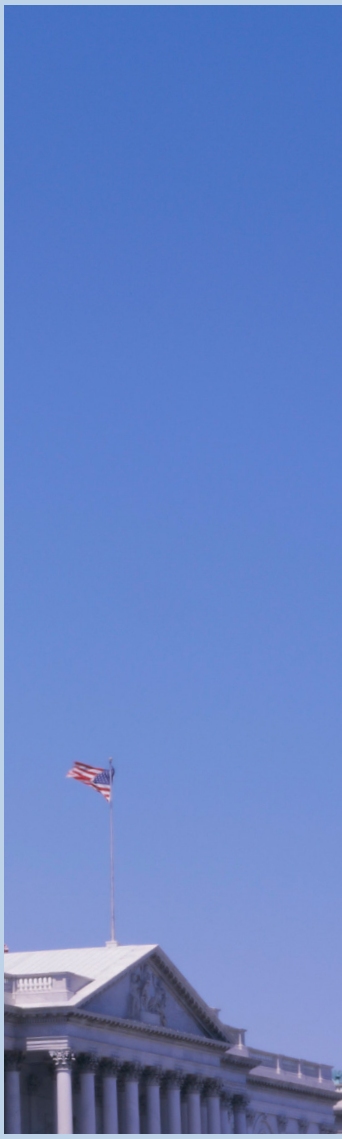
FDIC Office of Inspector General

Semiannual Report to the Congress

April 1, 2024 - September 30, 2024



Office of Inspector General

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 6,096 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data (June 30, 2024), the FDIC insured $10.65 trillion in domestic deposits in 4,539 institutions, of which the FDIC supervised 2,896. The Deposit Insurance Fund balance totaled $129.2 billion as of June 30, 2024. Active receiverships as of September 30, 2024, totaled 61, with assets in liquidation of about $34 billion.

Semiannual Report to the Congress

April 1, 2024 – September 30, 2024

1989–2024 35 YEARS

OFFICE OF INSPECTOR GENERAL

35 Years of Independent Oversight at the FDIC

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 April 1, 2024, to September 30, 2024. 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. Results from this semiannual reporting period attest to the positive difference we are making.

We issued 5 audit and evaluation reports with 42 recommendations to the FDIC designed to strengthen controls to address identified risks. Among the most important was our evaluation report on *The FDIC's Sexual Harassment Prevention Program*. We reported that the FDIC has not implemented an effective sexual harassment prevention program that facilitates the reporting of sexual harassment misconduct allegations and has not always investigated and addressed allegations of sexual harassment promptly and effectively. We made 24 recommendations for major improvements to the Anti-Harassment Program at the FDIC. Implementing and sustaining these improvements over time will assist the FDIC in creating a trusted environment for reporting allegations of sexual harassment.

We also issued a Management Advisory Memorandum where we emphasized the need for the FDIC to keep the OIG apprised in a timely manner of any allegations of misconduct on the part of senior officials. We also suggested improved communications with FDIC staff to ensure they were informed about the OIG and the OIG Hotline as a means to report allegations of misconduct. Another of our evaluations addressed Conflicts of Interest in the FDIC's Acquisition Process. Two other reports in the Information Technology realm covered Security Controls for the FDIC's Cloud Computing Environment and results of our annual report in accordance with the Federal Information Security Modernization Act.

As for Investigations, we are helping to maintain and preserve the integrity of the banking sector and to detect and deter financial fraud. One successful case that we highlight in this report involves the former President and Chief Executive Officer of the Heartland Tri-State Bank, Elkhart, Kansas, who was sentenced to 293 months in prison for his role embezzling $47.1 million of the bank's funds. These funds were ultimately lost in a "pig butchering" cryptocurrency scheme that caused the bank to fail and the Deposit Insurance Fund to incur a $54.2 million loss. Another of our cases resulted in a businessman found guilty of perpetrating an investment fraud ponzi scheme, for which he received a sentence of 288 months in prison for wire fraud and money laundering. In yet another case, Kabbage—a now bankrupt small business lending firm–agreed to pay up to $120 million to resolve allegations that it defrauded the Paycheck Protection Program by knowingly submitting false claims for loan forgiveness, loan guarantees, and processing fees to the Small Business Administration.

Overall, FDIC OIG investigations during the reporting period resulted in 81 indictments, 74 convictions, 53 arrests, and more than $290.6 million in fines, restitution ordered, and other monetary recoveries. Notably, and as illustrated in the Kabbage case referenced above, these results include the FDIC OIG's efforts combatting fraud in the Federal government's COVID-19 pandemic response, which resulted in 44 indictments and informations, 23 arrests, and 35 convictions. Monetary benefits resulting from these types of cases alone this period totaled in excess of $172.8 million—more than triple the amount reported in our last semiannual report. We continue to play a significant role within the law enforcement community in combating this type of fraud, and since inception of the CARES Act, have been involved in 198 such cases.

Importantly, our Office has also seen a rise in payment scams, and we include a special feature in this report to alert the public about the nature and consequences of such schemes, some of which have been perpetrated falsely using the names of FDIC and FDIC OIG officials. We advise 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 OIG 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 Committees and Working Groups, and participation on financial crime task forces and law enforcement working groups throughout the country.

I deeply appreciate the FDIC's long-standing, essential role in maintaining stability and public confidence in the U.S. financial system, beginning in 1933. Importantly, the FDIC OIG has an impressive history as well. In accordance with the IG Act Amendments of 1988, on April 17, 1989, by way of an FDIC Board Resolution, the FDIC established an independent Office to be headed by an IG who would function under the general supervision of the FDIC Chairman.

We marked our 35th Anniversary of providing independent oversight of the FDIC in April. We are committed to continuing to deliver credible results that drive meaningful change, enhance integrity and accountability, and foster public trust in the FDIC.

In closing, I am grateful for the strong support of the Congress, the FDIC Board and management, and colleagues in the IG and law enforcement communities as we to carry out our oversight mission. I am especially proud of the accomplishments of our dedicated staff who tirelessly and passionately serve the American people.

Jennifer L. Fain
Inspector General
October 2024

Table of Contents

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

Acronyms and Abbreviations

AHP	Anti-Harassment Program
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
DEIA	Diversity, Equity, Inclusion, and Accessibility
DFA	Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010
DIF	Deposit Insurance Fund
DOJ	Department of Justice
ECU	Electronic Crimes Unit
FBI	Federal Bureau of Investigation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act of 2014
HTSB	Heartland Tri-State Bank
IG	Inspector General
InTREx	Information Technology Risk Examination
IRS-CI	Internal Revenue Service-Criminal Investigation
IT	Information Technology
OI	Office of Investigations
OIG	Office of Inspector General
OLA	Orderly Liquidation Authority
OMB	Office of Management and Budget
ORMIC	Office of Risk Management and Internal Control
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
RSP	Regional Service Provider
SBA	Small Business Administration
SBNY	Signature Bank of New York
USAO	United States Attorney's Office

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 (April 1, 2024–September 30, 2024)	
Audit, Evaluation, and Other Products Issued	**5**
Recommendations	**42**
Investigations Opened	**37**
Investigations Closed	**39**
Judicial Actions:	
Indictments/Informations	**81**
Convictions	**74**
Arrests	**53**
OIG Investigations Resulted in:	
Special Assessments	**$15,700.00**
Fines	**$94,500.00**
Restitution	**$85,933,683.97**
Asset Forfeitures	**$34,592,049.96**
Civil Settlement	**$66,250,000.00**
Civil Restitution	**$53,750,000.00**
Civil Money Penalties	**$50,000,000.00**
Total	**$290,635,933.93**
Referrals to the Department of Justice (U.S. Attorney)	**60**
Investigative Reports Referred to FDIC Management for Action	**2**
Responses to Requests Under the Freedom of Information/Privacy Act	**19**
Subpoenas Issued	**N/A**

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 five reports addressing control improvements needed in in information technology (IT), contracting, and prevention of sexual harassment. We made a total of 42 recommendations to FDIC management in these reports. Of note, and as discussed below, our report on Cloud Computing contained 7 main recommendations, and an additional 48 related technical recommendations to management.

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 currently have one material loss review in process—that of Republic First Bank of Philadelphia. This bank failed on April 26, 2024, with losses to the DIF estimated at $667.1 million.

If the losses to the DIF as a result of a failure are less than the material loss threshold, the FDI Act requires the Inspector General of the appropriate Federal banking agency to determine the grounds upon which the state or Federal banking agency appointed the FDIC as receiver and whether any unusual circumstances exist that might warrant an In-Depth Review of the loss. As of the end of the reporting period, we had no such reviews in process.

Results of the audits, evaluations, and other reviews completed during the reporting period are summarized below. 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 the U.S. Department of Justice 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.

Importantly, in December 2023, the OIG announced two assignments that the Office initiated to address allegations regarding FDIC culture, sexual harassment, and other forms of misconduct. These allegations surfaced in a Wall Street Journal article and received other media and Congressional attention. The first assignment, which we completed in July 2024, and which is discussed below, is the evaluation of the FDIC's Sexual Harassment Prevention Program. The assignment's objective was 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 evaluation to a report that we issued in July 2020 on preventing and addressing sexual harassment.

The second assignment is a Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct. The objective is 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 are currently completing work on the Special Inquiry assignment and will report the results of that effort in an upcoming semiannual report.

Audits, Evaluations, and Other Reviews

The FDIC's Sexual Harassment Prevention Program

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. Our Office 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).

We determined the FDIC has not implemented an effective sexual harassment prevention program that facilitates the reporting of sexual harassment misconduct allegations and has not always investigated and addressed allegations of sexual harassment promptly and effectively. Specifically, we found that FDIC leadership at several levels:

- Has not demonstrated sufficient commitment to, and accountability for, the Anti-Harassment Program (AHP);
- Has not implemented an effective program structure or dedicated sufficient resources to the program;
- Does not have an effective system for tracking, addressing, and documenting allegations;
- Has not established adequate complaint procedures or an adequate AHP policy; and
- Has not provided sufficient training to its supervisors and staff.

This occurred because the FDIC has not sustained many program improvements that were initiated as a result of our prior 2020 evaluation. As a result, the FDIC is experiencing an environment of distrust, and many employees do not feel comfortable reporting sexual harassment at the FDIC or are afraid of reporting for fear of retaliation. Absent an AHP with committed leadership; an effective complaint tracking system; and updated policies, procedures, and training; the FDIC cannot ensure that it has taken all of the steps necessary to prevent sexual harassment, facilitate reporting, and promptly and appropriately address sexual harassment allegations.

We made 24 recommendations to the FDIC to address the findings in our report. The FDIC concurred with all of our recommendations and plans to complete corrective actions by March 31, 2025.

Management Advisory Memorandum to the FDIC Chairman as Part of the OIG's *Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct*

This interim memorandum emphasized the need for the FDIC to keep the OIG informed in a timely manner of any allegations of misconduct on the part of senior officials. It further suggested that corporate-wide communications can be improved to ensure that all FDIC staff are informed about the OIG and the OIG Hotline as a means to report allegations of misconduct.

