FDIC Office of Inspector General

Semiannual Report to the Congress

April 1, 2023 - September 30, 2023

Office of Inspector General

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

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

The FDIC is an independent agency created by the Congress to maintain stability and confidence in the Nation's banking system. The FDIC insures deposits; examines and supervises financial institutions for safety and soundness and consumer protection; makes large, complex financial institutions resolvable; and manages receiverships. Approximately 5,637 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured $17.19 trillion in domestic deposits in 4,645 institutions, of which the FDIC supervised 2,983. The Deposit Insurance Fund balance totaled $117.0 billion as of June 30, 2023. Active receiverships as of September 30, 2023 totaled 103, with assets in liquidation of about $79.7 billion.

Semiannual Report to the Congress

April 1, 2023 - September 30, 2023

OIG

Office of Inspector General

Federal Deposit Insurance Corporation

Acting Inspector General's Statement

On behalf of the Office of Inspector General (OIG) at the Federal Deposit Insurance Corporation (FDIC), I am pleased to present our Semiannual Report for the period April 1, 2023 through September 30, 2023.

This semiannual report highlights six audit and evaluation reports that we issued during the period. In the Supervision area, we conducted an evaluation to determine the effectiveness of the FDIC's examinations in identifying and addressing risks related to government-guaranteed loans (GGL) for banks that participate in GGL programs. Another evaluation examined whether the FDIC has implemented effective processes to ensure that financial institutions receive actionable and relevant threat and vulnerability information.

With regard to Resolutions, we evaluated whether the FDIC maintained a consistent focus on implementing and establishing key elements to execute its Orderly Liquidation Authority under the Dodd-Frank Wall Street Reform and Consumer Protection Act. In the area of Consumer Protection, we conducted work to determine whether the FDIC's Economic Inclusion Strategic Plan increased the participation of unbanked and underbanked consumers in the insured banking system. Finally, with respect to Information Technology, one of our reports addressed whether the FDIC had an effective strategy and governance processes to manage its cloud computing services, and we also assessed the overall effectiveness of the FDIC's information security program and practices, required by the Federal Information Security Modernization Act of 2014. In all, we made 71 recommendations to address needed improvements in these areas of FDIC programs and operations, and the FDIC is working to address them.

Our investigations during the reporting period resulted in 100 indictments, 53 convictions, 91 arrests, and more than $614 million in fines, restitution ordered, assessments, and other monetary recoveries. In one of our cases, the Former Chief Executive Officer of First NBC Bank 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 restitution totaling over $214 million to the FDIC. In another case, a Federal jury in Chicago convicted two real estate developers of participating in a conspiracy that embezzled millions of dollars from the failed Washington Federal Bank for Savings in Chicago. In yet another case, executives of a health technology company were convicted in a billion-dollar corporate fraud scheme.

Our investigations involving pandemic-related fraud continued to account for many judicial actions and monetary benefits during this period. In fact, monetary recoveries attributable to such cases totaled more than $22.7 million. To date, we have opened 194 cases associated with fraud in the Coronavirus Aid, Relief, and Economic Security (CARES) Act and American Rescue Plan programs. Prosecutions in these cases result in harsh sentences; ordered restitution; and seizures of cash proceeds, real estate, and luxury items from offenders who stole funds from Government programs intended for those most in need during the pandemic. In one of our cases this period, for example, a bank insider—a former Relationship Manager at Bank of America—was sentenced to 15 months' imprisonment, followed by 3 years of supervised released, and ordered to pay a $100 assessment for his role in a CARES Act loan fraud scheme involving businesses owned by him, his wife, and his brother-in-law.

Throughout the reporting period, we have also maintained our OIG Hotline, receiving 442 inquiries during this time. This Hotline allows individuals to report suspected fraud, waste, abuse, or mismanagement within FDIC programs, activities, contractor operations, or FDIC-regulated, and FDIC-insured financial institutions. We opened 16 investigations emanating from the Hotline inquiries we received. While many of the inquiries we receive via the Hotline are not within the OIG's purview, we refer individuals to the appropriate entities for solutions to their concerns.

Our Office said farewell during the reporting period to the Planning and Operations Manager in our Office of Audits, Evaluations, and Cyber (AEC) and an Audit Specialist from that same group, both of whom provided invaluable contributions to the OIG. We also welcomed talented new members and enhanced our OIG leadership team over the past 6 months. We named Regina Sandler as Acting General Counsel, and selected Vincent Zehme and Jason Scalzo as the Special Agents in Charge (SAC) of our Chicago Region and Electronic Crimes Unit, respectively. Additionally, Jeff Pittano transferred from San Francisco to the OIG's Mid-Atlantic Region to serve as SAC. We brought on Erin Muru as the Director of Human Resources and Dan Battitori as AEC's new Planning and Operations Manager. We filled three Investigative Desk Officer positions as well as a Senior Human Resources Specialist position, and recruited other auditors, special agents, and human resources professionals with outstanding backgrounds and expertise.

