

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

October 1, 2023 – March 31, 2024



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 5,952 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured \$17.34 trillion in domestic deposits in 4,587 institutions, of which the FDIC supervised 2,930. The Deposit Insurance Fund balance totaled \$121.8 billion as of December 31, 2023. Active receiverships as of March 31, 2024 totaled 65, with assets in liquidation of about \$39.3 billion.





Semiannual Report to the Congress

October 1, 2023 – March 31, 2024



Federal Deposit Insurance Corporation



Inspector General's Statement



On behalf of the Office of Inspector General (OIG) at the Federal Deposit Insurance Corporation (FDIC), I am pleased to present our Semiannual Report for the period October 1, 2023 through March 31, 2024.

I was sworn in as Inspector General (IG) of the FDIC on January 11, 2024. At my confirmation hearing before the Senate Banking Committee, I stated that it would be an honor to serve as the Inspector General of the FDIC. That has proven true. I also added that I would be committed to delivering results in an independent and objective manner on the effectiveness and efficiency of FDIC programs and operations, which ultimately would benefit the American people. Over the past 6 months, through the dedicated efforts of our staff, the FDIC OIG has done that. We are conducting important oversight work on behalf of the American people. 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 eight reports, including our Top Management and Performance Challenges report, and other significant audit and evaluation-related reports covering key areas of FDIC programs and operations. Among reports issued were Material Loss Reviews of the failures of two FDIC-supervised banks: Signature Bank of New York, with losses to the Deposit Insurance Fund (DIF) estimated at \$2.4 billion, and First Republic Bank, with estimated losses to the DIF of \$15.6 billion. Other reports addressed FDIC Strategies Related to Crypto-Asset Risks, the FDIC's Regional Service Provider Examination Program, the Purchase and Deployment of the FDIC's Acquisition Management System, the FDIC's Ransomware Readiness, and a Failed Bank Review of Citizens Bank, Sac City, Iowa. We made 31 recommendations in these reports designed to strengthen controls to address identified risks, and in one report, identified \$9.9 million in funds that could be put to better use. We continue to monitor the FDIC's implementation of these recommendations.

As for Investigations, we are helping to maintain and preserve the integrity of the banking sector and to deter financial fraud. One successful case that we update in this report involves the former President and Chief Executive Officer of the failed First NBC Bank, a prominent New Orleans banker, who was sentenced to 14 years and 2 months of imprisonment for bank fraud and making false statements in bank records. He was ordered to pay more than \$214 million in restitution to the FDIC. This investigation unraveled a multi-year fraud by senior bank officials and the largest bank borrowers, which triggered both a \$1 billion loss to the FDIC and loss of jobs for more than 500 employees. We highlight the sentencing of the bank's former Counsel and two customers in this report.

Overall, FDIC OIG investigations during the reporting period resulted in 82 indictments, 53 convictions, 67 arrests, and more than \$712 million in fines, restitution ordered, and other monetary recoveries. Notably, these results include the FDIC OIG's efforts in cases related to fraud in the Federal government's COVID-19 pandemic response, which resulted in 33 indictments and informations, 32 arrests, and 24 convictions. Monetary benefits resulting from these types of cases alone totaled in excess of \$54.9 million—more than double the amount reported in our last semiannual report. We continue to play a significant role within the law enforcement community in combating this fraud, and since inception of the CARES Act, have been involved in 197 such cases.

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 working groups throughout the country. Most recently, our Assistant Inspector General for Audits, Evaluations, and Cyber, Terry Gibson, took on the leadership role as Chair of the Federal Audit Executive Council. Responsibilities of that Council include coordinating joint audit projects, providing input on policies related to Federal government audits, and coordinating with other agencies, including the Government Accountability Office, Office of Management and Budget, and others on significant matters affecting audit policy.

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 Office to be headed by an IG who would function under the general supervision of the FDIC Chairman. We recently marked our 35th Anniversary of providing independent oversight of 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 continue to carry out the OIG mission in service to the American people. I also wish to acknowledge Tyler Smith and Mike McCarthy from our Office who admirably served as Acting IG and Deputy IG, respectively, prior to my swearing-in.

To all OIG staff past and present, I say thank you for the valuable contributions you have made to our Office and to the FDIC since 1989.

/s/

Jennifer L. Fain
Inspector General
April 2024



Table of Contents

Inspector General's Statement	i
Acronyms and Abbreviations	2
Introduction and Overall Results	3
Audits, Evaluations, and Other Reviews	4
Investigations	16
Other Key Priorities	32
Cumulative Results	42
Reporting Requirements	43
Appendix 1 Information in Response to Reporting Requirements	45
Appendix 2 Information on Failure Review Activity	63
Appendix 3 Peer Review Activity	64
Congratulations	67

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



Acronyms and Abbreviations

AEC	Audits, Evaluations, and Cyber
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CFETF	COVID-19 Fraud Enforcement Task Force
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIOO	Chief Information Officer Organization
COVID-19	Coronavirus Disease 2019
DEIA	Diversity, Equity, Inclusion, and Accessibility
DIF	Deposit Insurance Fund
DOJ	Department of Justice
ECU	Electronic Crimes Unit
FAEC	Federal Audit Executive Council
FAMS	FDIC Acquisition Management System
FBI	Federal Bureau of Investigation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act of 2014
IDOB	Iowa Division of Banking
IG	Inspector General
InTREx	Information Technology Risk Examination
IRS-CI	Internal Revenue Service-Criminal Investigation
MCA	Merchant Cash Advance
NLEAD	National Law Enforcement Accountability Database
NRC	Nuclear Regulatory Commission
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCA	Prompt Corrective Action
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
USPS	United States Postal Service



Introduction and Overall Results

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

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

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

Overall Results (October 1, 2023–March 31, 2024)	
Audit, Evaluation, and Other Products Issued	8
Recommendations	31
Investigations Opened	45
Investigations Closed	14
Judicial Actions:	
Indictments/Informations	82
Convictions	53
Arrests	67
OIG Investigations Resulted in:	
Special Assessments	\$8,900.00
Fines	\$534,300.00
Restitution	\$221,991,753.32
Asset Forfeitures	\$486,729,401.59
Civil Money Penalties	\$3,000,000.00
Total	\$712,264,354.91
Referrals to the Department of Justice (U.S. Attorney)	74
Investigative Reports Referred to FDIC Management for Action	5
Responses to Requests Under the Freedom of Information/Privacy Act	22
Subpoenas Issued	3



Audits, Evaluations, and Other Reviews

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

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

During the reporting period, we issued seven reports addressing key areas in information technology, contracting, and supervision. We made a total of 31 recommendations for improvements to FDIC programs and operations in these reports. We also identified \$9.9 million in funds put to better use in one of these reports.

We note that in addition to planned discretionary work, under the Federal Deposit Insurance (FDI) Act, our Office is statutorily required to review the failures of FDIC-supervised institutions causing material losses to the Deposit Insurance Fund (DIF) if those occur. The materiality threshold is currently set at \$50 million. On March 12, 2023, Signature Bank of New York, an FDIC-supervised institution failed, with losses to the DIF estimated at \$2.4 billion. On May 1, 2023, First Republic Bank, also FDIC-supervised, failed with estimated losses to the DIF of \$15.6 billion. Our Office completed Material Loss Reviews of these failures during this semiannual reporting period.

If the losses are less than the material loss threshold, the FDI Act requires the Inspector General of the appropriate Federal banking agency to determine the grounds upon which the state or Federal banking agency appointed the FDIC as receiver and whether any unusual circumstances exist that might warrant an In-Depth Review of the loss. During the reporting period, we conducted one Failed Bank Review of Citizens Bank, Sac City, Iowa, to make that determination and found no circumstances warranting further review.

Results of the audits, evaluations, and other reviews completed during the reporting period are summarized below. We also include a summary of issuance of an eighth product: our Top Management and Performance report, which we issued in February. 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. Postal Service 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.

Importantly, in December 2023, the OIG announced two assignments that the office has 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 is the evaluation of the FDIC's Sexual Harassment Prevention Program. The assignment's objective is 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 is a follow-up evaluation to our July 2020 report entitled, *Preventing and Addressing Sexual Harassment*, EVAL-20-006.

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 devoting substantial resources to both of these assignments and will report the results of these efforts in an upcoming semiannual report.

Audits, Evaluations, and Other Reviews

FDIC Strategies Related to Crypto-Asset Risks

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. While currently limited, if material exposure of financial institutions to the risks posed by crypto-related activities were to manifest, it may affect the FDIC's mission to maintain stability and public confidence in the Nation's financial system. We conducted a review to determine whether the FDIC has developed and implemented strategies that address the risks posed by crypto assets.

We determined that the FDIC has started to develop and implement strategies that address the risks posed by crypto assets. However, the Agency has not assessed the significance and potential impact of the risks. Specifically, the FDIC has not yet completed a risk assessment to determine whether the Agency can 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 is 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.