The OIG plans to include a summary of the FDIC's actions regarding this advisory, as well as more formal recommendations to address these matters, in its final special inquiry report.

The Audit of Security Controls for the FDIC's Cloud Computing Environment

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 with Sikich CPA LLC (Sikich) to conduct an audit of security controls for the FDIC's cloud computing environment. The objective of this audit was to assess the effectiveness of security controls for the FDIC's cloud computing environment. Sikich determined that the FDIC had not effectively implemented security controls in its cloud computing environment in five of nine areas, including Identity and Access Management, Protecting Cloud Secrets, Patch Management, Flaw Remediation, and Audit Logging. Due to the number of findings and similarities among them, Sikich identified six common themes of security weaknesses listed below:

1. **Insecure Coding Practices:** The FDIC cloud platform teams did not consistently implement secure coding practices.
2. **Misconfigured Security Settings:** The FDIC cloud platform teams did not consistently configure cloud platform security settings in accordance with cloud service providers and industry best practices.
3. **Least Privilege:** The FDIC did not consistently provision access to its cloud-based systems in accordance with the principle of least privilege.
4. **Outdated Software:** Cloud platforms relied on outdated software components.
5. **Ineffective Monitoring:** The FDIC did not adequately monitor the activity on its cloud-based systems.
6. **Cloud Service Provider Vulnerabilities:** Cloud service providers were solely responsible for causing certain vulnerabilities and should be responsible for their remediation.

Sikich made 7 formal recommendations supported by 48 related technical recommendations to improve cloud security controls in the 6 common themes of security weaknesses listed above. The FDIC concurred with all recommendations and plans to complete all corrective actions by December 30, 2026.

Conflicts of Interest in the FDIC's Acquisition Process

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.

Our Office conducted an evaluation to determine the extent to which the FDIC has processes and procedures to identify, analyze, respond to, and monitor for conflicts of interest of FDIC employees engaged in the acquisition process.

We found that the FDIC has processes and procedures to identify, analyze, respond to, and monitor for conflicts of interest in the acquisition process. However, improvements 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 that 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. The FDIC concurred with all recommendations and plans to complete corrective actions by August 31, 2025.

Federal Information Security Modernization Act—2024

Our Office issued its evaluation report pursuant to the Federal Information Security Modernization Act of 2014 (FISMA) during the reporting period. The objective of the evaluation was to evaluate the effectiveness of the FDIC's information security program and practices. The OIG engaged the firm of KPMG, LLP to perform this work based on guidance from the Office of Management and Budget.

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

The FDIC had established a number of information security program controls and practices that were consistent with information security policy, standards, and guidelines. However, the evaluation report describes security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices, including the following:

- The FDIC Did Not Fully Enforce Plans of Action and Milestones Documentation Requirements.
- The FDIC Needs to Enforce Role-Based Training Requirements.
- The FDIC Did Not Fully Implement Audit Logging Requirements on Assessed Information Systems.

- The FDIC Did Not Review Audit Logs at Sufficient Frequency Within Cloud Information Systems.
- The FDIC Did Not Remediate Overdue Plans of Action and Milestones Related to SI-2 (Flaw Remediation).

The report contained three recommendations related to addressing the weaknesses identified during this year's evaluation. In addition, there were two outstanding recommendations from prior FISMA reports along with other time-sensitive activities warranting the FDIC's continued attention. The FDIC concurred with the recommendations and plans to complete corrective actions by September 30, 2025.

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 February 2024 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.

In February 2024, we identified nine Top Challenges facing the FDIC. The Challenges identified risks to FDIC mission-critical activities and to FDIC internal programs and processes that support mission execution. These Challenges included all aspects of the Challenges that we reported last year, with important updates. Among these updates were the need for the FDIC to address increasing staff attrition–especially for examiners--and to focus on improving the FDIC's workplace environment. We also noted that the failures of Signature Bank of New York and First Republic Bank demonstrated the need for the FDIC to escalate supervisory actions when risks were identified, consistent with the FDIC's forward-looking supervision initiative. Further, we noted that the FDIC should consider emerging risks in its failure estimation process and ensure that the FDIC can execute its orderly liquidation resolution authority. Challenges identified were as follows:

1. Strategic Human Capital Management at the FDIC

- Addressing FDIC Staff Attrition
- Managing a Wave of Prospective Retirements at the FDIC
- Sustaining a Work Environment Free from Discrimination, Harassment, and Retaliation

2. Identifying and Addressing Emerging Financial Sector Risk

- Escalating Supervisory Actions to Address Identified Risks
- Assessing Emerging Risks Through Data Gathering and Analysis
- Considering Emerging Risks in the FDIC's Bank Failure Estimation Process
- Sharing Threat and Vulnerability Information with Financial Institutions

3. Ensuring Readiness to Execute Resolutions and Receiverships

- Readiness for FDI Act Resolutions
- Preparing for an Orderly Liquidation

4. Identifying Cybersecurity Risks in the Financial Sector

- Examining for Bank Third-Party Service Provider Cybersecurity Risk
- Improving Bank IT Examination Processes
- Ensuring FDIC Staff Have Requisite Financial Technology Skills
- Continuing to Assess Risks Posed by Emerging Technology

5. Assessing Crypto-Asset Risk

- Assessing the Impact of Crypto-Asset Risks to FDIC-Supervised Banks
- Clarifying Processes for Supervisory Feedback Regarding Bank Crypto-Asset-Related Activities

6. Protecting Consumer Interests and Promoting Economic Inclusion

- Assessing Risks in Bank Consumer Services Models
- Improving the FDIC's Ability to Increase Economic Inclusion
- Preparing to Examine for Changes to the Community Reinvestment Act
- Addressing Misuse of the FDIC Name and Misrepresentation of Deposit Insurance

7. Fortifying IT Security at the FDIC

- Strengthening the FDIC's Information Security Profile
- Improving Information Security Controls
- Managing Systems Migration to the Cloud
- Protecting the FDIC's Wireless Network
- Assessing the FDIC's Ransomware Attack Readiness

8. Strengthening FDIC Contract and Supply Chain Management

- Improving Contract Management
- Addressing Supply Chain Risk Management
- Ensuring Contractors Are Appropriately Vetted and Are Not Performing Inherently Governmental Functions
- Ensuring Whistleblower Rights and Protections for Contractor Personnel

9. Fortifying Governance of FDIC Programs and Data

- Strengthening Performance Goal Development and Monitoring
- Improving Internal Controls by Addressing Outstanding Recommendations
- Ensuring Data Quality to Assess Program Performance

Ongoing Work

At the end of the current reporting period, we had a number of ongoing audits, evaluations, and reviews emanating from our analysis of the Top Management and Performance Challenges and covering significant aspects of the FDIC's programs and activities, including those formally announced to the FDIC and highlighted below:

- **Evaluation of the FDIC's Resolution of Large Banks:** The objective is to assess the adequacy of the FDIC's resolution readiness and response efforts for the failures of Silicon Valley Bank, Signature Bank, and First Republic Bank, including the extent to which the FDIC adhered to established policies and procedures for key resolution functions.
- **Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct:** The objective is 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.
- **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.
- **Material Loss Review of Republic First Bank:** Our objectives for this review, as mandated by the FDI Act, are 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 FDI Act, and make recommendations for preventing any such loss in the future.
- **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.

Ongoing reviews are listed on our website, and, when completed, their results will be presented in an upcoming semiannual report.

We also note that we are assessing the challenges that face the FDIC currently and looking to the future, and we will issue our updated assessment of those Management Challenges in March 2025, in connection with the FDIC's issuance of its Annual Report.

Peer Review of the U.S. Department of Justice OIG's Inspection and Evaluation Function

Our Office of Audits, Evaluations, and Cyber reviewed the system of quality control for the U.S. Department of Justice (DOJ) OIG in effect for the year ended March 31, 2024. A system of quality control includes multiple aspects of an organization, including, but not limited to, policies and procedures designed to provide reasonable assurance of complying with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation*, December 2020 (Blue Book).

Our FDIC OIG review team reported on September 24, 2024, that in its opinion, the system of quality control for the DOJ OIG in effect for the year ended March 31, 2024, had been suitability designed and complied with to provide the DOJ OIG with reasonable assurance of performing and reporting in conformity with the Blue Book. Inspection and Evaluation organizations can receive a rating of pass, pass with deficiencies, or fail. The DOJ OIG received an External Peer Review rating of pass.

In addition to the report, the team issued a Letter of Comment that set forth findings that were not considered to be of sufficient significance to affect the review team's opinion expressed in its report.

Update on Issue Related to OIG Email Security

In our previous semiannual reports, and originating during the course of our 2021 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.

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 44 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 7 of the 44 should have been closed in a timelier manner. Six of the seven are currently being worked on by the FDIC and the closure form for the remaining one recommendation is under review by the OIG. ORMIC has also indicated that going forward, it will take steps to better ensure timely completion of outstanding OIG and Government Accountability Office recommendations.

ORMIC stated that it has developed a Power BI dashboard that will provide Senior Executives with greater insight into the status of all open recommendations (e.g., on-time, extension likely, past due). Additionally, ORMIC will work 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.

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

With FDIC Management for Action

(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).

(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-23-003) *The FDIC's Adoption of Cloud Computing Services*. July 25, 2023. **Recommendation 1:** Develop and maintain an inventory and catalog of all FDIC data used throughout the cloud data lifecycle.

(EVAL-23-002) *Sharing of Threat and Vulnerability Information with Financial Institutions*. August 29, 2023. **Recommendation 1:** Share threat and vulnerability information that is uniquely developed or summarized by the FDIC with financial institutions or other financial sector entities to further strengthen their threat intelligence activities. This includes results from the FDIC's 2022 Ransomware Horizontal Review and relevant trending and analysis conducted by the Division of Risk Management Supervision.

(REV-23-001) *Security Controls Over the FDIC's Wireless Network*. December 13, 2022. **Recommendation 2:** Develop and implement a policy to review, approve, and centrally manage the configuration settings of current and future Wi-Fi enabled devices in FDIC facilities, before set-up and subsequent updates.

(REV-23-002) *FDIC Oversight of a Telecommunications Contract*. March 31, 2023. **Recommendation 9:** Develop a strategy to periodically assess workload imbalances and implement a strategy to address such imbalances among Oversight Managers in the FDIC CIO Organization.