I am proud of the accomplishments of all members of the OIG during the reporting period. Importantly, in light of events in the banking sector, which saw the failures of both Signature Bank of New York in March 2023 and First Republic Bank in May 2023, we have spent the past several months overseeing statutorily-required Material Loss Reviews of these two failures with estimated combined total losses to the Deposit Insurance Fund of $18 billion. Conducted by Cotton & Company Assurance and Advisory, LLC, these reviews evaluate the causes of the failures and assess the FDIC's supervision of the bank, and its implementation of Prompt Corrective Action. Results of these important reviews will be available on our website upon completion and will be highlighted in an upcoming semiannual report.

In closing, I note that in mid-September 2023, the President announced his nominee to serve to serve as the FDIC's fourth Presidentially appointed and Senate-confirmed Inspector General (IG). I have been honored to serve as Acting IG and to perform the duties of the IG as the FDIC Deputy Inspector General during the past 8 months. I join others in our office in looking forward to the confirmation of a permanent IG to continue leading our successful efforts. We appreciate the support of Members of Congress, and that of senior officials at the FDIC and its Board of Directors as we carry out the mission of the FDIC OIG. We remain committed to serving the American people with our strong independent oversight of the FDIC.

/s/

Tyler Smith
Acting Inspector General
October 2023

Table of Contents

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

Acronyms and Abbreviations

AD	Active Directory
AEC	Audits, Evaluations, and Cyber
AIG	Assistant Inspector General
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
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
DFA	Dodd-Frank Wall Street Reform and Consumer Protection Act
DIF	Deposit Insurance Fund
DOJ	Department of Justice
ECU	Electronic Crimes Unit
EIDL	Economic Injury Disaster Loan
EISP	Economic Inclusion Strategic Plan
FBI	Federal Bureau of Investigation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act of 2014
FRB	Federal Reserve Board
FSOC	Financial Stability Oversight Council
IG	Inspector General
InTREx	Information Technology Risk Examination
IRS-CI	Internal Revenue Service-Criminal Investigation
IT	Information Technology
OCC	Office of the Comptroller of the Currency
OI	Office of Investigations
OIG	Office of Inspector General
OLA	Orderly Liquidation Authority
OMB	Office of Management and Budget
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
SBA	Small Business Administration
SCRM	Supply Chain Risk Management
SIFC	Systemically Important Financial Company
USAO	United States Attorney's Office

Introduction and Overall Results

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

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

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

Overall Results (April 1, 2023–September 30, 2023)	
Audit, Evaluation, and Other Products Issued	**6**
Nonmonetary Recommendations	**71**
Investigations Opened	**46**
Investigations Closed	**30**
Judicial Actions:	
Indictments/Informations	**100**
Convictions	**53**
Arrests	**91**
OIG Investigations Resulted in:	
Special Assessments	**$12,600.00**
Fines	**$273,800.00**
Restitution	**$287,783,346.33**
Asset Forfeitures	**$322,202,180.92**
Settlement	**$4,027,804.69**
Total	**$614,299,731.94**
Referrals to the Department of Justice (U.S. Attorney)	**67**
Responses to Requests Under the Freedom of Information/Privacy Act	**11**
Subpoenas Issued	**1**

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 six reports addressing key areas in information technology (IT), consumer protection, supervision, and resolution. We made a total of 71 recommendations for improvements to FDIC programs and operations in these reports. We also formed part of a working group of the Council of Inspectors General on Financial Oversight (CIGFO), and contributed to the joint project on the *Audit of the Financial Stability Oversight Council's Efforts to Address Climate-Related Financial Risk*, and provided input to CIGFO's Annual Report regarding the FDIC OIG's work contributing to the broader financial sector.

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 is conducting Material Loss Reviews of these failures and will report the results of those publicly on our website when they are completed and include them in an upcoming semiannual report.

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. We were not conducting any In-Depth Reviews as of the end of the reporting period.

Results of the audits, evaluations, and other reviews completed during the reporting period are summarized below. A listing of ongoing assignments, in large part driven by our assessment of the Top Management and Performance Challenges Facing the FDIC, is also presented. Additionally, we provide an update on a matter that we have been addressing with the FDIC's Chief Information Officer Organization (CIOO) related to the security of OIG emails. We also provide information on several recommendations that were without management decisions as of our prior semiannual report.

Audits, Evaluations, and Other Reviews

FDIC Examinations of Government-Guaranteed Loans

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.

Our Office 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. We determined that FDIC bank examinations were not always effective in identifying and addressing risks related to Government-guaranteed loans. We found that the:

- FDIC's guidance did not adequately address risks present in Government-guaranteed loan programs;
- FDIC could improve its supervision of bank activities in Government-guaranteed loan programs, including the Paycheck Protection Program;
- FDIC's guidance differed from that of other Federal bank regulators;
- FDIC did not provide adequate training to examination personnel on Government-guaranteed lending programs;
- FDIC did not maintain adequate data to identify, monitor, and research bank participation in Government-guaranteed loan programs; and
- FDIC did not effectively share information externally and internally to enhance risk oversight of banks that participated in Government-guaranteed loan programs.