Until the FDIC assesses the risks of crypto activities and provides supervised institutions with effective guidance, the FDIC and some FDIC-supervised institutions may not take appropriate actions to address the most significant risks posed by crypto assets. In addition, based on evidence obtained during our evaluation, the FDIC's lack of clear procedures causes uncertainty for supervised institutions in determining the appropriate actions to take. If financial institutions do not receive timely feedback from the FDIC and do not understand what constitutes the end of the FDIC's review process, this uncertainty creates risk that the FDIC will be viewed as not being supportive of financial institutions engaging in crypto-related activities.

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. The FDIC concurred with both recommendations and planned to complete corrective actions by January 30, 2024.

Material Loss Review of Signature Bank of New York

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 to be approximately \$2.4 billion.

Under a contract overseen by the OIG, Cotton & Company Assurance and Advisory, LLC (Cotton) performed the Material Loss Review (MLR). The objectives of the engagement were to (1) determine why the bank's problems resulted in a material loss to the Deposit Insurance Fund, 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. The FDIC concurred with all of the recommendations and planned to complete corrective actions by March 31, 2024.

Material Loss Review of First Republic Bank

Several months after the failure of Signature Bank as discussed above, 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 of \$15.6 billion.

Under another contract overseen by the OIG, Cotton & Company Assurance and Advisory, LLC performed the Material Loss Review. Similar to the MLR of Signature Bank, the objectives of the engagement were to (1) determine why the bank's problems resulted in a material loss to the Deposit Insurance Fund, and (2) evaluate the FDIC's supervision of the bank, including the FDIC's implementation of the PCA 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 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 warrants 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. The FDIC concurred with all of the recommendations and plans to complete corrective actions by July 31, 2024.

The FDIC's Regional Service Provider Examination Program

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. Specifically, the Act states that the services authorized under the Act are "...subject to regulation and examination ...to the same extent as if such services were being performed by the bank itself on its own premises."

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). We conducted an audit that focused on RSPs, which are smaller in size, less complex, and provide services to banks within a local region.

We conducted the 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.

Overall, we found that the FDIC had 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 noted these ways to improve the RSP examination program: (1) monitor reports of examination distribution timeliness; (2) comply with examination frequency guidelines; (3) provide additional guidance on how to use RSP examinations in support of the FDIC's InTREx program; and (4) establish 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, as identified in the memorandum. The FDIC agreed to take action on the recommendation by December 31, 2024.

The FDIC's Purchase and Deployment of the FDIC Acquisition Management System

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 (FAMS) and identify improvements for implementing future significant organizational changes.

We determined that the FDIC's deployment of FAMS was unsuccessful because the FDIC did not employ an effective change management process. The FDIC did not employ an effective change management process because 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.

If the FDIC had developed and implemented an effective change management process from conception of the change throughout the entire change process, then FDIC managers and employees would have had the opportunity to:

- Obtain a greater understanding of, and acceptance for, the changes;
- Engage more proactively in the process to develop and implement a new system;
- Implement the desired technological, structural, and procedural changes to ensure the FDIC's performance and achievement of its mission and goals; and
- Ultimately adopt and successfully implement the FDIC's new acquisition management system.

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, and are reporting this amount in this Semiannual Report to the Congress. This amount would be realized over time as the FDIC achieves better outcomes when implementing future change initiatives. The FDIC concurred with all of the recommendations and the funds to be put to better use. The FDIC plans to complete corrective actions by December 31, 2024.

Review of the FDIC's Ransomware Readiness

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. With this in mind, we conducted a review to assess the adequacy of the FDIC's process to respond to a ransomware incident. Ransomware prevention and detection measures were not in the scope of this review. Similarly, this review was not a comprehensive review of data governance or incident response.

Overall, 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 and restoring from backup data; (2) Continuity Implementation Plan maintenance; (3) Wireless Priority Service access; and (4) Disaster Recovery Awareness training.

We made eight recommendations for the FDIC: (1) evaluate and implement solutions to protect backup data; (2) evaluate and consider enhanced solutions to store backup data; (3) review and update policies and procedures to ensure timely control implementation of new Federal requirements; (4) test recovery of Active Directory from backups; (5) ensure the Continuity Implementation Plan is regularly updated in a timely manner to ensure it is current, complete, and accurate; (6) periodically review and update key personnel enrolled in Wireless Priority Service and perform quarterly testing as part of its Emergency Communications Program; and ensure that key individuals complete (7) initial and (8) subsequent annual Disaster Recovery Awareness training. The FDIC concurred with all of the recommendations and plans to complete corrective actions by February 28, 2025.

Failed Bank Review of Citizens Bank, Sac City, Iowa

On November 3, 2023, the Iowa Division of Banking (IDOB) closed Citizens Bank and appointed the FDIC as receiver. According to the FDIC's Division of Finance, the estimated loss to the DIF was \$14.8 million or 23 percent of the bank's \$65 million in total assets. Following a period of supervisory actions by regulators, the IDOB took possession and closed Citizens Bank during an ongoing examination because FDIC and IDOB examiners found significant loan losses in the loan portfolio. These loan losses eroded the institution's capital and earnings position and the bank had become insolvent.

When the DIF incurs a loss under \$50 million, the FDI Act requires the Inspector General of the appropriate federal banking agency to determine the grounds identified by the state or federal banking agency for appointing the FDIC as receiver and to determine whether any unusual circumstances exist that might warrant an In-Depth Review of the loss.

The OIG considers a series of factors to determine whether unusual circumstances warrant an In-Depth Review. These factors include: (1) the magnitude and significance of the loss to the DIF in relation to the total assets of the failed institution; (2) the extent to which the FDIC's supervision identified and effectively addressed the issues that led to the bank's failure or the loss to the DIF; (3) indicators of fraudulent activity that significantly contributed to the loss to the DIF; and (4) other relevant conditions or circumstances that significantly contributed to the bank's failure or the loss to the DIF.

Citizens Bank's failure occurred primarily due to insufficient Board and management oversight of its credit administration practices. Specifically, the bank issued loans to commercial trucking clients without adequate credit underwriting, risk management practices, or adequate expertise. When the commercial trucking industry began to experience supply-chain and financial issues, management compounded its risk by extending credit through overdrafts, without properly assessing these additional risks. Citizen Bank's Board and management also failed to complete recommended corrective actions to improve the bank's safety and soundness. The significant loan losses eroded Citizens Bank's capital levels and liquidity position, and ultimately led to the bank's failure.

Our review did not find unusual circumstances that warranted an In-Depth Review of the loss.

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.

We identified nine Top Challenges facing the FDIC. The Challenges identify risks to FDIC mission-critical activities and to FDIC internal programs and processes that support mission execution. These Challenges include all aspects of the Challenges that we reported last year, with important updates. Among these updates are 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 note 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 are identified, consistent with the FDIC’s forward-looking supervision initiative. Further, 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.
- **Audit of Security Controls for the FDIC's Cloud Computing Environment:** The objective is to assess the effectiveness of security controls for the FDIC's cloud computing environment.
- **Evaluation of the FDIC's Sexual Harassment Prevention Program:** The objective is 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 is a follow-up evaluation to our July 2020 report entitled *Preventing and Addressing Sexual Harassment*, EVAL 20-006.
- **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.
- **Conflicts of Interest in the Acquisition Process:** The objective is 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.
- **Federal Information Security Management Act – 2024:** The evaluation objective is to evaluate the effectiveness of the FDIC's information security program and practices.

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

Issuance of Peer Review of the U.S. Postal Service OIG's Inspection and Evaluation Function

Our Office of Audits, Evaluations, and Cyber completed its peer review of the U.S. Postal Service (USPS) OIG's compliance with the *CIGIE Quality Standards for Inspection and Evaluation*, December 2020 (Blue Book). The peer review was conducted from October 19, 2023 through March 27, 2024. The team issued its report on March 27, 2024.

Our FDIC Review Team determined that the USPS OIG's policies and procedures generally were consistent with the Blue Book standards addressed in the external peer review. All three reports that the team reviewed generally complied with the Blue Book standards. In addition to the report, the team issued a Letter of Comment that described findings that were not considered to significantly impact compliance with a Blue Book standard. USPS OIG agreed with four recommended actions in the Letter of Comment.

Update on Earlier Issue Raised Related to OIG Email Security

In previous semiannual reports, beginning for the period ending September 30, 2022, we noted that the FDIC process for emails included manual review by the FDIC (FDIC employees and/or contractors) of messages flagged by automated tools. 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, and safety risks that emails relevant to urgent law enforcement matters would not be received by the OIG in a timely manner.