Under Review by the OIG

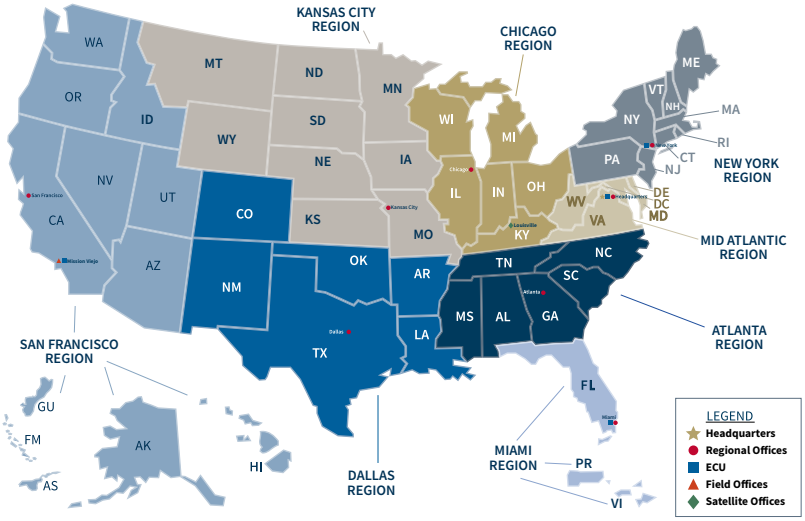
(EVAL-20-001) *Contract Oversight Management*. October 28, 2019. **Recommendation 2:** Provide enhanced contract portfolio reports to FDIC executives, senior management, and the Board of Directors.

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.



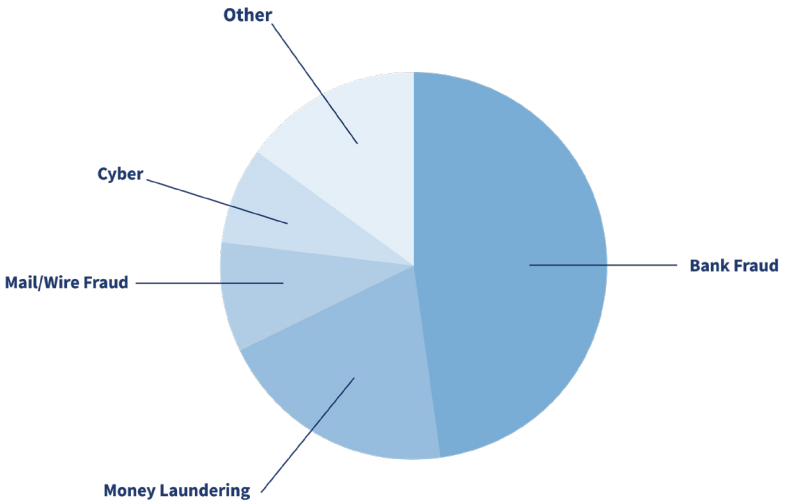
OIG Regional Map

FDIC OIG investigations during the reporting period resulted in 81 indictments/informations, 74 convictions, 53 arrests, and more than $290.6 million in fines, restitution ordered, and other monetary recoveries. We opened 37 cases and closed 39 during the reporting period. We referred two investigative reports to FDIC management for action.

Open Investigations

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

Open Investigations – Allegations



Note that **Other** may include the following: Embezzlement, Misappropriation of Funds, Employee-Related, Bank Secrecy Act Violations, Banking Client Fraud and Abuse, Bribery, Elder Fraud, and Misrepresentation/Impersonation Schemes.

Implementation of the OIG's Body Worn Camera Program

On May 25, 2022, the President issued Executive Order 14074 on *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*. One aspect of the order required Federal law enforcement to implement a Body Worn Camera program for all law enforcement officers and ensure the use of the body worn cameras in all appropriate circumstances, including during arrests and searches.

Our Office of Investigations (OI) successfully implemented its body worn camera program in the summer of 2023. Aligning with the requirements outlined in Executive Order 14074, OI collaborated with our Office of General Counsel to design a comprehensive training curriculum spanning 2 days, covering legal aspects, policy compliance, technical proficiency, application of skills, and scenario-based tactics training. OI agents were trained in Maryland, Texas, and Virginia. Upon the completion of the training, online refresher courses were also given. We continue to conduct refresher training and have incorporated the training as part of our New Agent Training.

Electronic Crimes Unit
Our Electronic Crimes Unit (ECU) is an important component within our Office of Investigations. Over the past several years, the OIG ECU has worked to overhaul and revamp its Forensic Laboratory. The ECU lab helps analyze voluminous electronic records in support of complex financial fraud investigations nationwide. The ECU lab also provides a platform for complex data analysis, eDiscovery, and forensic data services, and it supports the analysis of electronically stored information. To successfully investigate financial crimes, the ECU is continuously looking at emerging technology, developing strategic partnerships, and providing expert forensic support to our Special Agents.

We have made substantial investments in our ECU to ensure that in addition to traditional forensics capabilities, our agents are equipped with the latest cutting-edge technology and tools to investigate financial crimes. We are focusing on cyber-crimes at banks, including computer intrusions, dark web, supply chain attacks, phishing, and denials of service; cases involving cryptocurrency and fraudulent attempts by crypto exchanges to enter the financial markets; and ransomware attacks against banks. Our ECU is working to ensure that there are early-warning notifications, so that we can investigate and coordinate a law enforcement response against such adversarial cyber attacks. (Learn more about the FDIC OIG ECU in a video on our website at www.fdicoig.gov/oig-videos.)

We are also pursuing complex fraud schemes involving FinTech companies –where technology has led to security risks that allow for things like the use of synthetic identities to commit financial fraud. We are investigating account takeover and email compromise schemes as well, where unauthorized transfers of funds cause considerable harm to individuals, businesses, banks, and communities. We have investigated and charged many overseas defendants who participated in these schemes – leading to several international detentions and extradition proceedings.

Members of the OIG's Electronic Crimes Unit join law enforcement partners in employing technology to execute search warrants, as illustrated here.

FDIC OIG Continues to Support DOJ Initiatives to Combat COVID-19 Related Fraud

The FDIC OIG is one of 22 partner agencies that make up the DOJ - COVID-19 Fraud Enforcement Task Force. DOJ released its Annual Report highlighting the success of the Task Force in April 2024. The Fact Sheet of the report can be found here:

Since its inception in May 2021, members of the COVID-19 Fraud Enforcement Task Force have used a full range of tools to hold accountable fraudsters and other criminals who sought to exploit the government's pandemic response for their personal gain.

This work has resulted in:

- More than **3,500 defendants** charged with federal crimes.
- More than **$1.4 billion** in seizures and forfeiture orders to recover stolen CARES Act funds.
- More than **400 civil settlements and judgments**.

To achieve these results, Task Force members have built a comprehensive program to identify fraud, recover assets, and hold wrongdoers accountable. This has included:

- Five prosecutorial **COVID-19 Fraud Enforcement Strike Forces**—based in California, Colorado, Maryland, New Jersey, and Florida—with dedicated funding to pursue pandemic fraud.
- A first-of-its-kind **National Unemployment Insurance Fraud Task Force** that leverages data from state workforce agencies and the Small Business Administration to identify those who exploited pandemic relief programs.
- A **Pandemic Analytics Center of Excellence** that creates sophisticated data products designed to detect, deter, and stop pandemic fraud across multiple government agencies.

Pandemic-Related Financial Crimes

Since many of the programs in the Coronavirus Aid, Relief, and Economic Security (CARES) Act and related legislation are 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 198 such cases.

Notably, during the reporting period, the FDIC OIG's efforts related to the Federal government's COVID-19 pandemic response resulted in 44 charging actions (indictments, informations, and superseding indictments and informations), 23 arrests, and 35 convictions involving fraud in the CARES Act Programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases totaled in excess of $172. 8 million—more than triple the amount reported in our last semiannual report.

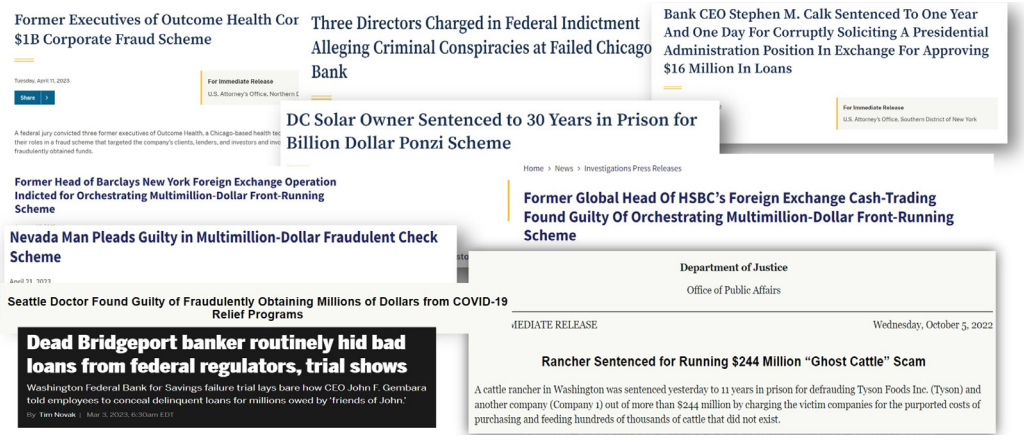
Leveraging Data Analytics

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 experts – in order to marshal our resources and harness voluminous data. During the reporting period, we migrated our first two data sets into the data lake to permit access to advanced analytical tools. We are looking for red-flag indicators and searching for aberrations in the underlying facts and figures. In that way, we will be able 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, involve collaboration with the Pandemic Response Accountability Committee (PRAC), the FDIC, Financial Crimes Enforcement Network, 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 strategic planning within the OIG.

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.



OIG Headlines

Former Bank President and CEO of Failed Bank Sentenced

On August 19, 2024, former Heartland Tri-State Bank (HTSB) President and Chief Executive Officer Shan Hanes was sentenced to 293 months in prison for his role in embezzling $47.1 million of HTSB funds, that were ultimately lost in a cryptocurrency scheme known as "pig butchering." This scheme led to the failure of HTSB, with a loss to the DIF of $54.2 million, and a complete loss of equity for investors. Hanes was remanded into the custody by the Federal Bureau of Prisons at the conclusion of the hearing. The restitution portion of his sentencing will be finalized at an upcoming separate hearing.

On July 28, 2023, HTSB was closed by the Kansas Office of the State Bank Commissioner and the FDIC was subsequently named Receiver. Hanes previously pleaded guilty to one count of embezzlement on May 23, 2024.

Beginning on or about May 30, 2023, and continuing through at least July 7, 2023, Hanes allegedly embezzled funds from HTSB by causing at least 11 wire transfers from the bank to purchase cryptocurrency and to make investments in gold for his own personal benefit. In total, approximately $47.1 million was fraudulently transferred from HTSB. Additionally, in an effort to cover up the scheme, Hanes allegedly stole money from accounts associated with investment clubs, churches, and other programs and accounts for which he had signature authority. Once Hanes had leveraged all available funds, he attempted to disguise the first of many wires to look like an associated transaction related to a U.S. Department of Agriculture loan involving a local farmer.

Source: FDIC Division of Resolutions and Receiverships.
Responsible Agencies: FDIC OIG, FBI, Federal Reserve Board (FRB) OIG and Federal Housing Finance Agency (FHFA) OIG.
Prosecuted by the USAO, District of Kansas.

