at a Maturity Level 4 (Managed and Measurable) with respect to the FY 2024 FISMA Metrics. While KPMG found that the FDIC established a number of information security program controls and practices that were consistent with FISMA requirements, the report describes security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. KPMG made three recommendations to address weaknesses identified during this evaluation. Recommendations 1 and 2 are unimplemented.	3	2	NA

Table II: Audit and Evaluation Reports				
Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	Title*	Total	Unsupported	
AEC Memo-25-01 October 31, 2024	<i>Oversight of the Infrastructure Support Services Contract</i>			
EVAL-25-01 November 12, 2024	<i>Material Loss Review of Republic First Bank</i>			
EVAL-25-02 December 10, 2024	<i>FDIC's Readiness to Resolve Large Regional Banks</i>			
REV-25-01 December 18, 2024	<i>Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct – Part 1</i>			
Totals for the Period		\$0	\$0	\$0

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

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	81
Number of Persons Referred to the Department of Justice for Criminal Prosecution	63
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	0
Number of Indictments and Criminal Informations	64

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

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

During this reporting period, there was one investigation involving a senior government employee where an allegation of misconduct was substantiated. A corporate manager failed to comply with the FDIC's Supplemental Standard of Ethical Conduct, 5 C.F.R. § 3201.102 (Extensions of Credit and Loans From FDIC-Insured Institutions) which prohibits any FDIC employee from participating in, inter alia, any matter involving an FDIC-insured institution with whom the employee has an outstanding extension of credit. The manager participated in a matter involving an insured institution where the manager held a loan. The investigation did not identify evidence that the employee misused their FDIC position or FDIC information or that there was any personal or financial benefit to the employee. The manager received verbal counseling and subsequently achieved compliance in coordination with the designated ethics official.

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 regard to closed investigations, there is one item to report. The matter discussed in Table VI was closed and not disclosed to the public.



Appendix 2

Information on Failure Review Activity

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

FDIC OIG Review Activity for the Period October 1, 2024, through March 31, 2025 (for failures that occur on or after January 1, 2014 causing losses to the Deposit Insurance Fund of less than \$50 million)

When the Deposit Insurance Fund (DIF) incurs a loss under \$50 million, Section 38(k) of the FDI Act requires the Inspector General of the appropriate federal banking agency to determine the grounds upon which the state or Federal banking agency appointed the FDIC as receiver and whether any unusual circumstances exist that might warrant an In-Depth review of the loss.

As of the end of the reporting period, there was one Failed Bank Review in process. We are reviewing the failure of Pulaski Savings Bank, Chicago, Illinois, which failed on January 17, 2025, causing an estimated loss of \$28.5 million to the DIF.



Appendix 3

Peer Review Activity

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

Definition of Audit Peer Review Ratings

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

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

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

Audit Peer Reviews

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

The Department of State OIG conducted a peer review of the FDIC OIG's audit function and issued its report on the peer review on September 16, 2022. The FDIC OIG received a rating of **Pass**. In the Department of State OIG's opinion, the system of quality control for the audit organization of FDIC OIG in effect for the year ended March 31, 2022, had been suitably designed and complied with to provide FDIC OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards and applicable legal and regulatory requirements in all material respects.

The Department of State OIG communicated additional findings that required attention by FDIC OIG management but were not considered to be of sufficient significance to affect the Department of State OIG's opinion expressed in its peer review report. There are no outstanding recommendations.

This [peer review report](#) is posted on our Website.



Inspection and Evaluation Peer Reviews

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

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

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

FDIC OIG Peer Review of Another OIG

As discussed earlier in this report, 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 peer 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, VA OIG sampled case files for investigations closed between October 1, 2022, and September 30, 2023.

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

On November 21, 2023, the VA OIG reported that in its opinion, the system of internal safeguards and management procedures for the investigative function of the FDIC OIG in effect for the year ending 2023, complied with the quality standards established by CIGIE and the other applicable guidelines and statutes cited above. These safeguards and procedures provided reasonable assurance of conforming with professional standards in the planning, execution, and reporting of FDIC OIG investigations.

Finally, we note that as of the end of the reporting period, we were completing the Qualitative Assessment Review of the investigative operations of the General Services Administration OIG.



Congratulations

We are proud of the members of the FDIC OIG who were recognized at the IG Community's Annual Awards Ceremony in November 2024.

FDIC Strategies Related to Crypto-Asset Risks — Excellence—Evaluations

In recognition of a comprehensive evaluation of crypto-asset risks, resulting in significant improvements to the FDIC's assessment of the risks posed by crypto assets to the banking sector and the FDIC's supervision of banks engaged in crypto activities.

Matt Simber, Catherine Gao, Jane Kim, YeYe Shen, Lueth Akuak, Lisa Price, Sharon Tushin, Rigene Mabry, Ryan Wasilick, Caitlin Savino.

The FDIC's Examination of Government-Guaranteed Loans — Excellence—Evaluations

In recognition of effecting significant change through an evaluation of the FDIC's Examination of Government-Guaranteed Loans, resulting in 19 recommendations to improve FDIC supervision and prompting \$7 million in civil money penalties and restitution.

Luke Itnyre, Katie Boutwell, Michael Reed, Ryan Wasilick, Shelley Shepherd, Cynthia Hogue, Sharon Tushin, Daniel Craven, Thomas Ritz, Usman Abbasi, Rigene Mabry, Melissa Mulhollen, Caitlin Savino.

Investigation of the Failure of First NBC Bank, New Orleans, Louisiana — Excellence—Investigations

In recognition of excellence in an investigation involving the failure of First NBC Bank, New Orleans, Louisiana.

Joseph Melle, Bobby Hood.

Also included in this award—our law enforcement partners from the FBI, Federal Reserve Board OIG, and the U.S. Attorney's Office, Eastern District of Louisiana.

Additionally of note— Special Agent Jonathan Heydon was nominated by Federal Housing Finance Agency OIG for his efforts as part of a team investigating a Paycheck Protection Program-related fraud scheme:

Texas Star Services Investigation Team—Excellence—Investigations

In recognition of remarkable investigative efforts leading to the successful prosecution of a multi-million-dollar, multi-defendant Paycheck Protection Program Recruitment Fraud Scheme, along with the additional successful efforts to identify and recover ill-gotten gains of the fraud.





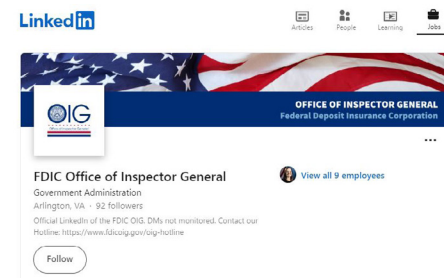
★ Learn more about the FDIC OIG.
Visit our website: www.fdicigoig.gov.



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



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



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



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



www.pandemicoversight.gov

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.fdicigov.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.





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