In March 2023, the CIOO provided a plan to update systems and processes to ensure the confidential and timely receipt of OIG email from complainants, whistleblowers, and law enforcement partners. The FDIC approved funding to further the steps that the CIOO intends to take during 2024 to modernize the FDIC and OIG email infrastructure. As an update, the CIOO communicated the project is on track for completion in 2024. Successful implementation, to include the resolution of technical challenges, is critical to meet the OIG's mission and maintain its independence.



Investigations

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

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

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

FDIC OIG investigations during the reporting period resulted in 82 indictments/informations, 53 convictions, 67 arrests, and more than \$712 million in fines, restitution ordered, and other monetary recoveries. We opened 45 cases and closed 14 during the reporting period. We referred five investigative reports to FDIC management for action.

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 (BWC) program for all law enforcement officers and ensure the use of the BWCs in all appropriate circumstances, including during arrests and searches.

Our Office of Investigations (OI) successfully implemented its BWC 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 incorporated the training as part of our New Agent Training during the reporting period.

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.

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, 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.fdicigoig.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.

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 (CFETF). DOJ released its Annual Report highlighting the success of the CFETF 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, CFETF 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 197 such cases.

Notably, during the reporting period, the FDIC OIG's efforts related to the Federal government's Coronavirus Disease-2019 (COVID-19) pandemic response resulted in 33 charging actions (indictments, informations, and superseding indictments and informations), 32 arrests, and 24 convictions involving fraud in the CARES Act Programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases totaled in excess of \$54.9 million—more than double 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. We are migrating our first 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 OIG 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 later in this report, during the reporting period, 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.

Former 1 Global Capital Chairman Sentenced for Role in \$250 Million Securities Fraud Scheme

Carl Ruderman was sentenced to 60 months of imprisonment and 3 years of supervised release in the Southern District of Florida.

Ruderman previously pled guilty to one count of conspiracy to commit securities fraud. He was the Chairman of 1 Global Capital, LLC, a commercial lending business that made the equivalent of “pay day” loans to small businesses at high interest rates, termed merchant cash advance loans or MCAs. To fund these loans, 1 Global Capital, LLC obtained funds from investors, offering short-term investment contracts that promised to use the investors’ money to fund the MCAs and to provide investors a proportionate share of the principal and interest payments as the loans were repaid. In order to raise capital and attract investors, Ruderman and others made false and misleading representations to investors and potential investors as to the profitability of 1 Global Capital, LLC’s business in marketing materials and periodic account statements. Investors were also falsely told that 1 Global Capital, LLC had financials that had been audited by a public accounting firm, that the investors’ money would be spent on the MCAs, and that they could expect double-digit returns on their investments, among other things.

In addition to investors, Ruderman also defrauded Community National Bank, now BNB Bank, by deliberately misrepresenting assets and income in order to obtain a modification to the terms of a loan obtained from the bank and to convince the bank to dismiss a lawsuit based on the misrepresentations. Ruderman took out a \$4 million loan funded through Community National Bank, now BNB Bank, of which \$3 million was backed by the Small Business Administration through its 7(a) loan program. The loan was purportedly to be used as working capital for a nutraceutical business Ruderman owned at the time. Ruderman and his wife were required to personally guarantee the loan in full.

Ruderman and his co-conspirators at 1 Global Capital, LLC were the subjects of an approximately \$330 million securities fraud scheme involving the MCAs and were previously charged civilly by the Securities and Exchange Commission.

Source: USAO, Southern District of Florida.

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

Prosecuted by the USAO, Southern District of Florida.

Former Bank Counsel and Two Bank Customers Sentenced for Conspiracy to Defraud First NBC Bank

Gregory St. Angelo, former counsel to First NBC Bank, New Orleans, LA, was sentenced to 4 years in prison and 5 years of supervised release for conspiracy to commit bank fraud. Warren G. Treme, a First NBC Bank customer, was sentenced to 24 months in federal prison and 36 months of supervised release for his role in the same conspiracy. Arvind Vira, another First NBC Bank customer, was sentenced to one year and a day, and 36 months of supervised release for his role in the conspiracy. Vira was also ordered to pay \$800,000 in restitution to the FDIC and forfeit \$420,271.07 to the government.

Between 2006 and April 2017, St. Angelo conspired with First NBC Bank President Ashton Ryan and others to provide First NBC Bank with materially false and fraudulent documents and personal financial statements, which, among other things, overstated the value of St. Angelo's and his entities' assets, understated their liabilities, and omitted material information. The materially false and fraudulent personal financial statements, collateral summaries, and other documents concealed St. Angelo's and his entities' true financial condition. The bank president and others disguised St. Angelo's and his entities' true financial condition by, among other things, issuing new loans to St. Angelo and certain other entities to pay older loans that St. Angelo was unable to repay and to cover his overdrafts. The new loans then appeared to be current, while the old loans and overdrafts appeared to have been paid. In reality, the new loans were designed to avert the downgrading or impairment of loans to St. Angelo and several entities and to avoid reporting them as nonperforming or losses to the bank.

St. Angelo also conspired with the bank president and others in a fraudulent tax credit investment scheme whereby the bank purportedly purchased historic tax credits from St. Angelo and his entities to assist St. Angelo in making his loan payments and curing overdrafts. By late April 2017, the balances on loans issued to St. Angelo and his entities totaled approximately \$46.7 million, and First NBC Bank had also paid St. Angelo approximately \$9.6 million for the fraudulent tax credit investments.

From 2006 through April 2017, Treme was a customer of First NBC Bank. Treme was a business owner and a real estate developer who owned numerous business entities, including several in partnership with Ryan. Treme, Ryan, William Burnell (First NBC Bank's Chief Credit Officer), and others made false statements and material omissions about Treme, his entities, and their loans in order to hide Treme's true financial condition. These false statements and material omissions hid the truth about the purpose of the loans, the borrowers' assets and liabilities, the borrowers' cash flow, and the expected source of repayment. They further disguised Treme's and his entities' true financial condition by issuing new loans to make payments on existing loans and to cover his overdrafts. The new loans were designed to hide Treme's inability to pay his existing loans without additional loan proceeds from the bank. Over the course of several years, Treme's debt to First NBC Bank increased to \$6.3 million.

From 2008 through April 2017, Vira was a customer of First NBC Bank. Between 2010 and April 2017, Vira provided personal loans to co-conspirators, some derived from First NBC Bank loan proceeds. Vira was instructed to conceal these loans from bank employees who were his co-conspirators, thus Vira did not include the loans in his personal financial statements. Vira's co-conspirators also ensured Vira and his family members received preferential treatment through lower interest rates on loans and higher interest rates on the savings and checking accounts. Vira also provided false information on his personal financial statements by inflating his assets.

Previously, on September 6, 2023, former Bank President Ashton Ryan was sentenced to 14 years and 2 months in prison. And on September 2, 2023, Burnell was sentenced to 48 months in prison.

Source: FDIC Legal Division.

***Responsible Agencies: FDIC OIG, FBI, and Federal Reserve Board OIG.
Prosecuted by the USAO, Eastern District of Louisiana.***

Attorney and Former Bank Director Sentenced to 30 Months in Prison for Bank Fraud

Attorney and former Park Avenue Bank Director Mendel Zilberberg was sentenced in the Southern District of New York to 30 months imprisonment followed by 3 years of supervised release. Zilberberg was also ordered to pay restitution of \$1,066,853, a \$100 special assessment fee for each count, and forfeiture in the amount of \$506,000 for his role in a commercial loan fraud scheme that resulted in a loss to the FDIC and Valley National Bank, which acquired The Park Avenue Bank after its failure in March 2010. On July 11, 2023, a Federal jury found Zilberberg guilty of five counts — conspiracy to commit bank fraud, bank fraud, conspiracy to make false statements to a bank, making false statements to a bank, and misapplication of bank funds — in connection with a scheme to obtain a fraudulent loan from Park Avenue Bank.

In or about 2009, Zilberberg conspired with Aron Fried, a New Jersey businessman, and others to obtain a fraudulent loan from Park Avenue Bank. Knowing that the conspirators would not be able to obtain the loan directly, the conspirators recruited a straw borrower to make the loan application. The straw borrower applied for a \$1.4 million loan from the Bank on the basis of numerous lies directed by Zilberberg and his co-conspirators.

Zilberberg used his privileged position at the bank to ensure that the loan was processed promptly. Based on the false representations made to the Bank and Zilberberg's involvement in the loan approval process, the Bank issued a \$1.4 million loan to the straw borrower, which was quickly disbursed to the defendants through multiple bank accounts and transfers. In total, Zilberberg received more than approximately \$500,000 of the loan proceeds. The remainder of the loan was split between Fried and another conspirator. The straw borrower received nothing from the loan. The loan ultimately defaulted, resulting in a loss of over \$1 million.

On November 15, 2022, Fried pled guilty to conspiracy to commit bank fraud. On April 10, 2023, Judge Daniels sentenced Fried to one year and one day in prison. (In or about 2009, Aron Fried and a co-conspirator not named in the Indictment (“CC-1”) sought to obtain a fraudulent loan from the Bank in Manhattan in order to finance an investment in a home health care business.)