Defendant Sentenced in Investment Fraud Ponzi Scheme by Unlicensed Brokerage Firm

On August 6, 2024, Avinash Singh was sentenced in the Middle District of Florida to 288 months in prison followed by 2 years of supervised release. In May 2024, Singh pleaded guilty to two counts of wire fraud and three counts of money laundering.

From 2013 to 2020, Singh operated a company called Highrise Advantage, LLC in Orlando, FL, and defrauded investors by purporting to invest the victims' funds in retail foreign currency contracts ("forex") with promises of no losses to his investors. Singh solicited and received more than $57 million from over 1,100 victims throughout the course of the scheme. Rather than invest his victims' funds in forex trading, Singh used funds from one investor to pay amounts owed to another investor. Singh misappropriated at least $45 million of the victims' funds in the form of payments to other investors and also spent millions of dollars in personal expenses, including the purchase of real estate, retail purchases, phone bills, events, dining, and reserving music studio space to record music with his band. Once the funds were received, they were laundered through several banks and converted to pay loans and credit cards related to Singh's personal expenses.

In December 2019, Singh signed a plea agreement for wire fraud and money laundering that was filed in the Middle District of Florida. Singh then failed to appear for his scheduled hearing and became a fugitive. Singh was subsequently indicted in February 2021, which superseded the previously filed criminal information and plea agreement. On October 19, 2023, Singh was apprehended in the country of Belize, deported to Miami, and taken into custody by the U.S. Marshals Service.

Source: USAO, Middle District of Florida, Financial Crimes Task Force. Responsible Agencies: FDIC OIG, Internal Revenue Service-Criminal Investigation (IRS-CI), and the Florida Office of Financial Regulation. Prosecuted by the USAO, Middle District of Florida.

Former President of Failed Bank Sentenced

Jackie Poulsen, aka Jack Poulsen of Ericson, Nebraska, was sentenced on August 1, 2024, in Federal court in Lincoln, Nebraska for bank fraud. Poulsen was sentenced to 18 months' imprisonment with 5 years of supervised release to follow. There is no parole in the Federal system. Poulsen was additionally ordered to pay $815,000 in restitution. On May 2, 2024, Poulsen, the former President of Ericson State Bank, pleaded guilty to an Information charging him with bank fraud. The bank previously failed on February 14, 2020, and the FDIC was named receiver.

As President of the bank, Poulsen was responsible for overseeing all of the bank's affairs, managing day-to-day operations, and keeping other Directors of the Board informed of the institution's financial condition. Poulsen had lending authority but was required to seek approval from the bank's loan committee for any loans exceeding $250,000. Further, Poulsen was not permitted to serve as the loan officer on loans for which he would have a personal conflict of interest.

Beginning in 2012, the bank began a lending relationship with an individual related to Poulsen. This individual and his business entities received numerous loans and opened several accounts with the bank. Beginning in at least June 2015, Poulsen began interfering with these insider-related loans and accounts for the purpose of hiding their unsoundness from the Board of Directors. These actions included advancing bank funds for more than the approved loan amounts; manipulating data contained in the bank's computer system by advancing Payment Due Dates and Loan Maturity Dates to conceal the past-due status of the insider-related loans from the Board of Directors; and advancing loans over the approved note amounts and applying the funds to conceal overdrafts on the insider-related checking accounts from the Board of Directors. Poulsen's actions continued until September 2019, when he was removed from his positions of authority with the bank. These insider-related loans had a balance in excess of $7 million, and ultimately caused significant losses to Ericson State Bank.

Source: FDIC Division of Risk Management Supervision. Responsible Agencies: FDIC OIG, FHFA OIG, FRB OIG, and the FBI. Prosecuted by the USAO, District of Nebraska.

Federal Attorney Sentenced to Conspiring to Sexually Exploit Numerous Children

On April 30, 2024, Mark Black, former Federal Deposit Insurance Corporation attorney, was sentenced to 20 years in prison with an additional 20 years of supervised release following his incarceration.

According to court documents, from January 2018 to October 2021, Black, of Arlington, Virginia, was a member of two online groups dedicated to exploiting children. The goal of the two groups was to locate prepubescent girls online and convince them to livestream themselves engaging in sexually explicit conduct. Black and his co-conspirators would covertly record this conduct and share the videos with each other.

In July 2019, Black induced a prepubescent minor to engage in sexually explicit conduct on a live-streaming application while screen-recording that activity. That same month, Black and a co-conspirator also groomed another prepubescent minor to engage in sexually explicit acts on a photo and video-sharing application. The co-conspirator surreptitiously hacked into that girl's live-video feed and recorded the sexual acts before sending them to Black.

Black's electronic devices were found to contain approximately 172,707 images of suspected child sexual abuse material. Of those files, over 1,300 depicted identified victims of the offenses of conviction.

Black was formerly the Arlington Aquatic Club board president.

On January 23, 2024, Black pleaded guilty to one count of conspiracy to produce child pornography and one count of coercion and enticement.

Source: USAO, Eastern District of Virginia.
Responsible Agencies: FDIC OIG and FBI.
Prosecuted by the USAO, Eastern District of Virginia.

Kabbage Agrees to Pay up to $120 Million to Resolve Allegations That It Defrauded the Paycheck Protection Program

On May 13, 2024, it was announced that bankrupt lender Kabbage, Inc. d/b/a KServicing, had agreed to resolve allegations that it knowingly submitted thousands of false claims for loan forgiveness, loan guarantees, and processing fees to the U.S. Small Business Administration (SBA) as part of the Paycheck Protection Program (PPP), in violation of the False Claims Act. Kabbage is now winding down its operations as KServicing Wind Down Corp. after filing for Chapter 11 bankruptcy in the District of Delaware in October 2022. The resolution consists of two separate settlements with KServicing Wind Down Corp., that together provide the United States with an allowed, unsubordinated, general unsecured bankruptcy claim for recovery of up to $120 million. The amount the government will recover on this claim will depend on the ultimate amount of assets available to the bankruptcy estate for distribution to unsecured creditors.

The first settlement, which provides the United States with a claim for recovery of up to $63.2 million, resolves allegations that Kabbage systemically inflated tens of thousands of PPP loans, causing the SBA to guarantee and forgive loans in amounts that exceeded what borrowers were eligible to receive under program rules. As part of the settlement, KServicing Wind Down Corp. admitted and acknowledged that Kabbage double-counted state and local taxes paid by employees in the calculation of gross wages; failed to exclude annual compensation in excess of $100,000 per employee; and improperly calculated payments made by employers for leave and severance. The United States alleged that Kabbage was aware of its errors as early as April 2020, yet Kabbage failed to remedy all incorrect loans that had already been disbursed and continued to approve additional loans with miscalculations. The resolution also provides for Kabbage to receive a $12.5 million credit for payments it previously returned to the SBA during the Department's investigation of this alleged misconduct. Half of the $63.2 million settlement amount is considered restitution, or about $25.4 million.

The second settlement, which provides the United States with a claim for recovery of up to $56.7 million, resolves allegations that Kabbage knowingly failed to implement appropriate fraud controls to comply with its PPP and Bank Secrecy Act/Anti-Money Laundering obligations. In particular, the United States alleges that Kabbage removed underwriting steps from its pre-PPP procedures in order to process a greater number of PPP loan applications and maximize processing fees. The government further alleged that Kabbage knowingly set substandard fraud check thresholds despite knowledge of SBA's concerns that fraudulent borrowers might seek to benefit from the PPP; relied on automated tools that were inadequate in identifying fraud; devoted insufficient personnel to conduct fraud reviews; discouraged its fraud reviewers from requesting information from borrowers to substantiate their loan requests; and submitted to the SBA thousands of PPP loan applications that were fraudulent or highly suspicious for fraud. Half of the $56.7 million settlement amount is considered restitution, or about $28.4 million.

Prior to becoming an SBA approved Lender, Kabbage acted as an Agent completing PPP loan applications on behalf of banks and financial institutions throughout the United States. Celtic Bank was Kabbage's primary banking partner which was already a partner in the SBA's 7(a) program and originated Kabbage's small business loans and served as Kabbage's initial intermediary.

Source: USAO for the District of Massachusetts.
Responsible Agencies: FDIC OIG, FBI, SBA OIG, FRB OIG, DOJ's Fraud Section, DOJ's Civil Commercial Litigation Branch, and the USAOs for the District of Massachusetts and the Eastern District of Texas.

Pharmacy Owner Sentenced to 72 Months for Role in a COVID-19 Money Laundering and Health Care Fraud Case

On April 11, 2024, Arkadiy Khaimov was sentenced in the Eastern District of New York to 72 months in prison to be followed by 2 years of supervised release. Khaimov was also ordered to pay restitution in the amount of $18,921,139.21.

Khaimov and Peter Khaim (guilty plea to money laundering in 2022) used COVID-19 emergency override billing codes in order to submit fraudulent claims to Medicare, for which they were paid over $30 million for cancer medication Targretin Gel 1%. Fraudulent submissions included claims where the medication never was purchased by the pharmacies, prescribed by physicians, or dispensed to patients – often during periods when pharmacies were non-operational – and using doctors' names on prescriptions without their permission. The defendants allegedly acquired control over more than a dozen New York pharmacies by paying others to pose as the owners of the pharmacies and hiring pharmacists to pretend to be supervising pharmacists at the pharmacies for the purpose of obtaining pharmacy licenses. Targretin Gel 1% has an average wholesale price of approximately $34,000 for each 60-gram tube.

In addition, Khaimov and Khaim utilized U.S. financial institutions to engage in a sophisticated money laundering conspiracy by creating sham pharmacy wholesale companies, which they named after pre-existing pharmacy wholesalers, and fabricated references to invoices to make it appear that funds transferred from the pharmacies to the sham pharmacy wholesale companies were for legitimate pharmaceutical drug purchases. In the first phase of this conspiracy, the defendants conspired with an international money launderer who utilized financial institutions to arrange for funds to be wired from the sham pharmacy wholesale companies to companies in China for distribution to individuals in Uzbekistan. In exchange, the defendants received cash from an unlicensed money transfer business, minus a commission that was deducted by the money launderer. In the second phase of this conspiracy, when the fraudulent proceeds exceeded the amount of cash available, the defendants caused others to transfer funds back from the sham wholesale companies to the defendants, their relatives, or their designees, in the form of certified cashier's checks and cash that was dropped off at their residences in the middle of the night. The defendants used the proceeds of the scheme to purchase real estate and luxury items.

Source: USAO, Eastern District of New York, and DOJ, Criminal Division, Fraud Section.
Responsible Agencies: FDIC OIG, IRS-CI, Health and Human Services OIG, and FBI.
Prosecuted by the USAO, Eastern District of New York, and DOJ Criminal Division, Fraud Section.