We also found that the FDIC's examination guidance did not provide clear instructions on the retention of examination workpapers.

We made 19 recommendations to the FDIC to address the findings in our report. The FDIC concurred or partially concurred with all of our recommendations and plans to complete corrective actions by March 31, 2024.

The FDIC's Adoption of Cloud Computing Services

In 2021, the FDIC began to accelerate its cloud migration to reduce its on-premises infrastructure and modernize its IT portfolio. The FDIC invested significant resources and made IT modernization the main priority of its IT strategy to improve internal operations. At the time of our audit, the FDIC planned to have most of its mission essential and mission critical systems operating in the cloud by 2024.

According to the FDIC, "mission essential" is defined as a system whose loss would cause a stoppage of the core operations supporting the FDIC's mission. "Mission critical" refers to a system whose loss would produce a significant impact on the FDIC's operations, but not its core mission.

Migration to the cloud introduces different security risks and privacy concerns, as cloud environments differ from traditional on-premises IT architectures. In addition, organizations need to align cloud adoption with organizational performance goals by taking into consideration business goals and operational efficiencies when developing and implementing cloud systems. Therefore, it is imperative that organizations have an effective IT modernization strategy to ensure an effective transition occurs and that governance processes are in place to manage different risks.

We performed an audit to determine whether the FDIC has an effective strategy and governance processes to manage its cloud computing services.

Overall, we found 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 the Office of Management and Budget (OMB), National Institute of Standards and Technology, and FDIC guidance in the following areas:

- **Data Inventory for Cloud-Based Systems:** The FDIC did not have an inventory of all data assets residing in its cloud environments or a fully developed data catalog (that is, an organized inventory of its cloud data assets).
- **Cloud Exit Strategy:** The FDIC did not establish an exit strategy as part of its cloud strategy planning to address issues (for example -- triggering events, roles and responsibilities, and portability and transitioning of data) if the FDIC needed to terminate a contract with a cloud service provider.
- **Contract Management Plans:** The FDIC did not develop Contract Management Plans for all 17 contract actions for cloud services valued at over $546 million.
- **Decommissioning Plans for Legacy Systems:** The FDIC did not develop disposal strategies and/or decommission plans for legacy systems.

These ineffective governance and strategy controls over cloud computing posed increased risks to the FDIC, including (1) security and privacy concerns due to the lack of visibility into cloud data, (2) inability to effectively move from an existing cloud service provider to another, (3) not identifying and mitigating performance risks and vulnerabilities in cloud contracts, and (4) increased potential for cyber attacks and costs from the lack of disposal strategies for legacy systems.

We determined that the FDIC had effective controls in seven other control areas related to application rationalization, IT governance bodies' alignment with cloud risks, cloud expenditures, cloud workforce transformation, assessment and authorization, continuous monitoring, and business continuity.

We made nine recommendations to strengthen the strategy and related governance processes for the FDIC's adoption of cloud computing services. FDIC management agreed with these recommendations and plans to complete corrective actions by September 2024.

Sharing of Threat and Vulnerability Information with Financial Institutions

Financial institutions face a wide range of significant and persistent threats to their operations. 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.

Our Office conducted an evaluation to determine whether the FDIC has implemented effective processes to ensure that financial institutions receive actionable and relevant threat and vulnerability information. We determined the FDIC has 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, the FDIC can improve the effectiveness of its processes to ensure financial institutions receive actionable and relevant threat and vulnerability information. We determined that:

- The FDIC can improve its sharing of threat and vulnerability information with financial institutions and other financial sector entities;
- The FDIC can improve its controls over the recording of computer-security incidents to support threat intelligence operations and sharing activities;
- The FDIC can mature its threat information sharing program by establishing procedures for sharing non-cyber related threat information and revising the program's existing threat sharing policies and procedures; and
- The FDIC can enhance its capabilities to identify threat and vulnerability information.

We made 10 recommendations to the FDIC to address the findings in our report. The FDIC concurred with all of our recommendations and plans to complete corrective actions by March 31, 2024.

FDIC Efforts to Increase Consumer Participation in the Insured Banking System

By way of background, the FDIC's *2021 FDIC National Survey of Unbanked and Underbanked Households* found that an estimated 4.5 percent of U.S. households were unbanked—meaning no one in the household had a checking or savings account at a bank or credit union. Additionally, an estimated 14.1 percent of U.S. households were underbanked—meaning someone in the household had a bank account, but they also used nonbank products or services, such as money orders, check cashing, international remittances, rent-to-own services or payday, pawn shop, tax refund anticipation, or auto title loans.

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 published its Economic Inclusion Strategic Plan (EISP) in June 2019. Its 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." From 2020 to 2023, the FDIC identified an FDIC Performance Goal to increase participation in the insured banking system through the implementation of the FDIC EISP.