Source: FDIC Legal Division, New York Region.

Responsible Agencies: FDIC OIG and FBI.

Prosecuted by the USAO, Southern District of New York.

Twice Convicted Bank Fraud Felon Sentenced to 110 Months

Wavy Curtis Shain pled guilty to one count of bank fraud and one count of money laundering in the United States District Court, Western District of Kentucky. The victim institutions were PNC Bank and Small Business Bank. Shain was sentenced to 110 months of incarceration, followed by 5 years of supervised release. In addition, he was ordered to pay \$4,455,755 in restitution.

From 2019 to 2020, Shain, an individual previously convicted of mail fraud and bank fraud, carried out a scheme to defraud multiple banks and non-bank lenders through an identity theft and fraudulent documents scheme. While incarcerated on a prior bank fraud conviction, Shain met and befriended numerous other inmates while assisting in appealing their criminal convictions. After his release from prison, Shain used the victims’ identities to obtain fraudulent loans. He devised a scheme to defraud the banks by obtaining second mortgages and refinance loans on homes owned by his friends and other associates without their consent or knowledge. Shain created fraudulent identification and financial documents to induce lenders into making loans. To hide the loans from the victims, Shain intercepted correspondence from lenders by diverting late notifications to post office boxes he created in furtherance of the fraud. In some instances, Shain posed as a lawyer to obtain the information needed to carry out the fraud. He laundered the proceeds of his fraud through real estate purchases, debt repayments, and the purchase of luxury cars. Shain also obtained seven CARES Act loans by creating fraudulent businesses he claimed were owned by his various victims.

Source: USAO, Western District of Kentucky.

Responsible Agencies: FDIC OIG and IRS-CI.

Prosecuted by the USAO, Western District of Kentucky.

Subject of Business Email Compromise Scam Pleads Guilty to Wire Fraud and Aggravated Identity Theft

Abdulafeez Oluwatoyin Adebiyi pled guilty to one count of wire fraud and one count of aggravated identity theft in the Eastern District of Virginia. He was previously arrested in the United Kingdom in September 2022 pursuant to an Interpol Wanted Notice related to the Indictment in this matter from the Eastern District of Virginia.

On October 23, 2020, Cognosante Holdings became aware that it had received an email believed to have been sent from a subcontractor Pharos Group, but it was actually sent from a fraudulent/fictitious domain disguised to appear as if it was from Pharos Group. Adebiyi initially gained access to a Pharos Group email account, found email exchanges between Pharos and Cognosante and discovered there were invoices due to Pharos Group totaling over one million dollars. Adebiyi then forwarded several emails and attachments (invoices, ACH, banking information) to the Cognosante email account to perpetrate the fraud.

Adebiyi and/or other conspirators then created a fraudulent/fictitious domain with a similar name (pharosgroupinc.com). Adebiyi used the pharosgroupinc.com domain to submit fraudulent invoices and change the bank account information from Pharos' Wells Fargo bank to the co-conspirators' Wells Fargo account. Cognosante paid the invoices and wired \$1,041,087.43 from its Capital One Bank to one of the co-conspirator's, Monica R. Lopez's, Wells Fargo Bank account. Lopez's Wells Fargo Bank account was depleted using 12 cashier checks, 2 wires, a cash withdrawal, and fund transfers to multiple companies and individuals. The United States Secret Service seized approximately \$350,000 from various bank accounts that received the money from Lopez.

Source: FBI.

Responsible Agencies: FDIC OIG and FBI.

Prosecuted by the USAO, Eastern District of Virginia.

Three Co-Conspirators Plead Guilty in Bank Fraud Scheme

Gregory Thurman pled guilty to one count of conspiracy to commit bank fraud. Travis Wright pled guilty to one count of conspiracy to commit wire fraud in the Southern District of Texas, and Munson Hunter III, AKA Paul Hunter, pled guilty to wire fraud in the Southern District of Texas.

Beginning on or before 2014, Thurman, Wright, Hunter, an unidentified co-conspirator, and Janem Gibbs, a former Capital One Multi-Branch Manager, conspired to steal funds from a Capital One customer's account. On June 8, 2016, Gibbs instructed Capital One to wire \$200,000 from an unknowing Capital One customer's account to a Wells Fargo account controlled by Hunter. A co-conspirator then laundered the funds through multiple bank accounts and disbursed the funds. Thurman received approximately \$73,000 of the stolen funds and Wright received \$37,500.

Beginning on or before February 2013 through February 24, 2023, Hunter opened bank accounts using fictitious names and other individuals' social security cards 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.

Previously, in September 2023, Gibbs pled guilty to one count of conspiracy to commit bank fraud in the Southern District of Texas.

Source: Capital One.

Responsible Agencies: FDIC OIG and FBI.

Prosecuted by the USAO, Southern District of Texas.

Federal Attorney Pleads Guilty to Conspiring to Sexually Exploit Numerous Children

A former FDIC attorney pled guilty to conspiring to sexually exploit numerous children. Between January 2018 and October 2021, Mark Black 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 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 pleaded guilty to one count of conspiracy to produce child pornography and one count of coercion and enticement. He faces a mandatory minimum of 15 years in prison and a maximum penalty of life in prison.

Source: Project Safe Childhood, a nationwide initiative to combat the epidemic of child sexual exploitation and abuse launched in May 2006 by the DOJ.

Responsible Agencies: FDIC OIG and FBI.

Prosecuted by the USAO, Eastern District of Virginia, and Trial Attorneys from the DOJ.

Two Individuals Plead Guilty for Operating an Unlicensed Money Transmitting Business

Yufeng Gao pled guilty to operating an unlicensed money transmitting business and moving approximately \$134 million through various financial institutions in the District of New Jersey. Francisco Rodriguez pled guilty to operating an unlicensed money transmitting business in the District of New Jersey. The two were part of a conspiracy orchestrated by Da Ying Sze, who pled guilty earlier to one count of conspiring to commit money laundering, one count of operating and aiding and abetting the operation of an unlicensed money transmitting business, and one count of corruptly giving anything of value to an employee of a financial institution in connection with financial transactions.

From 2016 through 2021, Sze laundered more than \$653.3 million in cash, consisting of narcotics and other illicit proceeds, utilizing a variety of financial institutions and methods. Sze routinely accepted illicit proceeds in cash and deposited the cash into financial institutions in New York, New Jersey, Pennsylvania, and elsewhere, utilizing bank accounts in the names of shell companies and conspirators. Sze then further obfuscated the source of the illegal cash by purchasing official bank checks, writing personal and business checks, and making international and domestic wires to transfer the illegal cash to thousands of individuals and entities in the United States, China, Hong Kong, and elsewhere. For his services, Sze received a fee of approximately 1 to 2 percent of the cash laundered. Gao was a co-conspirator in the fraud by operating an unlicensed money transmitting business and laundering approximately \$134 million through various financial institutions. Sze paid Gao for Gao's role in the scheme. From in and around 2019 to around May 2021, Rodriguez conspired with Sze while owning and operating a money transmitting business.

Source: USAO, District of New Jersey, and IRS-CI.

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

Prosecuted by USAOs for the Districts of New Jersey, Puerto Rico, and Washington and the DOJ Money Laundering and Asset Recovery Section (MLARS).

Sixth Employee Admits Role in Cash Flow Partners' Bank Fraud Conspiracy

Dayel Mordan, an employee of Cash Flow Partners, LLC, pled guilty to one count of conspiracy to commit bank fraud in the District of New Jersey.

Between March 2016 and September 2019, Cash Flow Partners, LLC, a business consulting firm with offices in New York and New Jersey, released internet advertisements and held seminars offering to assist customers in obtaining bank loans, including loans from financial institutions insured by the FDIC like Santander Bank and Wells Fargo Bank. Mordan operated the accounting department for Cash Flow Partners. When customers submitted documentation supporting their bank loan applications to Cash Flow Partners, Mordan and others created false documentation to make customers' loan applications appear more financially viable than they actually were. Victim banks sustained losses of over \$4 million.

Five of Mordan's co-conspirators previously pled guilty to charges relating to their role in the Cash Flow bank fraud conspiracy and are awaiting sentencing.

Source: Santander Bank.

Responsible Agencies: FDIC OIG and FBI.

Prosecuted by the USAO, District of New Jersey.

Former Chief Financial Officer of Eastern International Bank Agrees to Plead Guilty to Bank Fraud for Embezzling over \$700,000

Sammy Sims, the former Chief Financial Officer at Eastern International Bank (EIB) pled guilty to bank fraud for embezzling over \$700,000 in bank funds. Sims also improperly accessed EIB's accounts and ledgers, as well as the confidential personal information of EIB employees.