Business Owner and Bank Customers Sentenced for Role in Bank Fraud Scheme

On July 23, 2024, Erik Richard Jones and Mitchell Allen Melega were sentenced to multi-year prison sentences following their convictions for conspiracy to commit bank fraud, bank fraud, and money laundering. Jones was sentenced to 54 months of imprisonment to be followed by 5 years of supervised release. Melega was sentenced to 75 months of imprisonment to be followed by 5 years of supervised release. Both defendants were also ordered to pay $4,840,944.63 in restitution.

On October 20, 2020, Jones and Melega were charged by Indictment with one count of conspiracy to commit bank fraud, eight counts of bank fraud, and three counts of money laundering in a scheme where they submitted fraudulent invoices for purposes of receiving advances on their lines of credit at both First Midwest Bank and Northwest Bank & Trust Company. The funds from these lines of credit were subsequently diverted for uses rather than the stated purpose on the credit applications. On September 5, 2023, Jones entered a guilty plea to all 12 counts of the indictment. On March 12, 2024, Melega pleaded guilty to all 12 counts of the indictment.

In March 2014, Jones, while operating I-80 Equipment, executed a Loan Agreement and Promissory Notes with First Midwest Bank to obtain working capital lines of credit. The primary working capital line of credit loan, not to exceed $9,500,000, was to be used for truck purchases and improvements. Between August 2016 and September 2017, Jones and Melega requested and obtained loan advances from First Midwest Bank for vehicles that were never purchased or inflated purchase prices for vehicles in order to obtain additional funds from First Midwest Bank related to the advances. In order to accomplish this, I-80 Equipment provided fabricated or altered purchase invoices to First Midwest Bank. First Midwest Bank relied on these fraudulent invoices to approve the loan advances and determine the amount of funds to be advanced. Additionally, I-80 Equipment obtained legitimate invoices, but did not use the advanced funds to purchase the vehicles. This caused First Midwest Bank to issue approximately $5,304,547 for 110 vehicles, in purchase and improvement advances based on the fraudulent scheme that Jones and Melega conducted. Jones and Melega also sold approximately 32 vehicles that First Midwest Bank had advanced approximately $1,594,801 to purchase but failed to pay off the outstanding advances as required by the loan agreement.

In addition to the above scheme, Jones--operating JP Rentals--executed a commercial real estate mortgage with Northwest Bank & Trust Company in July 2016 to obtain loan funding, not to exceed a maximum principal amount of $1,959,894. Subsequently, Jones and Melega diverted approximately $400,000 for uses other than as intended and stated in the loan agreement.

Source: USAO, Central District of Illinois.
Responsible Agencies: FDIC OIG and IRS-CI.
Prosecuted by the USAO, Central District of Illinois.

Husband and Wife Plead Guilty to Wire Fraud and Money Laundering Conspiracy Related to $1,356,000 in Fraudulent PPP Loans

On August 28, 2024, Christopher and Erin Mazzei pleaded guilty to conspiracy to commit wire fraud affecting a financial institution, as well as money laundering conspiracy.

Christopher and Erin Mazzei 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 Mazzeis 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 invest in an unallowable business venture.

As part of the guilty plea, Christopher and Erin Mazzei consented to the entry of a forfeiture money judgment in the amount of $1,365,332 and also agreed to the forfeiture of a property in Kapolei, HI; a property in Arroyo Grande, CA; $583,993.60 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 to date total $2,421,374.37. The seized funds exceed the value of the fraudulent PPP loans received by Christopher and Erin Mazzei because the Mazzeis also engaged in bank/mortgage fraud activity as part of their scheme. Christopher and Erin Mazzei were not charged with the bank/mortgage fraud, but the plea agreement stipulates that the Court can consider the events underlying those potential charges for sentencing purposes.

Source: USAO, District of Hawaii.
Responsible Agencies: FDIC OIG, FRB OIG, Treasury Inspector General for Tax Administration, and the IRS-CI.
Prosecuted by the USAO, District of Hawaii.

Nevada Man Convicted of $11.2M COVID-19 Fraud

On September 4, 2024, a Federal jury in the District of Nevada convicted Meelad Dezfooli for defrauding three banks of more than $11.2 million in COVID-19 pandemic relief funds intended to help small businesses impacted by the pandemic. Dezfooli was found guilty on three counts of bank fraud, three counts of money laundering, and four counts of engaging in monetary transactions in criminally derived property.

Dezfooli submitted three fraudulent PPP loan applications to Federally regulated and insured banks, obtaining more than $11.2 million in proceeds from those loans. The evidence at trial showed that Dezfooli falsely represented certain material information in his loan applications, including information about payroll, employees, and use of the loan proceeds. After fraudulently obtaining more than $11.2 million in PPP funds, Dezfooli laundered and/or spent the proceeds, including buying approximately 25 residences and 2 luxury cars, funding a personal investment account, and gambling extensively. After he was originally charged, Dezfooli continued laundering criminal proceeds by selling five of the residences that he acquired with the fraudulently obtained PPP funds.

Dezfooli is scheduled to be sentenced on December 5, 2024.

Source: Federal Reserve Board-Consumer Financial Protection Bureau, Office of Investigations (FRB/CFPB OIG).
Responsible Agencies: FDIC OIG, FRB-CFPB OIG, SBA OIG, and IRS-CI.
Prosecuted by the Criminal Division's Money Laundering and Asset Recovery Section and the USAO, District of Nevada.

Former Capital One Multi-Branch Manager and Co-Conspirators Sentenced

On August 16, 2024, Janem Gibbs was sentenced to 6 months in prison followed by 2 years' supervised release. Gibbs was also ordered to pay $110,500 in restitution to Capital One. Gibbs previously pleaded guilty to one count of conspiracy to commit bank fraud in the Southern District of Texas on September 29, 2023. Gibbs was previously charged on February 22, 2023, in a four-count sealed indictment for her role in a bank fraud scheme in which she conspired to steal $200,000 from a Capital One customer's account causing a loss of $200,000 to Capital One.

Beginning on or before 2014, Former Capital One Multi-Branch Manager Gibbs conspired with multiple co-conspirators to steal funds from customer accounts. Gibbs misused her position at Capital One to query customer accounts to determine the account activity and balances. On June 8, 2016, an unidentified co-conspirator entered a Capital One branch impersonating a Capital One customer and met with Gibbs. Gibbs then instructed Capital One to wire $200,000 from an unknowing Capital One customer's account to co-conspirator Munson Hunter III's account at Wells Fargo. Hunter then laundered the funds through multiple bank accounts and disbursed the funds among the co-conspirators.

Beginning on or before February 2013 through February 24, 2023, Hunter opened bank accounts using fictitious names and other individuals' social security numbers for use in multiple fraud schemes. Hunter used the fictitious identities to obtain multiple credit cards at financial institutions, including Capital One and Chase Bank. Hunter also used the stolen identities of two separate individuals to apply for SBA loans in the business names Max Money and Management, LLC, and Money Management, Inc. Hunter also attempted to steal funds from a Capital One account via ACH transfers from an unknowing victim. Agents from the FDIC OIG and the FBI served a search warrant on Hunter's residence in June 2023 and found hundreds of pieces of evidence, including identification documents with Hunter's picture and fictitious names (including names used in the money laundering scheme), driver's licenses and social security cards of numerous other individuals, financial statements and checkbooks linked to accounts used in the money laundering scheme, and over 200 electronic devices, which were processed by the FDIC OIG's Electronic Crimes Unit.

On May 10, 2024, Hunter was sentenced in the Southern District of Texas to 51 months in prison followed by 3 years of supervised release. Hunter was ordered to pay $235,438.83 in restitution to victims Capital One, Chase Bank, and the U.S. Small Business Administration (SBA). Co-conspirator Gregory Thurman was sentenced on May 16, 2024, to 2 years of probation. Thurman was also ordered to pay $73,000 in restitution to Capital One. On June 14, 2024, co-conspirator Travis Wright was sentenced to 6 months in prison followed by 2 years of supervised release. Wright was ordered to pay $37,500 in restitution to Capital One.

Source: Based on a referral from the financial institution.
Responsible Agencies: FDIC OIG and FBI.
Prosecuted by the USAO, Southern District of Texas.

Man Sentenced for Role in Defrauding The Park Avenue Bank

On May 15, 2024, Abraham Kahan was sentenced in the Southern District of New York to time served, 3 years of supervised release, and 200 hours of community service for his role in a commercial loan fraud scheme involving a loan originated by The Park Avenue Bank, a failed FDIC-regulated institution, which ultimately resulted in a substantial loss to the FDIC and Valley National Bank. (After its failure in March 2010, The Park Avenue Bank was acquired by Valley National Bank.) Kahan was also ordered to pay restitution of $1,066,853, a $700 special assessment fee, and forfeiture in the amount of $505,000. On May 21, 2024, the plea and criminal information charging Kahan were unsealed.

Between June 2009 and October 2013, Kahan colluded with multiple other individuals to fraudulently obtain a $1,400,000 commercial bank loan from The Park Avenue Bank. Specifically, Kahan conspired with Aron Fried, Hershel Sauber, and former Park Avenue Bank Board of Director and attorney, Mendel Zilberberg, to secure a nominee loan in Sauber's name. Sauber then disbursed the loan's proceeds amongst Kahan, Fried, and Zilberberg.

The scheme was initiated when Kahan decided to become a partner in Emmanuel Services, a healthcare company with which Fried was affiliated. Fried required $900,000 before granting Kahan a partnership. Kahan, a previously convicted felon, was unable to obtain a loan meeting Fried's threshold. Therefore, Kahan recruited Sauber to apply for a $1.4 million business loan on his behalf. Following Sauber's recruitment, Fried introduced Kahan to Zilberberg, a former bank Board member. Between 2009 and 2013, Fried, Kahan, and Zilberberg met on several occasions to structure the loan. Ultimately, Sauber filed a loan application claiming: (1) the loan's proceeds were to be used as working capital for his businesses; (2) that Sauber was Zilberberg's client; and (3) Sauber's purported net worth qualified him for the loan. Sauber later admitted he had no intention of using the money, he did not recall meeting Zilberberg, and his reported net worth was inflated to secure the loan.

On September 8, 2009, Sauber received a $1.4 million dollar loan. Upon receipt, Sauber immediately transferred the loan proceeds to Fried. Then on the same day, Fried transferred $466,000 to Zilberberg's company, One World United. The loan became delinquent in January 2010. The Park Avenue Bank failed in March 2010. Valley National Bank subsequently assumed Sauber's loan. The loan eventually defaulted, and Valley National Bank recognized a loss of $213,370. Pursuant to the loss share agreement between the FDIC and Valley National Bank, the FDIC incurred a loss of $853,483.

Source: The FDIC's Legal Division, New York Region.
Responsible Agencies: FDIC OIG and FBI.
Prosecuted by the USAO, Southern District of New York.