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. Key findings were as follows:

- The EISP aligned with several strategic planning best practices. However, the FDIC can strengthen the effectiveness of future EISPs by incorporating additional best practices into the strategic planning process. These include performing a comprehensive assessment of the landscape; developing outcome-based measures for monitoring and evaluating progress; and identifying the internal risks and resources needed to achieve desired outcomes.
- The stated goal of the EISP generally supported the FDIC Performance Goal of increasing consumer participation in the insured banking system. However, the FDIC can strengthen connections between the annual FDIC Performance Goal and the EISP by ensuring that the expressed intent of annual goals related to the FDIC's economic inclusion efforts matches the goals and objectives articulated in the EISP.
- The FDIC can improve the implementation of future EISPs by aligning internal resources to achieve program objectives and measuring the outcomes of its economic inclusion efforts.
- The FDIC's risk mitigation strategies to address economic inclusion efforts could more clearly address risks related to implementing strategic objectives, effective controls, and responsive programs to promote economic inclusion.

Collectively, these actions would help the FDIC make the best use of Agency resources, ensure accountability, monitor progress, and make its strategic plan more effective in promoting economic inclusion.

We made 14 recommendations in the report. The FDIC concurred with all recommendations and plans to complete corrective actions by December 30, 2024.

The FDIC's Orderly Liquidation Authority

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.

We conducted an evaluation to determine whether the FDIC maintained a consistent focus on implementing the OLA program and established key elements to execute the OLA under the DFA.

We determined that the FDIC has made progress in implementing elements of its OLA program, including progress in OLA resolution planning for the global systemically important financial companies (SIFC) based in the United States. However, we found that in the more than 12 years since the enactment of the DFA, the FDIC has not maintained a consistent focus on maturing the OLA program. Since the enactment of the DFA, the FDIC's focus on other important, but competing, priorities delayed maturity of the OLA program.

We also found that the FDIC has not fully established key elements to execute its OLA responsibilities, including in the following areas:

- **OLA Policies and Procedures.** The FDIC has made significant progress in developing high-level policies and procedures for the execution of an OLA resolution of a systemically important bank holding company. However, it has not completed operational-level policies and procedures, nor identified how it would need to adjust its policies and procedures for an OLA resolution of other types of SIFCs. In addition, the FDIC has not developed two regulations required by the DFA or completed policies and procedures for ongoing OLA resolution planning activities.
- **OLA Roles and Responsibilities.** The FDIC has not fully defined governance and individual practitioner-level roles and responsibilities related to the execution of an OLA resolution.
- **OLA Resources, Training, and Exercises.** The FDIC needs to obtain additional staff resources to plan for an OLA resolution, and to fully identify and document the staff and contractor resources needed to execute an OLA resolution. In addition, the FDIC needs to enhance OLA-related training and exercises to regularly ensure that personnel have the skills needed to execute an OLA resolution.

- **Monitoring of OLA Activities.** The FDIC does not have adequate monitoring mechanisms in place to ensure it promptly implements the OLA program and consistently measures, monitors, and reports on the OLA program status and results.
- **Crisis Readiness-Related Planning.** The FDIC has not documented a readiness plan for executing OLA resolution authorities in a financial crisis scenario involving concurrent failures of multiple SIFCs.

Absent a consistent focus and fully established key elements for executing the OLA, the FDIC may not be able to readily meet the OLA requirements for every type of SIFC the FDIC might be required to resolve. If the FDIC were unable to resolve a SIFC, the banking sector and the stability of the U.S. and global financial systems could be severely affected.

We made 17 recommendations to the FDIC intended to improve key elements for executing the FDIC's OLA responsibilities. The FDIC concurred with all of these recommendations and plans to complete corrective actions by December 31, 2025.

The Federal Deposit Insurance Corporation's Information Security Program – 2023
The OIG issued its annual audit report pursuant to the Federal Information Security Modernization Act of 2014 (FISMA) during the reporting period. The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. The OIG engaged the firm of Cotton & Company Assurance and Advisory, LLC to perform this work based on guidance from the Office of Management and Budget.

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

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

- **The FDIC Needs to Fully Implement a Software Inventory Automation Program to Manage End-of-Life and End-of-Service Assets:** The FDIC's platform for monitoring software assets contained unreliable data that limited the FDIC's ability to manage software approaching or reached end-of-life or end-of-service.
- **The FDIC's Supply Chain Risk Management (SCRM) Program Lacks Maturity:** The FDIC is still developing policies and procedures to address the SCRM finding from the FY 2021 FISMA report. Additionally, the OIG evaluation report of *The FDIC's Implementation of Supply Chain Risk Management* (issued March 2022) included nine recommendations, five of which remained unimplemented as of July 28, 2023.