Sims stole hundreds of thousands of dollars in EIB funds to make personal investments in music concerts, pay off his large debts, make payments towards his personal income taxes and those of his wife, and pay for trips to Las Vegas, among other misappropriations. He also created false entries in EIB's general ledger to disguise these transactions as legitimate EIB expenses.

Sims falsely told several EIB employees that they had to switch their EIB-funded life insurance policies due to their age. He then transferred over \$300,000 in EIB funds to pay for the premiums for new life insurance policies for those EIB employees. The policies were obtained through Sims' wife who was a life insurance broker. Sims' wife then received a commission for each of the life insurance policies inappropriately funded by Sims through EIB.

Source: FDIC Division of Risk Management Supervision.

Responsible Agencies: FDIC OIG and FBI.

Prosecuted by the Major Frauds Section, USAO, Central District of California.

Six Houston Residents Sentenced for Roles in COVID-19 Fraud Scheme

The following persons were sentenced in the Southern District of Texas for their roles in a fraud scheme to unlawfully obtain more than \$20 million in forgivable Paycheck Protection Program (PPP) loans that the Small Business Administration (SBA) guaranteed under the Coronavirus Aid, Relief, and Economic Security Act. (CARES Act):

Hamza Abbas, 44 months' prison, 3 years' supervised release, \$2,380,160 restitution.

Syed Ali, 24 months' prison, 3 years' supervised release, \$937,499 restitution.

Muhammad Anis, 21 months' prison, 3 years' supervised release, \$483,333 restitution.

Ammas Uddin, 18 months' prison, 3 years' supervised release, \$498,415 restitution.

Arham Uddin, 18 months' prison, 3 years' supervised release, \$491,664 restitution.

Jesus Acosta Perez, 12 months' prison, 3 years' supervised release, \$391,300 restitution.

The defendants in this case conspired to submit more than 80 fraudulent PPP loan applications by falsifying the number of employees and the average monthly payroll expenses of the applicant businesses. In support of these fraudulent loan applications, they submitted fraudulent bank records and federal tax forms. PPP loan applications were submitted on behalf of companies the defendants controlled as well as entities owned by third parties. The defendants laundered a portion of the fraudulent proceeds by writing checks from companies that received PPP loans to fake employees. Those that received checks included some of the defendants and their relatives. The fake paychecks were then cashed at Fascare International Inc., doing business as Almeda Discount Store, a cash checking company owned by one of the defendants. Over 1,100 fake paychecks totaling more than \$5 million in fraudulent PPP loan proceeds were cashed at this business. In total, the co-conspirators sought over \$50 million through fraudulent PPP loans.

Source: Initiated by the FDIC OIG based on information from a related investigation.

Responsible Agencies: FDIC OIG, SBA OIG, Homeland Security Investigations, Federal Housing Finance Agency OIG, and Treasury Inspector General for Tax Administration.

Prosecuted by the USAO, Southern District of Texas and the DOJ Criminal Division's Fraud Section.

Former Bank Officer Pleads Guilty to Bank Fraud

Kristy Barger pled guilty to bank fraud in the Western District of Arkansas based on her scheme against her former employer, Relyance Bank, Pine Bluff, Arkansas.

In 2014, Barger began her employment with Relyance Bank as a Senior Trust Officer and was later promoted to Vice President in 2017. In her duties as Senior Trust Officer and Vice President, Barger was responsible for all aspects of the bank's trust department. From approximately 2014 through 2020, she embezzled \$890,764.26 from trust accounts managed within the bank's trust department. The trust accounts were primarily owned by elderly and disabled customers who were no longer able to manage their own finances. Barger embezzled the funds by using fraudulent cashier's checks and trust department checks to unlawfully issue \$890,764.26 in payments to her various credit card accounts for her personal expenses.

Source: USAO, Western District of Arkansas.

Responsible Agencies: FDIC OIG and U.S. Secret Service.

Prosecuted by the USAO, Western District of Arkansas – Pine Bluff.

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 67 judicial districts in 37 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	Wisconsin
Iowa	New Jersey	
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, COVID-19 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	New York Identity Theft Task Force; 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 for: Southern District of Florida, Middle District of Florida, Northern District of Florida; SAR Review Groups for: 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; 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; Northern District of Illinois Bankruptcy Fraud Working Group; 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; U.S. Secret Service Louisville Electronic Crimes 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, Eastern District of Michigan SAR Review Team, Western District of Michigan SAR Review Team, Northern District of Ohio SAR Review Team, Southern District of Indiana SAR Review Team.
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.
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.
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; and International Organized Crime Intelligence and Operations Center (IOC-2).



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 an FDIC Global message reminding FDIC employees of their Whistleblower Protections and employee obligations to report fraud, waste, abuse, misconduct or mismanagement.
- 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 several of the FDIC's "One FDIC" forums 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. Produced our first podcast covering our Material Loss Review work and enhanced our approach to videos on issued reports.

- Presented at the Federal Financial Institutions Examination Council's Fraud Investigation Techniques for Examiners course. This course is geared to state and Federal bank examiners and intended to enhance skills in interviewing, documenting, tracing, and managing fraud-related cases. Two OI Special Agents provided an overview of the OIG, discussed the criminal investigations conducted by OI, presented an overview of cyber investigations and digital forensics, and shared success stories of criminal prosecutions initiated through examiner referrals.
- 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.
- Completed a peer review of the Inspection and Evaluation function of the U.S. Postal Service (USPS) OIG, and communicated that its policies and procedures generally were consistent with the Blue Book standards addressed in the external peer review. Made four recommendations in a Letter of Comment, with which USPS OIG concurred.
- Assisted Peace Corps OIG with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) peer review of the Nuclear Regulatory Commission (NRC) OIG's digital forensics program and assisted with the review of the CIGIE quality standards for investigations. In February 2024, members of our ECU conducted the onsite review of NRC OIG using the CIGIE C-2 checklist, conducted employee interviews, and reviewed evidence.
- 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.
- Held briefings in November with several Congressional Committees on past and planned OIG work related to the workplace culture at the FDIC, including the OIG's 2020 report on *Preventing and Addressing Sexual Harassment*, and answered Committee questions related to future planned work in this area. Committees briefed included Senate Banking Majority and Minority staff; House Financial Services Majority and Minority staff; and House Appropriations Majority staff. In March, we briefed Senate Banking Committee Majority and Minority and House Financial Services Committee Majority and Minority staff on the Top Management and Performance Challenges facing the FDIC and related ongoing and planned work.

- Maintained the OIG Hotline to field complaints and allegations of fraud, waste, abuse, and mismanagement affecting FDIC programs and operations from the public and other stakeholders. The OIG's Whistleblower Protection Coordinator also helped educate FDIC employees who had made or were contemplating making a protected disclosure as to their rights and remedies against retaliation for such protected disclosures. Our web-based hotline portal at <https://www.fdicigo.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 235 Hotline inquiries, 7 of which led to our opening investigations.
- Participated at two CIGIE Career Fairs to familiarize participants with the mission of the FDIC OIG, and share potential career opportunities with students, recent graduates, and professionals from across the D.C. metropolitan area.
- Presented at the CIGIE Federal Audit Executive Council (FAEC) Annual Conference on the Toolkit for Identifying and Reporting Monetary Impact. The presentation included the different methodologies the OIG community uses to approach monetary impact and best practices for OIGs to leverage in determining monetary impact moving forward.
- 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.
- Presented remarks by the Planning and Operations Manager of our Office of Audits, Evaluations, and Cyber (AEC) on "Assessing and Responding to Errors in Published Reports: A Framework for OIG Quality Assurance Reviewers" to the CIGIE/FAEC Quality Management Committee, with about 80 individuals across the OIG community in attendance.
- Presented at the FDIC Data Summit in the FDIC's Bair Auditorium on "Integrating Data Into OIG Bank Fraud Investigations." Two of OI's Special Agents in Charge provided an overview of the OI mission, structure, and authorities; summaries of select bank and cyber fraud cases; and an exchange with summit participants regarding key data-related considerations in OIG investigations. The OIG's Chief Data Officer also offered technical expertise and answered questions.
- Spoke at American University to a group of students interested in careers as Federal law enforcement officers or as Federal prosecutors. The FDIC Assistant IG for Investigations discussed white-collar crime investigations, the investigative process, and how special agents and prosecutors work together throughout the investigation and prosecution phases of a case.