Former Bank Vice President Sentenced for Bank Fraud Scheme

On September 12, 2024, Stacia Wilson was sentenced by to 3 years and 10 months in Federal prison without parole. The court also ordered Wilson to pay $1,435,491.05 in victim restitution. On May 9, 2024, Wilson, former Vice President of St. Clair County State Bank, Osceola, Missouri, pleaded guilty to one count of bank fraud in the Western District of Missouri. Under the terms of the plea agreement, Wilson must forfeit to the government a money judgment of $1,528,321, which represents the proceeds she obtained as a result of the fraud scheme.

Wilson was employed as a Vice President at the bank, where she held authority as a loan processor to access and create loans within the bank's system. Using this authority, Wilson created a scheme to defraud the bank by creating false and fictitious loans using bank customer information, without their knowledge. Wilson would have these false and fictitious loans funded with proceeds from the bank's general ledger. She would then convert the proceeds for her own personal benefit. Through this scheme, Wilson created numerous false and fictitious loans that resulted in a loss of $1,528,321 to St. Clair County State Bank.

Source: The FDIC's Division of Risk Management Supervision.
Responsible Agencies: FDIC OIG and FBI.
Prosecuted by the USAO, Western District of Missouri.

Special Feature

Beware: Payment Scams Are on the Rise

The FDIC OIG's Office of Investigations (OI) has seen a rise in Payment Scams during the reporting period. The four most common type 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 "Pig Butchering" scheme 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. These schemes have affected individuals and financial institutions alike. In the failed bank investigation of Heartland Tri-State Bank, as noted in this report, it was determined that the bank CEO embezzled and invested over $47 million dollars of victim funds in a Pig Butchering scheme that ultimately caused the bank to fail. https://www.fdicoig.gov/news/investigations-press-releases/former-ceo-failed-bank-sentenced-prison

In a government impersonation scam, a scammer fraudulently identifies as a government official to manipulate or steal from the victim. In a business email compromise scam, a 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. Government impersonation scams of FDIC OIG OI senior officials have been on the rise, with scammers purporting to be OI Special Agents in Charge to gain legitimacy with victims in order to demand payments. The FDIC OIG has issued an Office of Inspector General Alert in order to better educate the public on this growing problem.

According to the FTC's Consumer Sentinel Network Data Book, consumers reported losing over $10 billion to fraud in 2023. Impersonation scams accounted for nearly $2.7 billion of these losses, resulting from 853,935 reports. Additionally, consumers reported losing $4.6 billion to investment-related fraud in 2023, stemming from 107,699 reports of scammers offering fake investment opportunities.

According to the FBI's Internet Crime Complaint Center's (IC3) 2023 Internet Crime Report, individuals reported losing $4.57 billion to investment scams and $2.95 billion to business email compromise scams in 2023. These figures stem from 39,750 complaints and 21,489 complaints, respectively. The number of complaints of scams, and the amounts of losses, reported to the IC3 generally grew in the past 3 years.

If you believe you have been the victim of such schemes, contact the **OIG Hotline**.

Strong Partnerships with Law Enforcement Colleagues

The OIG has partnered with various USAOs throughout the country in bringing to justice individuals who have defrauded the FDIC or financial institutions within the jurisdiction of the FDIC, or criminally impeded the FDIC's examination and resolution processes. The alliances with the USAOs have yielded positive results during this reporting period. Our strong partnership has evolved from years of hard work in pursuing offenders through parallel criminal and civil remedies resulting in major successes, with harsh sanctions for the offenders. Our collective efforts have served as a deterrent to others contemplating criminal activity and helped maintain the public's confidence in the Nation's financial system.

During the reporting period, we partnered with USAOs in judicial districts in 38 locations in the U.S.

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

We also worked closely with DOJ; 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.
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; Council of the Inspectors General on Integrity and Efficiency (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).
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.

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 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 scheduled Audit Committee meetings. Apprised the Chairman and other internal Board Member accordingly.
- Issued a joint message from the FDIC Chairman and FDIC IG recognizing the importance of Whistleblower Appreciation Day.
- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
- Presented at the FDIC's "One FDIC" forum for new staff members and shared information on the mission, goals, and accomplishments of the FDIC OIG.
- Continued to enhance our external website, videos, 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, and the results of our investigations into financial fraud. Disseminated an informational video on fraudulent "pig butchering" scams to alert consumers and bankers of the dangers of such schemes.

- 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 such cases, as appropriate.
- Presented at the "Get to Know the FDIC's OIG" event hosted by the FDIC library on May 23. One of our Special Agents in the Mid-Atlantic Region presented on the FDIC OIG Office of Investigations' mission, priorities, and some interesting cases the Office of Investigations has been involved in.
- Participated in, and presented at, the FDIC and DOJ 2024 Financial Crimes Conference. FDIC OIG Presentations included a Keynote Address from the IG, a presentation on "Synthetic ID Fraud" presented by a Senior Special Agent in our Miami Regional Office, a presentation on "The Downfall of First NBC Bank" presented by a Special Agent in our Dallas Regional Office, and an "Overview of Fraud Trends" presented by an Office of Investigations Desk Officer.
- 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 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 Banking Majority staff on the OIG's report on the FDIC's Sexual Harassment Prevention Program.
- Briefed staff from the House and Senate Appropriations Committees on the FDIC OIG Fiscal Year 2025 Budget Request.
- Maintained the OIG Hotline to field complaints and allegations of fraud, waste, abuse, and mismanagement affecting FDIC programs and operations from the public and other stakeholders. The OIG's Whistleblower Protection Coordinator also helped educate FDIC employees who had made or were contemplating making a protected disclosure as to their rights and remedies against retaliation for such protected disclosures. Our web-based hotline portal at https://www.fdicoig.gov/oig-hotline 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 322 Hotline inquiries, 11 of which led to our opening investigations. Our on-line form, email, telephone, and postal mail were the most common vehicles for inquiries.

- Issued two alerts and a video warning banks and consumers about a 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.

- 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 Department of Justice prosecutors, the Federal Bureau of Investigation, 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.

- Participated in the Chairman's Diversity Advisory Council's (CDAC) Second Quarter Informational Series. Representatives from the OIG presented an overview of the OIG, focusing on Who We Are, What We Do, How the OIG Can Help FDIC Staff, Ways to Follow the OIG, and How to Learn More.

- Ensured the OIG's compliance with a newly implemented reporting mandate under Executive Order 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*. The Attorney General created the National Law Enforcement Accountability Database as "a centralized repository of official records documenting instances of law enforcement officer misconduct as well as commendations and awards."

- Supported the broader IG community by attending monthly CIGIE meetings and other meetings, such as those of the CIGIE Legislation Committee; the Employee Engagement and Innovation 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. Also continued to adopt features of the PRAC's Agile Product Toolkit to provide our stakeholders a means of receiving more expedient information on results of oversight efforts, for example to convey emerging concerns identified during audits and evaluations.

- Participated on 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.
- Coordinated with the Office of Management and Budget to address matters of interest related to our FY 2024 and 2025 budgets and proposed budget for FY 2026.
- Worked closely with representatives of the DOJ, including the Main Justice Department, 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.
- 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 established LinkedIn page; and presence on the IG community's Oversight.gov website, which enables users to access, sort, and search thousands of previously issued IG reports and other oversight areas of interest.
- Ensured transparency of our work for stakeholders on Oversight.gov by posting press releases related to investigative cases and related actions, in addition to posting our audits and evaluations, and updated on an ongoing basis the status of FDIC OIG recommendations remaining unimplemented, those recommendations that have been closed, and those recommendations that we consider to be priority recommendations.

Administering resources prudently, safely, securely, and efficiently.

- 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.
- 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.

- Continued development and implementation of the OIG's IT infrastructure, in coordination with the Division of Information Technology and the CIOO. The OIG's intent is to deliver robust and modern IT solutions to advance capabilities in supporting the OIG mission; support IT innovation and foster growth of technical skills and talent among OIG users; streamline and digitize information management workflows and processes; minimize development and operational costs; enhance the public relations of the OIG through the Internet-facing website; facilitate sharing of information and best practices; improve the OIG's overall security posture and disaster recovery capabilities; and enhance support for telework and the digital workplace. Kept staff fully apprised of steps they needed to take to ensure the ongoing security of OIG information systems, data, equipment, and electronic devices.

- Continued to refine, adjust, and leverage a new audit management platform, eCase. It creates a system of record to document the work performed and review of that work to support report findings consistent with applicable professional standards. It also allows us to build dashboards to track assignments relative to Office benchmarks; monitor the FDIC's implementation of OIG report recommendations; and ensure that staff meet professional standards. Ensured that that the OIG's new platform complies with the FDIC's system security requirements and has the ability to adapt to new technical requirements and advancements.

- Leveraged the OIG's Electronic Crimes Unit's laboratory. The laboratory allows field Agents to remotely access a server-based lab environment which 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 cyber crimes 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 migrated its first two datasets into the data lake, supporting both audits and investigations. Currently, all OIG employees can access cloud-based data management software. The governance for machine learning and natural language processing tools is in progress and the tools should be accessible by CY25. 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 Paycheck Protection Program fraud through collaboration with the PRAC, the FDIC, the Financial Crimes Enforcement Network, 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, especially in a virtual environment, and to provide component offices more control over and access to information, guidance, and procedures, to better conduct their work.
- 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 began development on seven OIG-specific policies, including a new policy for computer security incident handling (internal to the OIG) and one updated policy covering the OIG's petty cash program.
- Carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. Positions filled during the reporting period included Senior IT Audit Specialists, Senior Operations Specialists, Oversight Manager, Senior Financial Management Analyst, and Special Agents.
- Accomplished a number of human resources initiatives, including processing professional license reimbursements, training requests, and student loan repayment applications; updating OIG position descriptions; and keeping staff informed of important topics such as WebTA, Thrift Savings Plan, TRowe Price, and FedHR 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.
- Successfully engineered, tested, and deployed Windows 11 for OIG staff.
- Transitioned to the GlobalScape tool and provided training to all OIG staff on its use.
- Planned and executed an OIG-wide test of the Emergency Notification System in the interest of preparedness and safety of all OIG staff in the event of an emergency.

- Conducted an Office of Management survey to give FDIC OIG staff an opportunity to provide vital feedback needed to make the OIG a better environment for everyone.
- Commemorated National Whistleblower Appreciation Day by hosting two nationally recognized leaders in whistleblower advocacy from the non-profit Government Accountability Project, who discussed the organization's work in assisting whistleblowers who seek to improve government.

Exercising leadership skills and promoting teamwork.