- **The FDIC Did Not Remove Accounts Belonging to Separated Personnel in a Timely Manner:** The FDIC did not consistently remove accounts for individuals who departed the FDIC. Of the accounts belonging to 44 employees and contractors sampled that departed the FDIC in 2023, six accounts belonging to three employees and two contractors were not disabled within one business day of the user separation as required. Access for the six accounts was removed between 4 and 84 days after the user separation date, including one privileged account.

- **The FDIC Did Not Configure Privileged Accounts in Accordance with the Principle of "Least Privilege":** In the OIG's earlier audit report of the *FDIC's Security Controls Over Windows Active Directory*, the OIG identified several instances where accounts were configured with elevated account settings that were not needed for administrators to perform their business roles. In other instances, users had elevated access longer than needed. The OIG issued 15 recommendations, 5 of which directly related to privileged accounts and remained unimplemented as of July 28, 2023.

- **The FDIC Needs to Enforce Cybersecurity and Privacy Awareness Training Requirements:** Over 400 personnel did not complete Cybersecurity and Privacy Awareness Training as required. As of July 13, 2023 (13 days after the training due date), these users retained access to the FDIC network and resources despite not having completed the required training due to technological issues preventing the application of existing training-related user access restrictions.

The report contained two recommendations related to removal of accounts belonging to separated personnel, and cybersecurity and privacy awareness training. The FDIC concurred with the recommendations and plans to complete corrective actions by June 28, 2024.

Audit of the Financial Stability Oversight Council's Efforts to Address Climate-Related Financial Risk *(Issued by CIGFO)*

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) authorizes CIGFO to convene working groups of its members to address issues within its jurisdiction. Accordingly, in September 2021, CIGFO voted to establish a Working Group to conduct an audit to assess the Financial Stability Oversight Council's (FSOC) response to Executive Order (EO) 14030, Climate-Related Financial Risk, issued in May 2021. FDIC OIG participated as a member of the Working Group.

CIGFO concluded that FSOC's actions were consistent with the policy, objectives, and directives set forth in EO 14030. Additionally, FSOC engaged with the member agencies to assess climate-related financial risk, and implemented an effective process to develop its Report on Climate-Related Financial Risk. CIGFO determined that the FSOC Report satisfactorily met the requirements set forth in EO 14030. Finally, FSOC established a means to facilitate ongoing coordination and information sharing among its member agencies on climate-related financial risk.

While the CIGFO Working Group made no recommendations in the report, the audit report encouraged FSOC, through the newly established Climate-Related Financial Risk Committee, to consider member agency suggestions and feedback to enhance the assessment and sharing of climate-related financial risk data and information.

CIGFO Annual Report 2023

CIGFO published its annual report in July 2023. This report highlights CIGFO activities and presents write-ups from the member agency OIGs related to their work to help strengthen the financial system through their oversight of Federal programs. We summarized several of our key assignments and provided input to this report. Of particular interest for this year and implications for the broader financial sector, our audit and evaluation work covered topics such as information security program controls and practices pursuant to the Federal information Security Modernization Act of 2014, background investigations for privileged account holders, security controls over the FDIC's wireless network, implementation of the FDIC's information technology examination program, and security controls over the FDIC's Windows Active Directory. We also summarized our February 2023 assessment of the Top Management and Performance Challenges Facing the FDIC.

Also included in the annual report are highlights from several financial fraud investigations that the FDIC OIG conducted. Such schemes can involve bank fraud, embezzlement, money laundering, currency exchange manipulation, and other crimes involving banks, executives, directors, officials, insiders, and financial professionals. Our Office also continues to play a key role in the investigation of individuals and organized groups perpetrating fraud through the Paycheck Protection Program (PPP) under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) and American Rescue Plan. The CIGFO Annual Report includes an example of one such case.

Top Management and Performance Challenges Drive Ongoing Work

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 2023 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, as follows:

- Preparing for Crises in the Banking Sector
- Mitigating Cybersecurity Risks at Banks and Third Parties
- Supervising Risks Posed by Digital Assets
- Fostering Financial Inclusion for Underserved Communities
- Fortifying IT Security at the FDIC
- Managing Changes in the FDIC Workforce
- Improving the FDIC's Collection, Analysis, and Use of Data
- Strengthening FDIC Contracting and Supply Chain Management
- Implementing Effective Governance at the FDIC

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 highlighted below:

- *FDIC Strategies Related to Crypto-Asset Risks.* The objective is to determine whether the FDIC has developed and implemented strategies that address the risks posed by crypto assets.
- *The FDIC's Purchase and Deployment of the FDIC Acquisition Management System.* The objective is to determine the primary factors that led to the FDIC's unsuccessful deployment of the FDIC Acquisition Management System.
- *The FDIC's Ransomware Readiness.* The objective is to assess the adequacy of the FDIC's process to respond to a ransomware incident.
- *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.
- *Material Loss Review of Signature Bank of New York.* The objectives, as mandated by the FDI Act, are to (1) evaluate the FDIC's supervision of the bank, including the FDIC's implementation of the Prompt Corrective Action (PCA) requirements of section 38 of the FDI Act and (2) determine why the bank's problems resulted in a material loss to the DIF.
- *The FDIC's Regional Service Provider Examination Program.* The objective is to assess the effectiveness of the FDIC's Regional Service Provider examination program in managing third-party risks to financial institutions.
- *Material Loss Review of First Republic Bank.* The objectives, as mandated by the FDI Act, are to (1) evaluate the FDIC's supervision of the bank, including the FDIC's implementation of the PCA requirements of section 38 of the FDI Act and (2) determine why the bank's problems resulted in a material loss to the DIF.