- Conducted outreach and information sharing by the FDIC OIG New York Region Special Agent in Charge and a Special Agent from our San Francisco Region with colleagues at the Association of Certified Anti-Money Laundering Specialists' conference in Las Vegas.
- Represented the FDIC OIG during the American Bankers Association Financial Crimes Enforcement Conference held at the Gaylord National Resort and Convention Center in National Harbor. Conducted outreach activities with thousands of banking, legal, data analytics, compliance, and financial industry professionals. As part of the conference, one of our Senior Special Agents participated on a panel discussion with colleagues from the Department of Labor and Department of Commerce OIGs entitled, "Introducing...Government Entities Involved in Financial Crimes You May Not Know!" This session provided attendees with an understanding of the OIGs' role in partnering with financial institutions and other agencies.
- Delivered the Keynote at the Association of Certified Anti-Money Laundering Specialists San Diego Baja California's 6th Annual Financial Crimes Forum on December 5. Approximately 150-200 participants attended, including Anti-Money Laundering professionals, attorneys, and other members of law enforcement. The Special Agent in Charge of our San Francisco Region's keynote address focused on the importance of relationships between law enforcement and financial institutions. He also gave an overview of the FDIC OIG, highlighted several recent case successes, and discussed the importance of Bank Secrecy Act (Suspicious Activity Report) reporting.
- 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 (NLEAD) as "a centralized repository of official records documenting instances of law enforcement officer misconduct as well as commendations and awards." We ensured the OIG's timely first submission to the NLEAD in full compliance with the Executive Order.
- Supported the broader IG community by attending monthly CIGIE meetings and other meetings, such as those of the CIGIE Legislation Committee; the Diversity, Equity, Inclusion, and Accessibility (DEIA) 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 (CIGFO), as established by the Dodd-Frank Wall Street Reform and Consumer Protection Act, and coordinated with the IGs on that Council. This Council facilitates sharing of information among CIGFO 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 budget and proposed budget for FY 2025.
- 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 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 newly 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 \$52.6 million for FY 2025, approximately 5 percent above the OIG's budget request for FY 2024 of \$49.8 million. The requested budget would maintain flat staffing levels, sustain prior investments in information technology and data analytics, and support oversight focused on cybersecurity, statutorily-mandated reviews of failed banks, the resolution and receiverships of the largest bank failures in U.S. history, and congressionally requested reviews of workplace culture and harassment allegations at the FDIC. The budget would further support investigations conducted by Special Agents.

- Established a Regional Office presence for the OIG's Office of Investigations in Miami, Florida, with responsibility for a growing number of cases in Florida, Puerto Rico, and the Virgin Islands. Staffed the site with a Special Agent in Charge and three Special Agents.
- Developed the OIG's Shutdown Plan and corresponding FAQs for any potential lapses in appropriations given potential government shutdowns. The OIG receives an annual appropriation in which Congress sets an amount that the FDIC is required to provide from the Deposit Insurance Fund for OIG operations. Absent the passage of a continuing resolution or enactment of an appropriations bill, our Office would be required to shut down.
- Adhered to an updated telework policy for the OIG. A main element of this policy was that Managers should schedule in-office collaboration for their staffs at least one day per pay period, effective on July 2, 2023. Kept apprised of FDIC management's plans and guidance for Return to Office after July 15, 2024 and considered the implications of those plans on the operations and policy of the OIG.
- 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 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. Focused on establishing an OIG data governance framework, implementing a data analytics platform, establishing data integration technologies, and migrating our first data sets into the FDIC data lake to permit access to advanced analytical tools.
- 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.
- 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, operational, 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. For example, updated and/or posted policies regarding such topics as the OIG’s Delegations of Authority, Travel and Relocation, Training and Professional Development, Staffing and Hiring Process, and Records Retention.
- 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 Special Agent in Charge of our San Francisco Region, Director of Management Services, HR Benefits Specialist, Sr. Audit Specialist, and five Special Agents.

- Oversaw contracts to qualified firms to provide audit, evaluation, IT, and other services to the OIG to provide support and enhance the quality of our work and the breadth of our expertise as we conduct audits, evaluations, and investigations, and to complement other OIG functions, and closely monitored contractor performance.
- Continued to integrate and leverage the use of MS Teams throughout our Office to promote virtual collaboration and communication.

Exercising leadership skills and promoting teamwork.

- Hosted an OIG Town Hall event in the Bair Auditorium in February. This forum provided an opportunity to welcome IG Fain to the OIG team and for OIG staff to see and hear from Office of Management representatives, the Workforce Council, and the Assistant IGs for Audits, Evaluations, and Cyber and for Investigations..
- Examined the OIG's results from the 2023 Federal Employee Viewpoint Survey (FEVS). This confidential survey administered by OPM measures key factors in the Federal workplace and is an important tool to gather feedback on the FDIC OIG's leaders, organization, and work environment. Considered staff opinions about what the FDIC OIG is doing well and where improvements can be made.
- Recognized a Senior Special Agent in our Miami Regional Office of Investigations as the recipient of a prestigious Attorney General's Award for Fraud Prevention. This award recognizes his exceptional dedication and effort with law enforcement partners to prevent, investigate, and prosecute fraud, white-collar crimes, and official corruption. His contributions to the investigation of the scheme orchestrated to defraud USAA Federal Savings Bank and CARES Act Programs are noteworthy.
- Hosted OI's "New Agent Training" at Virginia Square for OI Special Agents who are new to the Office. Presentations included case studies; legal topics; Audits, Evaluations, and Cyber overview; FDIC overview; and other enforcement-related topics. Incorporated a segment on Body-Worn Cameras during the current reporting period.
- 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.

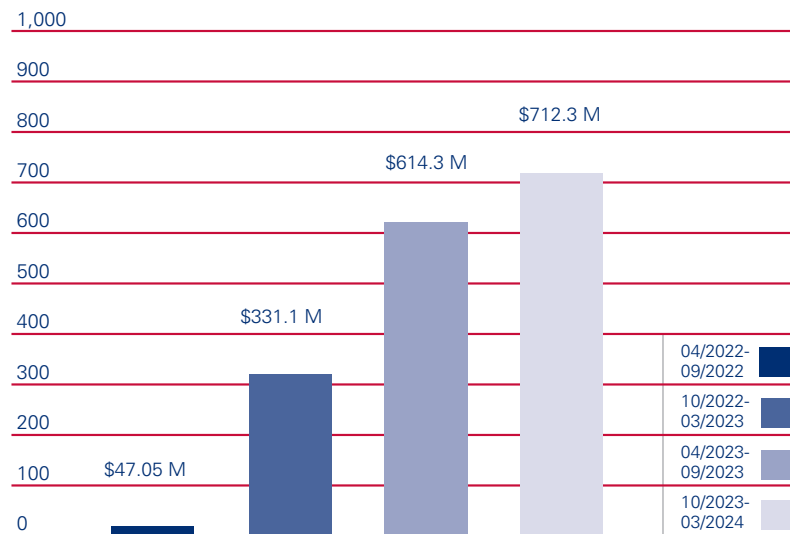
- Held OIG senior leadership coordination meetings to affirm the OIG’s unified commitment to the FDIC OIG mission and to strengthen working relationships and collaboration among all FDIC OIG offices.
- Supported efforts of the Workforce Council. The mission of this Council is to foster and support a 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.
- Held an FDIC OIG Office of Management (OM) All-Hands Conference, the theme of which was “Connect.” The event included updates from each component within OM, a Work Life presentation, Corporate University Presentation, and a session on Connection in the Workplace.
- Developed “OM Connect” information sessions hosted by the supervisors and senior staff of OM. The intent is to provide latest information regarding processes, policies, human resources, management services, information technology changes, and engagement and learning opportunities. The first session focused on performance management and interactions with employees. The second was a presentation by members of the OIG’s IT Group and Chief Data Analytics Officer.
- 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.
- Held a 2-day AEC Forum for AEC staff, the theme of which was “Acknowledging, Empowering, Connecting.” The agenda included chats with OIG and FDIC leadership, a panel discussion with Audit Executives across the IG community, and exercises and presentations on self-awareness and connecting with your peers both in-person and in a hybrid culture.
- Organized several social activities, including component-specific Coffee Chats, to promote community, teamwork, and collegiality among OIG staff.
- Held training on Arbing Institute principles for OIG staff to support the use of tools and practices that move individuals, teams, and organizations from the default self-focus of an inward mindset to the results focus of an outward mindset. Continued to introduce the concepts to additional employees through scheduled courses.

- 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 Assistant IG 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 is to assess and help ensure consistency in how OIGs report and track monetary impacts.
- Shared information from our Engagement and Learning Officer throughout the OIG to promote employee engagement, career development, and a positive workplace culture. The Engagement and Learning Officer offered training on the Neuroscience of Group Dynamics; announced training and professional development opportunities internal and external to the FDIC; and offered office hours and other opportunities to consult on culture, leadership, and teamwork insights and best practices.
- Fostered a sense of teamwork and mutual respect through various activities led by the the OIG's DEIA Working Group. Hosted a series of events to highlight diversity, including to recognize Veterans Day, National Black History Month, National Women's History Month, National Hispanic Heritage Month, and National Disability Awareness Month.
- Continued involvement and coordination with CIGIE's DEIA Committee. Supported issuance of *The Ally* Newsletter to share information from the Work Group, which works to affirm, advance, and augment CIGIE's commitment to promote a diverse, equitable, and inclusive workforce and workplace environment throughout the IG Community. Participated at the December monthly CIGIE DEIA Committee meeting, where our OIG Engagement and Learning Officer shared research supporting our DEIA efforts.