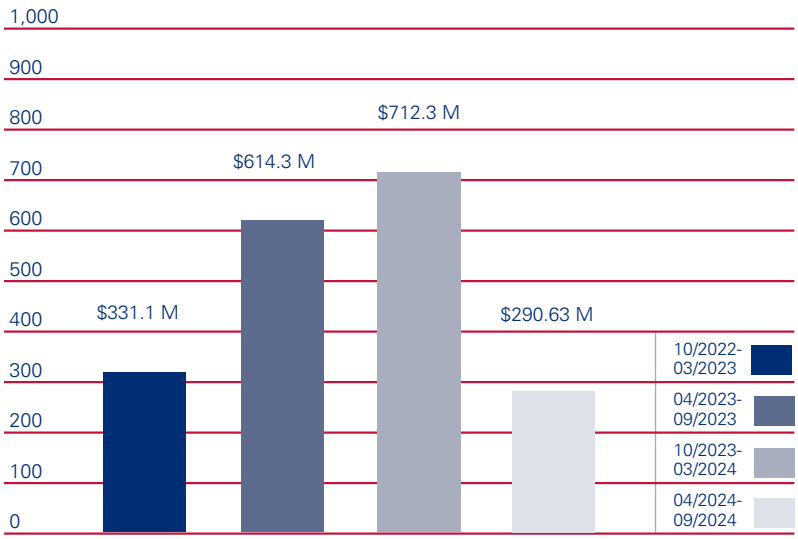
- Held a Town Hall meeting in June, during which updates on telework were shared, and the Management Special Inquiry and Complaint Review Process were discussed.
- Represented the FDIC OIG on the Council of Inspectors General on Integrity and Efficiency's Federal Audit Executive Council. Our Assistant Inspector General for Audits, Evaluations, and Cyber serves as the Council's Chair.
- Held a session for our entire Audits, Evaluations, and Cyber staff on fraud trends that the FDIC OIG Office of Investigations is observing, presented by an FDIC OIG OI Desk Officer.
- Held the FDIC OIG annual awards ceremony to recognize the accomplishments of FDIC OIG colleagues in the areas of leadership; collaboration; innovation; business support; championing Diversity, Equity, Inclusion, and Accessibility; new staff; and OIG excellence.
- Held the Office of Investigations' annual All Hands Training in Charleston, South Carolina. Special Agents from Regional Offices and Headquarters engaged in both classroom and tactical training sessions. The Agents collaborated, sharing their expertise through investigative case studies and participating in classes covering a range of law enforcement and investigative tools and best practices. Additionally, OI enhanced and refreshed their tactical capabilities with training in ballistic shield usage, mechanical breaching techniques, and control tactics.
- Implemented features of the OIG's DEIA Strategic Plan, consisting of four components: *Purpose:* ways in which we strive to inspire each OIG team member to feel connected to our OIG Mission and Vision. This is accomplished through maintaining a diverse workforce in which all are engaged and can bring their authentic selves to the workplace in an environment of safety and acceptance and contribute to the success of the Office. *People:* in order to create a space of belonging in which we foster trusting relationships, invite opinions, and engage in relationship building, recognizing that our accomplishments are not possible without the hard work and dedication of the OIG team. *Processes:* to ensure that we uphold the OIG principles in our recruitment, hiring, promotion, recognition, awards, training, developmental opportunities, operations, procedures, workflows, policies, and technology. *Progress:* to hold ourselves accountable to these strategic goals, we will monitor progress as we mature our DEIA program.

- 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 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; and bimonthly 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, banking schools, and certifications to enhance their expertise and knowledge. These included staff participation at The Graduate School and American University, membership in the Institute of Internal Auditors, and certification through the Association of Certified Fraud Examiners.
- Organized several social activities, including component-specific Coffee Chats, to promote community, teamwork, and collegiality among OIG staff.
- Continued a leadership role in a working group on behalf of CIGIE's Audit and Inspection and Evaluation Committees related to Monetary Impact. The FDIC OIG AIG for Audits, Evaluations, and Cyber and an Audit/Evaluation Manager led a group comprised of representatives from other OIGs across the community. The purpose of the group was to assess and help ensure consistency in how OIGs report and track monetary impacts. The group has issued a guide and conducted training sessions in that regard.
- Shared information from our Engagement and Learning Officer throughout the OIG to promote employee engagement, training, career development, and a positive workplace culture. Among topics covered were improving Federal resume writing and job interview skills.
- Fostered a sense of teamwork and mutual respect through various activities led by the OIG's Diversity, Equity, Inclusion and Accessibility (DEIA) Working Group. Hosted a series of events to highlight diversity, including to recognize Asian American and Pacific Islander Heritage Month, Juneteenth, Whistleblower Appreciation Day, and Women's Equality Day.
- Continued involvement and coordination with CIGIE's Employee Engagement and Innovation Committee. Supported issuance of The Ally Newsletter to share information from the Committee, which works to affirm, advance, and augment CIGIE's commitment to creating and supporting a workplace that is focused on belonging, equity, innovation, and accessibility, throughout the IG community.

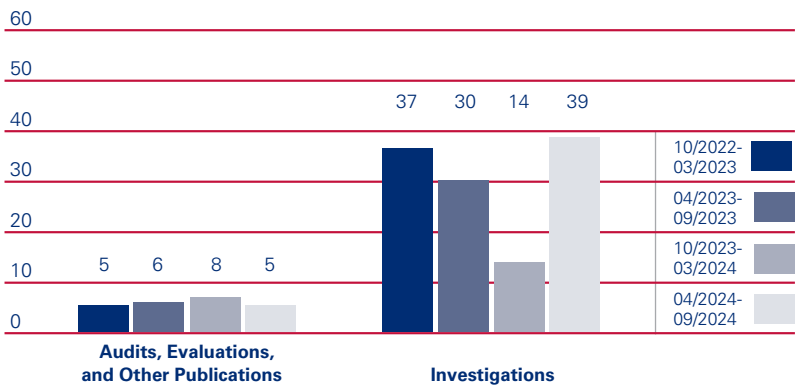
Cumulative Results (2-year period)

Recommendations	
October 2022 – March 2023	56
April 2023 – September 2023	71
October 2023 – March 2024	31
April 2024 – September 2024	42

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



Products Issued and Investigations Closed



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.	4-9
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.)	46-63
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.	64
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.	65
Section 5(a)(7): The information described under section 804(b) of the Federal Financial Management Improvement Act of 1996.	65
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.	68-69

Reporting Requirements (continued)	Page
Section 5(a)(9): A list of any outstanding recommendations from any peer review conducted by another Office of Inspector General that have not been fully implemented, including a statement describing the status of the implementation and why implementation is not complete.	68-69
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.	68-69
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.	65
Section 5(a)(12): A description of metrics used for Section 5(a)(11) information.	65
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.	65
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.	66
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.	66
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.	66

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, as presented in a letter to the Executive Chairperson of CIGIE, the Deputy Director for Management, Office of Management and Budget. As stated in the letter, if enacted, these CIGIE Legislative Priorities for the 118th Congress would provide much needed tools and authorities for strengthening independent government oversight:

- Prohibiting the Use of Appropriated Funds Government-wide to Deny IGs Full and Prompt Access
- Improving CIGIE Transparency and Accountability through a Single Appropriation
- Permanent Data and Analytics Capability for the IG Community
- Enhancing Independence and Efficiency by Providing Separate and Flexible OIG Funding
- Establishing Authority for IGs to Provide Continuous Oversight During a Lapse in Appropriations
- Testimonial Subpoena Authority.

Additional recommended good government reforms supported by CIGIE that will help strengthen government oversight were also included in the letter:

- Reforming the Program Fraud Civil Remedies Act
- Protecting Cybersecurity Vulnerability Information
- Congressional Notification When Legislative Branch IGs are Placed on Non-Duty Status
- Statutory Exclusion for Felony Fraud Convicts to Protect Federal Funds
- Enhancing CIGIE's Role in Recommending IG Candidates.

Of note, during the reporting period, on July 23, 2024, Honorable Mark Greenblatt, Chairperson of CIGIE and U.S. Department of the Interior IG testified before the House Committee on Oversight and Accountability, Subcommittee on Government Operations and the Federal Workforce on "Oversight of the Council of the Inspectors General on Integrity and Efficiency." He focused on three of the legislative priorities: (1) creating a permanent data and analytics capability for the IG community; (2) establishing a Government-wide prohibition on the use of appropriated funds to deny IGs full and prompt access; and (3) enhancing independence and efficiency by providing separate and flexible OIG funding.

The Legislation Committee subsequently continued to engage with the Congress on CIGIE's legislative priority on Permanent Data and Analytics Capability for the IG Community. The Committee also engaged with the Congress on the issue of the IG pay freeze, which has been in effect since 2014 and shared updated information on legislative mandates that impact the IG community and individual IGs.

In anticipation of the 119th Congress, the Committee reviewed and summarized the status of each CIGIE Legislative Priority for the 118th Congress. The summary will be useful in assessing whether to include each of the 118th priorities in the 119th Letter. The Committee has also solicited new proposals for consideration for inclusion in the CIGIE Legislative Priorities Letter for the 119th Congress.

Table I: Unimplemented Recommendations from Previous Semiannual Periods

Notes:

1. A current listing of each of the unimplemented recommendations is available at https://www.fdicoig.gov/unimplemented-recommendations. The listing is updated monthly.
2. Recommendations open for more than one year are marked **. These total 44 recommendations.
3. Each report summary notes the specific recommendations that are unimplemented.