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

Update on Unresolved Recommendations Relating to Sharing of Threat Information to Guide the Supervision of Financial Institutions

Banks face a wide range of threats to their operations, including cyber attacks, money laundering, terrorist financing, pandemics, and natural disasters. The consequences of these threats may significantly affect the safety and soundness of numerous financial institutions – as well as the stability of the Nation's financial system.

Therefore, it is important that the FDIC develop policies, processes, and procedures to ensure that vital threat information is shared with its personnel – such as FDIC policymakers, bank examiners, supervisory personnel, and Regional Office staff – so that the data may be used in an actionable and timely manner. Our Office conducted a review to determine whether the FDIC had established effective and efficient processes to share threat information with its personnel. We identified several weaknesses in the FDIC's sharing of threat information and reported on those in a report issued in January 2022. We made 25 recommendations to the FDIC to strengthen its governance processes for acquiring, analyzing, disseminating, and using relevant and actionable threat information to guide the supervision of financial institutions.

In our semiannual report for the period ending September 30, 2022, we reported that two recommendations were unresolved and without management decisions. We indicated that if the recommendations were not resolved with management decisions by February 2023, we would elevate the matter to the FDIC's Follow-Up Official. We subsequently took that action, and received the Follow-up Official's final determination on these recommendations as of the end of this current reporting period. Additional information on these management decisions is presented in Table III in the Appendix of this report.

Update on Earlier Issue Raised in FISMA Report October 2021

In previous semiannual reports, 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. As an update for this semiannual reporting period, the FDIC has approved funding to further the steps that the CIOO intends to take during 2024 to modernize the FDIC and OIG email infrastructure. 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 100 indictments, 53 convictions, 91 arrests, and more than $614 million in fines, restitution ordered, and other monetary recoveries. We opened 46 cases and closed 30 during the reporting period.

Body Worn Camera training to comply with Executive Order 14074 requirements.

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

Our Office of Investigations (OI) successfully implemented its Body Worn Camera Program 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 held three in-person training sessions and three virtual sessions 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.fdicoig.gov/oig-videos.)

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

FDIC OIG Supports DOJ Initiatives to Combat COVID-19 Related Fraud

On August 23, the Justice Department announced the results of a coordinated, nationwide enforcement action to combat COVID-19 fraud, which included 718 enforcement actions - including Federal criminal charges against 371 defendants - for offenses related to over $836 million in alleged COVID-19 fraud.

DOJ also announced the launch of two additional COVID-19 Fraud Enforcement Strike Forces: one at the U.S. Attorney's Office for the District of Colorado, and one at the U.S. Attorney's Office for the District of New Jersey. These two strike forces add to the three strike forces launched in September 2022 in the Eastern and Central Districts of California, the Southern District of Florida, and the District of Maryland.

Several members of the FDIC OIG represented our Office at the meeting where the enforcement action was announced. The FDIC OIG is one of the many agencies that investigated these cases. The FDIC OIG will continue its strong support of these efforts.

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; USAOs; and 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 194 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 49 indictments and informations; 15 arrests; and 17 convictions and one pre-trial diversion, involving fraud in the CARES Act Programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases totaled in excess of $22.7 million.

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 datasets, developing tools and technology, and have hired data-science experts – in order to marshal our resources and harness voluminous data. We are looking for red-flag indicators in the statistics and information – 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.

Former Bank Chairman and Chief Executive Officer Sentenced to 14 Years in Prison for Conspiracy to Defraud Bank

Former First NBC Bank Chief Executive Officer, Ashton Ryan Jr. was sentenced to a term of imprisonment of 14 years and 2 months for bank fraud and making false statements in bank records. Ryan was ordered to pay restitution totaling over $214 million to the FDIC.

Following a 5-week trial, a jury convicted Ryan in February 2023 on all 43 counts against him. The charges related to Ryan's tenure as President, Chief Executive Officer, and Chairman of the Board at First NBC, a now-defunct Federally-insured financial institution with its main branch in New Orleans, Louisiana. Ryan and others conspired to defraud the bank through a variety of schemes, including by disguising the true financial status of certain borrowers and their troubled loans, and concealing the true financial condition of the bank from the bank's board, external auditors, and federal examiners. As Ryan's fraud grew, it included several other bank employees and business people from around the Gulf South area. Several of the borrowers who conspired with Ryan used First NBC money to pay Ryan individually or fund Ryan's own businesses. Using the bank's money this way helped Ryan conceal his use of such money for his own benefit.