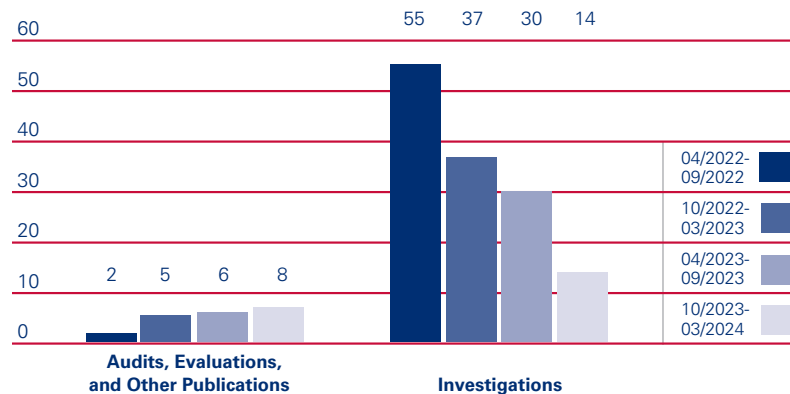
Cumulative Results (2-year period)

Recommendations	
April 2022 – September 2022	1
October 2022 – March 2023	56
April 2023 – September 2023	71
October 2023 – March 2024	31

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



Products Issued and Investigations Closed





Reporting Requirements

Index of Reporting Requirements

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

Reporting Requirements	Page
Section 4(a)(2): Review of legislation and regulations.	45
Section 5(a)(1): A description of significant problems, abuses, and deficiencies relating to the administration of programs and operations of the establishment and associated reports and recommendations for corrective action made by the Office.	4-11
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.)	47-59
Section 5(a)(3): A summary of significant investigations closed during the reporting period.	16-29
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.	60
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.	61
Section 5(a)(7): The information described under section 804(b) of the Federal Financial Management Improvement Act of 1996.	61
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.	64-66
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.	64-66

Reporting Requirements (continued)	Page
Section 5(a)(10): A list of any peer reviews conducted by the Inspector General of another Office of Inspector General during the reporting period, including a list of any outstanding recommendations made from any previous peer review (including any peer review conducted before the reporting period) that remain outstanding or have not been fully implemented.	64-66
Section 5(a)(11): Statistical tables showing, for the reporting period: <ul style="list-style-type: none"> • 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. 	61
Section 5(a)(12): A description of metrics used for Section 5(a)(11) information.	61
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.	61
Section 5(a)(14): <ul style="list-style-type: none"> (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. 	62
Section 5(a)(15): Information related to interference by the establishment, including— <ul style="list-style-type: none"> (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. 	62
Section 5(a)(16): Detailed descriptions of the particular circumstances of each - <ul style="list-style-type: none"> (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. 	62



Appendix 1

Information in Response to Reporting Requirements

Review of Legislation and Regulations

The FDIC OIG's review of legislation and regulations during the past 6-month period involved continuing efforts to monitor enacted law or proposed legislative matters. 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.

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.

The FDIC OIG supports the efforts of the IG community as it works with Congress on these priorities and government reform issues. Of note, during the reporting period, the Committee's efforts included engagement on a number of proposals and initiatives, including Permanent Data and Analytics Capability for the IG Community, Establishing Authority for IGs to Provide Continuous Oversight During a Lapse in Appropriations, Statutory Exclusion for Felony Fraud Convicts to Protect Federal Funds, and the IG Pay Freeze.

Regarding its Permanent Data and Analytics Capability for the IG Community proposal, the Legislation Committee provided Congressional staff with a detailed briefing and a follow-up demonstration describing how the Pandemic Analytics Center of Excellence currently operates and how a permanent data and analytics capability could support fraud prevention, detection, and program integrity if enacted. The Committee also engaged with Congressional Committees on the need to reform or repeal certain IG mandates that may no longer add value to Congress or the public. By addressing these requirements, IG resources could be freed up to conduct additional risk-based oversight work. Of interest as well, the Committee monitored and reported out on proposed legislation: H.R. 7532, [The Federal AI Governance and Transparency Act](#).

Table I: Unimplemented Recommendations from Previous Semiannual Periods

Notes:

1. A current listing of each of the unimplemented recommendations is available at <https://www.fdicigo.gov/unimplemented-recommendations>. The listing is updated monthly.
 2. Recommendations open for more than one year are marked **.
- These total 20 recommendations.

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-20-001 <u>Contract Oversight Management</u> October 28, 2019	<p>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.</p> <p>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 (OM) to oversee assigned contracts; OM training and certifications; and security risks posed by contractors and their personnel.</p> <p>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 OMs lacked workload capacity to oversee contracts, and certain OMs were not properly trained or certified.</p> <p>The report contained 12 recommendations to strengthen contract oversight.</p>	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	
REV-22-001 Whistleblower Rights and Protections for FDIC Contractors January 4, 2022	<p>Whistleblowers play an important role in safeguarding the Federal Government against waste, fraud, and abuse. In 2016, Congress enacted legislation to permanently expand whistleblower protections to the employees of government contractors and subcontractors.</p> <p>We conducted a review to determine whether the FDIC aligned its procedures and processes with laws, regulations, and policies designed to ensure notice to contractors and subcontractors about their whistleblower rights and protections.</p> <p>We found that the FDIC procedures and processes were not aligned with laws, regulations, and policies designed to ensure notice to contractor and subcontractor employees about their whistleblower rights and protections. Further, the FDIC's Legal Division, under its separately delegated contracting authority, had not adopted any whistleblower provisions or included any whistleblower clauses in its contracts.</p> <p>In addition, we determined that the FDIC had not established any requirements for FDIC officials to determine whether contractors had carried out their obligations under the FDIC's Whistleblower Rights Notification Clause. The FDIC also did not obtain Confidentiality Agreements from all of its contractors and contract personnel, as required. We also found that Legal Division guidance may be unclear and confusing to contractor or subcontractor whistleblowers as to whom they should report criminal behavior or allegations of fraud, waste, abuse, or mismanagement.</p> <p>The report contained 10 recommendations intended to ensure that contractors and subcontractors are informed of their whistleblower rights and protections.</p>	10	1 **	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
<p>AUD-22-003</p> <p><u>Sharing of Threat Information to Guide the Supervision of Financial Institutions</u></p> <p>January 18, 2022</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	25	1 **	NA
<p>EVAL-22-003</p> <p><u>The FDIC's Implementation of Supply Chain Risk Management</u></p> <p>March 1, 2022</p>	<p>In 2021, the FDIC awarded 483 contracts totaling over \$2 billion for the acquisition of products and services. These products and services were provided by many types of vendors, contractors, and subcontractors. The supply chain for each vendor, contractor, or subcontractor may present unique risks to the FDIC. Therefore, the FDIC must implement a robust Supply Chain Risk Management (SCRM) Program to identify and mitigate supply chain risks that threaten its ability to fulfill its mission.</p> <p>We conducted an evaluation to determine whether the FDIC developed and implemented its SCRM Program in alignment with the Agency's objectives and best practices.</p> <p>We found that the FDIC had not implemented several objectives established in the SCRM Implementation Project Charter, including identifying and documenting known risks to its supply chain and establishing metrics and indicators for their continuous monitoring and evaluation. Further, the FDIC was not conducting supply chain risk assessments during its procurement process.</p> <p>In addition, FDIC had not integrated Agency-wide supply chain risks into its Enterprise Risk Management processes. We also determined that Contracting Officers did not maintain contract documents in the Contract Electronic File system, as required.</p> <p>The report contained nine recommendations to improve the FDIC's SCRM Program and retention of contract documents.</p>	9	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-22-004 The FDIC's Information Security Program - 2022 September 27, 2022	<p>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.</p> <p>We conducted an audit to evaluate the effectiveness of the FDIC's information security program and practices.</p> <p>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.</p> <p>The report contained one recommendation for the FDIC to address the 31 flaw remediation Plans of Action and Milestones.</p>	1	1 **	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
REV-23-001 Security Controls Over the FDIC's Wireless Networks December 13, 2022	<p>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.</p> <p>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.</p> <p>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:</p> <ol style="list-style-type: none"> 1. Configuration of Wireless Networks 2. Wireless Signal Strength 3. Security Assessments and Authorizations 4. Vulnerability Scanning 5. Wireless Policies, Procedures, and Guidance <p>The report contained eight recommendations intended to strengthen the security controls over the FDIC's wireless networks.</p>	8	1 **	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
<p>AUD-23-001</p> <p><u>Implementation of the FDIC's Information Technology Risk Examination (InTReX) Program</u></p> <p>January 31, 2023</p>	<p>The FDIC conducts information technology (IT) examinations to evaluate bank management's ability to identify IT and cyber risks and maintain appropriate compensating controls.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>The report contained 19 recommendations to strengthen the InTReX program.</p>	19	4**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
<p>AUD-23-002</p> <p>The FDIC's Security Controls Over Microsoft Windows Active Directory</p> <p>March 15, 2023</p>	<p>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 (AD) to centrally manage user identification, authentication, and authorization. AD 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 AD infrastructure.</p> <p>We conducted an audit to assess the effectiveness of controls for securing and managing the Windows AD 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.</p> <p>Cotton determined that the FDIC had not fully established and implemented effective controls for securing and managing the Windows AD to protect the FDIC's network, systems, and data in 7 of the 12 areas we assessed.</p> <p>The report contained 15 recommendations to improve AD security controls.</p>	15	6**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
REV-23-002 FDIC's Oversight of a Telecommunications Contract March 31, 2023	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The report contained 14 recommendations to enhance contracting controls.</p>	14	4**	\$1,500,000