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-20-001 **Contract Oversight Management** October 28, 2019	The FDIC relies heavily on contractors for support of its mission, especially for information technology, receivership, and administrative support services. Over a 5-year period from 2013 to 2017, the FDIC awarded 5,144 contracts valued at $3.2 billion. We conducted an evaluation to assess the FDIC's contract oversight management, including its oversight and monitoring of contracts using its contracting management information system; the capacity of Oversight Managers to oversee assigned contracts; Oversight Manager training and certifications; and security risks posed by contractors and their personnel. We concluded that the FDIC must strengthen its contract oversight management. Specifically, we found that the FDIC was overseeing its contracts on a contract-by-contract basis rather than a portfolio basis and did not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency. We also found that the FDIC's contracting files were missing certain required documents, Personally Identifiable Information was improperly stored, some Oversight Managers lacked workload capacity to oversee contracts, and certain Oversight Managers were not properly trained or certified. The report contained 12 recommendations to strengthen contract oversight. Recommendation 2 is unimplemented.	12	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-22-003 **Sharing of Threat Information to Guide the Supervision of Financial Institutions** January 18, 2022	To fulfill its mission, the FDIC acquires, analyzes, and disseminates threat information relating to cyber and other threats to the financial sector and FDIC operations. Effective sharing of threat information enriches situational awareness, supports informed decision-making, and guides supervisory strategies and policies. We conducted an audit to determine whether the FDIC established effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. We found that the FDIC did not establish effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. The FDIC acquired and analyzed certain information pertaining to threats against financial institutions and disseminated some information to certain supervisory personnel. However, we identified gaps in each component of the Threat Sharing Framework: Acquisition, Analysis, Dissemination, and Feedback. The report contained 25 recommendations to strengthen the FDIC's processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. Recommendation 8 is unimplemented.	25	1**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-22-004 **The FDIC's Information Security Program - 2022** 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 Total	Recommendations Outstanding	Potential Cost Savings
REV-23-001 **Security Controls Over the FDIC's Wireless Networks** 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 Total	Recommendations Outstanding	Potential Cost Savings
AUD-23-001 **Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program** January 31, 2023	The FDIC conducts information technology (IT) examinations to evaluate bank management's ability to identify IT and cyber risks and maintain appropriate compensating controls. We conducted an audit to determine whether the FDIC's IT Risk Examination (InTREx) program effectively assesses and addresses IT and cyber risks at financial institutions. We found that the FDIC needed to improve its InTREx program to effectively assess and address IT and cyber risks at financial institutions, as follows: • The InTREx program was outdated and did not reflect current Federal guidance and frameworks for three of four InTREx Core Modules; • The FDIC did not communicate or provide guidance to its examiners after updates were made to the program; • FDIC examiners did not complete InTREx examination procedures and decision factors required to support examination findings and examination ratings; • The FDIC had not employed a supervisory process to review IT workpapers prior to the completion of the examination, in order to ensure that findings were sufficiently supported and accurate; • The FDIC did not offer training to reinforce InTREx program procedures to promote consistent completion of IT examination procedures and decision factors; • The FDIC's examination policy and InTREx procedures were unclear, which led examiners to file IT examinations workpapers in an inconsistent and untimely manner; • The FDIC did not provide guidance to examination staff on reviewing threat information to remain apprised of emerging IT threats and those specific to financial institutions; • The FDIC was not fully utilizing available data and analytic tools to improve the InTREx program and identify emerging IT risks; and • The FDIC had not established goals and performance metrics to measure its progress in implementing the InTREx program. The report contained 19 recommendations to strengthen the InTREx program. Recommendation 17 is unimplemented.	19	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 **The FDIC's Security Controls Over Microsoft Windows Active Directory** 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. Recommendations 10, 11, and 12 are unimplemented.	15	3**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
REV-23-002 **FDIC's Oversight of a Telecommunications Contract** 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	
AUD-23-003 **The FDIC's Adoption of Cloud Computing Services** July 25, 2023	The FDIC began limited operations in the cloud in September 2016. In 2021, the FDIC accelerated its movement into the cloud after the White House issued Executive Order 14028, Improving the Nation's Cybersecurity (2021), which required that the head of each agency update existing plans to prioritize the adoption and use of cloud technology, and provide a report to the Office of Management and Budget (OMB) detailing that plan. Since then, the FDIC has been reducing its on-premises infrastructure and modernizing its IT portfolio by migrating to the cloud. We conducted an audit to determine whether the FDIC had an effective strategy and governance processes to manage its cloud computing services. Overall, the FDIC had an effective strategy and governance processes to manage its cloud computing services. However, the FDIC did not adhere to several cloud-related practices recommended by OMB, National Institute of Standards and Technology, and FDIC guidance in 4 of the 11 areas we assessed: data governance, cloud exit strategy, contract management plans, and decommissioning plans for legacy systems. The audit also found that the FDIC had effective controls in the remaining seven control areas assessed related to application rationalization, IT governance bodies' alignment, cloud expenditures, cloud workforce transformation, assessment and authorization, continuous monitoring, and business continuity. The report contained nine recommendations to strengthen the strategy and governance over the FDIC's adoption of cloud computing services. Recommendations 1, 2, and 9 are unimplemented.	9	3**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-23-002 **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 United States 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 1, 5, 6, 7, 8, and 10 are unimplemented.	10	6**	NA

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

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

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-23-003 **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. Recommendations 1, 3, 4, 5, 6, 7, 8, 9, 11, 12, and 13 are unimplemented.	14	11**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-23-004 **The FDIC's Orderly Liquidation Authority** September 28, 2023	Before the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (DFA), the FDIC only had the authority to resolve FDIC-insured depository institutions. Title II of the DFA, Orderly Liquidation Authority (OLA), aimed to provide the necessary authority to the FDIC to liquidate failing financial companies that pose a significant risk to the financial stability of the United States in a manner that mitigates such risk and minimizes moral hazard. Our evaluation objective was 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 SIFCs 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, 5, 6, 7, 8, 9, 11, 12, 14, 15, 16, and 17 are unimplemented.	17	14**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-24-01 **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	

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-24-02 **Material Loss Review of Signature Bank of New York** October 23, 2023	On March 12, 2023, the New York State Department of Financial Services closed Signature Bank of New York (SBNY) and appointed the FDIC as receiver. On April 28, 2023, the FDIC estimated the loss to the Deposit Insurance Fund (DIF) to be approximately $2.4 billion. We engaged Cotton & Company Assurance and Advisory, LLC (Cotton) to perform a Material Loss Review. The objectives were to (1) determine why the bank's problems resulted in a material loss to the DIF, and (2) evaluate the FDIC's supervision of the bank, including the FDIC's implementation of the Prompt Corrective Action (PCA) requirements of section 38 of the Federal Deposit Insurance Act, and make recommendations for preventing any such loss in the future. SBNY's failure was caused by insufficient liquidity and contingency funding mechanisms, which impeded the bank's ability to withstand a run on deposits. In addition, SBNY management prioritized aggressive growth over the implementation of sound risk management practices needed to counterbalance the liquidity risk associated with concentrations in uninsured deposits. Cotton found that the FDIC: • Missed opportunities to downgrade SBNY's Management component rating and further escalate supervisory concerns; • Did not consistently perform supervisory activities in a timely manner and was repeatedly delayed in issuing supervisory products; • Appropriately downgraded SBNY's Liquidity component rating, but changing market conditions warrant the FDIC's review and potential revision of examination guidance; and • Determined that SBNY was well capitalized throughout each examination cycle prior to its failure based on defined capital measures. Cotton made six recommendations intended to improve the FDIC's supervision processes and its ability to apply effective forward-looking supervision in a changing banking environment. Recommendations 1, 2, 3, 4, and 5 are unimplemented.	6	5	

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-24-03 **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 First Republic Bank's component ratings consistent with the FDIC's forward-looking supervisory approach; • The FDIC assessed First Republic 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 • First Republic 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	

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AEC Memorandum-24-01 **The FDIC's Regional Service Provider Examination Program** 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, we identified several opportunities to improve the RSP examination program by: (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	

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-24-04 **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, 2, and 3 are unimplemented.	3	3	$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, 3, 4, 5, 7, and 8 are unimplemented.	8	6	

Table II: Audit and Evaluation Reports				
Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	Title*	Total	Unsupported	
Immediate Office Communication-24-01 May 23, 2024	*Management Advisory Memorandum on Reporting Allegations of Misconduct*			
EVAL-24-05 July 31, 2024	*The FDIC's Sexual Harassment Prevention Program*			
AUD-24-01 September 4, 2024	*Security Controls for the FDIC's Cloud Computing Environment*			
EVAL-24-06 September 23, 2024	*Conflicts of Interest in the Acquisition Process*			
EVAL-24-07 September 25, 2024	*The FDIC's Information Security Program - 2024*			
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 no unresolved management decisions on OIG recommendations from past reporting periods to note.

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	39
Number of Persons Referred to the Department of Justice for Criminal Prosecution	60
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	1
Number of Indictments and Criminal Informations	81

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

Senior FDIC Employee Misconduct – Conflict of Interest:

During this reporting period, we investigated a Senior FDIC Employee who worked personally and substantially on the contract of a vendor in which the Senior Employee held a significant financial stake. The Senior Employee's official position at the FDIC and financial stake in the vendor company represented a prohibited conflict of interest under Federal law. As a result of the investigation, the Senior Employee was issued a Letter of Reprimand and reassigned to a new position from the conflicted position in order to eliminate the conflict.

Senior FDIC Employee Misconduct – Conflict of Interest:

During this reporting period, we investigated an additional Senior FDIC Employee who worked personally and substantially on the contract of a vendor in which the Senior Employee held a significant financial stake. The Senior Employee's official position at the FDIC and financial stake in the vendor company represented a prohibited conflict of interest under Federal law. As a result of the investigation, the Senior Employee was issued a Letter of Reprimand and reassigned to a new position from the conflicted position in order to eliminate the conflict.

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

G. 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.

H. 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. There were no investigations of senior government officials that were closed and not disclosed publicly.

Additional Reporting in Response to Section 10(c) of Executive Order 14074
Section 10(c) of Executive Order 14074 calls for the heads of Federal law enforcement agencies to issue annual reports to the President – and to post those reports publicly – setting forth the number of no-knock entries that occurred pursuant to judicial authorization; the number of no-knock entries that occurred pursuant to exigent circumstances; and disaggregated data by circumstances for no-knock entries in which a law enforcement officer or other person was injured in the course of a no-knock entry. The information below sets forth the public reporting of FDIC OIG's No Knock Entries:

For this semiannual reporting period there have been no circumstances in which an FDIC OIG Special Agent executed a court-authorized no-knock entry or executed a no-knock entry pursuant to exigent circumstances.

Appendix 2

Information on Failure Review Activity

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

FDIC OIG Review Activity for the Period April 1, 2024, through September 30, 2024 (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 incurs a loss under $50 million, Section 38(k) of the Federal Deposit Insurance 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 were no Failed Bank Reviews in process.

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.fdicoig.gov/reports-publications/peer-reviews/external-peer-review-report-federal-deposit-insurance-corporation

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 Offices of Inspector General with Statutory Law Enforcement Authority and Section 6(e) of the Inspector General Act of 1978, as amended. Those documents authorize law enforcement powers for eligible personnel of each of the various Offices of Inspectors General. Law enforcement powers may be exercised only for activities authorized by the IG Act, other statutes, or as expressly authorized by the Attorney General.

On November 21, 2023, the VA OIG reported that in its opinion, the system of internal safeguards and management procedures for the investigative function of 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.

Congratulations to FDIC OIG CIGIE Award Winners

We are proud of the members of the FDIC OIG who will be recognized at the IG Community's Annual Awards Ceremony in November 2024 for excellent work conducted during the past year.

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, FRB OIG, and the U.S. Attorney's Office, Eastern District of Louisiana.

*****

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

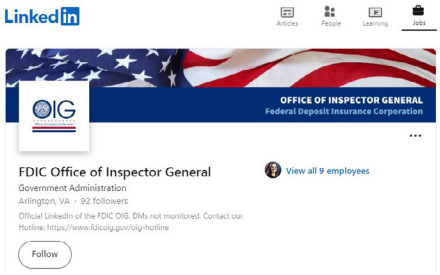
Texas Star Services Investigation Team—Excellence—Investigations
In recognition of remarkable investigative efforts leading to the successful prosecution of a multi-million-dollar, multi-defendant Paycheck Protection Program Recruitment Fraud Scheme, along with the additional successful efforts to identify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

DESIGN: FDIC/OCOM/GRAPHIC DESIGN AND PRINTING UNIT

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

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

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



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

OVERSIGHT.GOV
ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE

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

PANDEMIC RESPONSE ACCOUNTABILITY COMMITTEE

www.pandemicoversight.gov

★**Learn more about the IG community's commitment to belonging, equity, innovation, and accessibility.** Visit: **www.ignet.gov**.

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

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

FDIC-038-2024