When the bank's board, external auditors, and FDIC examiners asked about loans to these borrowers, Ryan and his fellow conspirators lied about the borrowers and their loans, hiding the truth about the borrowers' inability to pay their debts. As a result, the balance on the borrowers' fraudulent loans continued to grow, resulting, ultimately, in the failure of First NBC in April 2017. This failure caused approximately $1 billion in loss to the FDIC and the loss of approximately 500 jobs.

Source: The FDIC Legal Division.
Responsible Agencies: FDIC OIG, FBI, and Federal Reserve Board (FRB) OIG.
Prosecuted by the USAO, Eastern District of Louisiana.

Bank Insider Sentenced for COVID-19 Fraud

Omar Johann Esquivel Bello was sentenced to 15 months' imprisonment, followed by 3 years of supervised release, and ordered to pay a $100 assessment for his role in a CARES Act loan fraud scheme involving businesses owned by him, his wife, and his brother-in-law. Esquivel pled guilty to one count of wire fraud in November 2022.

Esquivel made material misrepresentations and submitted fraudulent documentation in connection with three applications for CARES Act Economic Injury Disaster Loans (EIDL) totaling $242,700 for companies he and his wife owned. Esquivel was a Relationship Manager at Bank of America during the time he applied for the loans. As part of his plea agreement, Esquivel agreed to consent to regulatory action taken by Federal financial institution regulatory agencies to permanently remove him from office and/or prohibit him from participating in the affairs of any insured depository institution.

From, in, or around June 2020, through in, or around August 2020, Esquivel fraudulently obtained for himself and for his wife, $242,700 in funds from the Small Business Administration (SBA) for companies connected to them, which he claimed had been adversely affected by the COVID-19 pandemic. In truth, the companies were defunct businesses. Esquivel filed annual reports with the State of Florida on the same day as the applications in order to make it falsely look like the businesses were operational. Esquivel also made false and fraudulent representations regarding the gross revenues of the businesses in order to secure larger loan amounts. Once the loan proceeds were received, accounts at Wells Fargo Bank, Bank of America, JP Morgan Chase Bank, Bank OZK, and Citibank were used to launder the loan proceeds. The loan proceeds were used to pay off Esquivel's vehicle loan and his wife's credit-card debts, to invest in real estate under his wife's brother's name, and to fund a new pool business for his wife's brother - all contrary to the intended purpose of the loans.

Source: Referral from the Fraud Section of the Criminal Division of the Department of Justice.
Responsible Agencies: FDIC OIG and the U.S. Department of the Treasury OIG.
Prosecuted by the USAO, Middle District of Florida.

Executives of Health Technology Company Convicted in $1B Corporate Fraud Scheme

In April 2023, a Federal jury convicted Outcome Health Chief Executive Officer and co-founder Rishi Shah, President and co-founder Shradha Agarwal, and Chief Operating Officer/Chief Financial Officer Brad Purdy for their roles in a fraud scheme that targeted the company's clients, lenders, and investors and involved approximately $1 billion in fraudulently obtained funds. Three other former employees of Outcome Health pled guilty prior to trial. Rishi Shah was convicted of five counts of mail fraud, ten counts of wire fraud, two counts of bank fraud and two counts of money laundering. Shradha Agarwal was convicted of five counts of mail fraud, eight counts of wire fraud and two counts of bank fraud. Brad Purdy was convicted on five counts of mail fraud, five counts of wire fraud, two counts of bank fraud, and one count of false statements to a financial institution.

Outcome Health, formerly Context Media, is a healthcare technology company. From 2012 through early 2017, former executives at Outcome Health engaged in a scheme to defraud and mislead pharmaceutical client companies about the extent and value of its services. Outcome Health presented fraudulent and false data, and made false representations in the delivering of their advertising services to their clients, lenders, and investors. Under-delivery of Outcome Health's services resulted in a material overstatement of its revenue in 2015 and 2016. Outcome Health used the inflated revenue numbers in its 2015 and 2016 audited financial statements to raise $110 million in debt financing in April 2016, $375 million in debt financing in December 2016, and $487.5 million in equity financing in early 2017. The $110 million in debt financing resulted in a $30.2 million dividend to Rishi Shah and a $7.5 million dividend to Shradha Agarwal; the $487.5 million in equity financing resulted in a $225 million dividend to Shah and Agarwal.

Source: Department of Justice, Criminal Division, Fraud Section and USAO, Northern District of Illinois.
Responsible Agencies: FDIC OIG and the FBI.
Prosecuted by the USAO, Northern District of Illinois and the Department of Justice, Criminal Division, Fraud Section. The Securities and Exchange Commission is litigating a related civil investigation.

Outreach by the OIG's Office of Investigations at a conference sponsored by the National Organization of Black Law Enforcement Executives.