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-23-001 FDIC Examinations of Government- Guaranteed Loans May 5, 2023	<p>Federal agencies administer several Government-guaranteed loan programs to assist individuals and businesses with, among other things, buying homes, financing agricultural production, financing businesses, and purchasing equipment. FDIC-supervised banks participate in these programs, originating billions of dollars in Government-guaranteed loans. These programs promote lending to rural and underserved communities and to borrowers with collateral weaknesses or that lack adequate credit history. Without proper due diligence and supervision, Government-guaranteed loan programs can present substantial risks to banks. These risks include but are not limited to operational risk, compliance risk, reputational risk, fraud risk, and strategic risk.</p> <p>We conducted an evaluation to determine the effectiveness of the FDIC's examinations in identifying and addressing risks related to Government-guaranteed loans for banks that participate in Government-guaranteed loan programs.</p> <p>We found that FDIC bank examinations were not always effective in identifying and addressing risks related to Government-guaranteed loans. In addition, the FDIC's examination guidance did not provide clear instructions on the retention of examination workpapers.</p> <p>The report contained 19 recommendations to improve the FDIC's supervision of banks that participate in Government-guaranteed loan programs.</p>	19	7	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-23-003 The FDIC's Adoption of Cloud Computing Services July 25, 2023	<p>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.</p> <p>We conducted an audit to determine whether the FDIC had an effective strategy and governance processes to manage its cloud computing services.</p> <p>Overall, the FDIC had 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.</p> <p>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.</p> <p>The report contained nine recommendations to strengthen the strategy and governance over the FDIC's adoption of cloud computing services.</p>	9	6	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-23-002 Sharing of Threat and Vulnerability Information with Financial Institutions August 29, 2023	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	10	9	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
<p>AUD-23-004</p> <p><u>The Federal Deposit Insurance Corporation's Information Security Program – 2023</u></p> <p>September 13, 2023</p>	<p>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.</p> <p>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 [DHS] FISMA Reporting Metrics).</p> <p>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 DHS FISMA Reporting Metrics.</p> <p>The report contained two recommendations on user network access and required security and privacy training.</p>	2	2	NA
<p>EVAL-23-003</p> <p><u>FDIC Efforts to Increase Consumer Participation in the Insured Banking System</u></p> <p>September 13, 2023</p>	<p>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.</p> <p>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.</p> <p>The FDIC developed an Economic Inclusion Strategic Plan (EISP) 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 EISPs by incorporating additional strategic planning best practices into the strategic planning process.</p> <p>The report contained 14 recommendations intended to improve the development and implementation of future FDIC EISPs.</p>	14	14	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-23-004 The FDIC's Orderly Liquidation Authority September 28, 2023	<p>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.</p> <p>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.</p> <p>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.</p> <p>The report contained 17 recommendations to improve key elements for executing the FDIC's OLA responsibilities.</p>	17	17	NA

Table II: Audit and Evaluation Reports

<u>Audit/Evaluation Report</u>		<u>Questioned Costs</u>		<u>Funds Put to Better Use</u>
<u>Number and Date</u>	<u>Title*</u>	<u>Total</u>	<u>Unsupported</u>	
EVAL-24-01 October 17, 2023	<i>FDIC Strategies Related to Crypto-Asset Risks</i>			
EVAL-24-02 October 23, 2023	<i>Material Loss Review of Signature Bank of New York</i>			
EVAL-24-03 November 28, 2023	<i>Material Loss Review of First Republic Bank</i>			
AEC Memorandum 24-01 December 20, 2023	<i>The FDIC's Regional Service Provider Examination Program</i>			
EVAL-24-04 January 24, 2024	<i>The FDIC's Purchase and Deployment of the FDIC Acquisition Management System</i>			\$9.9 million
REV-24-01 March 20, 2024	<i>Review of the FDIC's Ransomware Readiness</i>			
AEC Memorandum 24-02 March 22, 2024	<i>Failed Bank Review-Citizens Bank, Sac City, Iowa</i>			
Totals for the Period		\$0	\$0	\$9.9 million

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

Note: Other products issued:

- Top Management and Performance Challenges. (February 22, 2024)

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	14
Number of Persons Referred to the Department of Justice for Criminal Prosecution	74
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	None
Number of Indictments and Criminal Informations	82

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 – Theft and Lack of Candor: During this reporting period, we conducted an investigation involving Theft of Government Property and Lack of Candor by a Senior FDIC Employee. We initiated this investigation based upon the receipt of an allegation that a senior FDIC employee stole items from the FDIC and lacked candor during a prior Background Investigation. The OIG investigation found that the employee did remove items from the FDIC that did not belong to the employee and that the employee lacked candor during the Background Investigation process. The OIG completed its investigation and provided its investigative findings to the FDIC.

Table VII: Instances of Whistleblower Retaliation

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

Table VIII: Instances of Agency Interference with OIG Independence

- A. During this reporting period, there were no attempts to interfere with OIG independence with respect to budget, resistance to oversight activities, or delayed access to information.
 - B. We made no reports to the head of the establishment regarding information requested by the IG that was unreasonably refused or not provided.
-

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

During this reporting period, there were no no evaluations or audits that were closed and not disclosed to the public. There were no investigations of senior government employees 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 the 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 October 1, 2023 through March 31, 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.

We issued one Failed Bank Review during the reporting period. The review covered the failure of Citizens Bank, Sac City, Iowa. (See earlier write-up in this semiannual report.) The estimated loss to the Deposit Insurance Fund was \$14.8 million or 23 percent of the bank's \$65 million in total assets. We determined that there were no unusual circumstances warranting 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. There are no outstanding recommendations. This peer review is posted on our Website: <https://www.fdicigoig.gov/sites/default/files/reports/2022-08/Letter%20Jay%20N%20Lerner%20Final%20Report%20FDIC%20OIG%20IE%20Peer%20Review%206%2028%2022.pdf>.

Investigative Peer Reviews

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

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

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

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



Congratulations to FDIC OIG CIGIE Award Winners

A number of OIG staff were recognized at the CIGIE Annual Awards Ceremony on November 7, 2023.

Award for Excellence—Investigation: Dave Ceron, Toshiro Muragaki, and Mike Rexrode (retired): *Investigation and Prosecution of the Cody Easterday/Easterday Ranches, Inc. \$244 million 'Ghost Cattle' Fraud Scheme.*

Award for Excellence—Audit: Terry Gibson, Cynthia Hogue, Stacey Luck, Rigene Mabry, Michael Reed: *CIGFO Crisis Readiness - Guidance in Preparing for and Managing Crises.*

Award for Excellence—Multiple Disciplines: Terry Gibson, Luke Itnyre, Melissa Mulhollen, Wendy Alvarado: *PRAC Agile Oversight Forum Team.*

Award for Excellence—Law and Legislation: Mike McCarthy and other colleagues from the IG community. *Legislation Committee Team for the 117th Congress.*



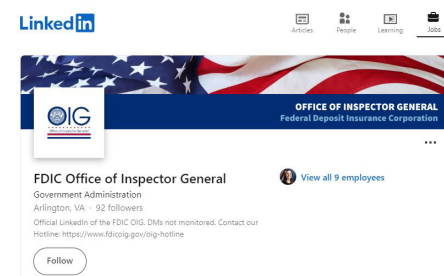
★ Learn more about the FDIC OIG.
Visit our website: www.fdicigoig.gov.



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



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



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




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



www.pandemicoversight.gov

★ Learn more about the IG community's commitment to diversity, equity, and inclusion. Visit: <https://www.ignet.gov/diversity-equity-and-inclusion-committee>.

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



Office of Inspector General
Federal Deposit Insurance Corporation



HOTLINE


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

For example:

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

Make a Difference and Contact Us:

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

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

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

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



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