Two Real Estate Developers Convicted of Conspiring to Embezzle Millions from Failed Chicago Bank

A Federal jury in Chicago convicted two real estate developers of participating in a conspiracy that embezzled millions of dollars from the failed Washington Federal Bank for Savings in Chicago. Washington Federal was shut down in 2017 after the Office of the Comptroller of the Currency (OCC) determined that the bank was insolvent and had at least $66 million in nonperforming loans.

On Friday, September 22, 2023, after a 2-week trial, Miroslaw Krejza and Marek Matczuk were each found guilty of conspiracy to embezzle, aiding and abetting embezzlement, and conspiracy to make false entries in the books and records of the now failed Washington Federal Bank for Savings. Evidence presented at trial showed that Krejza and Matczuk conspired with Washington Federal's president, John F. Gembara, and others to use purported loans as a vehicle to embezzle funds from the bank, with Krejza receiving $2.6 million and Matczuk receiving $6 million. Specifically, Krejza and Matczuk were each contractors who obtained construction loans from Washington Federal. Despite the fact that the properties upon which the loans were based were predominantly unfinished, and loan payments were not made, Krejza and Matczuk continued receiving checks posted to the loan accounts. In order to conceal the fact that payments were not being made, Washington Federal's loan servicer (a co-conspirator) would "advance" the loan payments by increasing the loan principal by the amount of the loan payment, falsely making it appear the payment was being made. In order to conceal the fraudulent loans from regulators, Washington Federal employees and co-conspirators lied to the OCC by claiming the bank's system could not export a loan trial balance using the industry standard format, instead providing the OCC with an Excel-based loan trial balance, which allowed them to manipulate the data to conceal the fraud.

For more than a decade, the developers were part of a conspiracy that embezzled millions of dollars in bank funds. The fraud continued for at least the last 10 years of the bank's existence, until it was discovered during an OCC bank examination in November 2017. During the examination, Gembara disappeared from the bank and did not return. Gembara was found deceased in Matczuk's home on December 13, 2017, and Washington Federal Bank for Savings failed on December 15, 2017. To date, the FDIC has lost over $80 million as a result of the failure.

In total, 16 individuals have been charged because of the bank's failure. Ten defendants pled guilty, two entered into deferred prosecution agreements, and the remaining four were found guilty via three separate trials.

Source: USAO, Northern District of Illinois.
Responsible Agencies: FDIC OIG, FBI, Housing and Urban Development OIG, Federal Housing Finance Agency OIG, Internal Revenue Service-Criminal Investigation (IRS-CI), Treasury OIG, City of Chicago OIG, and the Chicago Housing Authority.
Prosecuted by the USAO, Northern District of Illinois.

Two Loan Brokers and Former Vice President of Business Banking Plead Guilty

Two operators of a loan brokerage businesses, Ted Capodilupo, and Joseph Masci, pled guilty in Federal court in Boston to conspiring to defraud a Massachusetts-based bank and the SBA. Co-defendant Brian Ferris, a former Vice President of Business Banking at Berkshire Bank, pled guilty to conspiracy to commit bank fraud pursuant to an information filed in the District of Massachusetts.

Between 2015 and 2018, Capodilupo, Masci, and Ferris agreed to defraud the bank and the SBA by submitting fraudulent loan applications to the bank, which administered the SBA's small business express loan program, to secure bank loans guaranteed by the SBA. Specifically, Capodilupo and Masci submitted dozens of fraudulent loan applications to the bank on behalf of borrowers who were ineligible for traditional business loans. These loan applications misrepresented, among other things, the identity of the real loan recipients and the businesses for which the loans were sought.

Capodilupo and Masci also fabricated Federal tax forms submitted in support of the fraudulent loan applications, falsified applicant signatures, and falsely indicated that no broker had assisted in preparing or referring the loan applications. Capodilupo and Masci charged borrowers fees for obtaining these fraudulent loans. Ferris, who worked as a loan officer at the bank, caused the bank to issue loans for which Capodilupo and Masci submitted applications and received a kickback from Capodilupo and Masci of approximately $500 per loan. The scheme generated approximately $270,000 in fees for Capodilupo and Masci. Many of the loans that the bank issued as a result of the fraudulent applications ultimately defaulted, resulting in substantial losses to the bank.

Source: FDIC's Division of Risk Management Supervision.
Responsible Agencies: FDIC OIG, FBI, FRB OIG, and SBA OIG.
Prosecuted by the USAO, District of Massachusetts.

Members of the OIG's Office of Investigations speak on "Fighting Fraud and Ensuring Integrity" at the FDIC Accounting and Auditing Conference.

Attorney and Former Park Avenue Bank Board Member Convicted at Trial

Mendel Zilberberg, an attorney and former Park Avenue Bank Board member, was convicted in the Southern District of New York for violations of conspiracy to commit bank fraud, bank fraud, conspiracy to make false statements to a bank, making false statements to a bank, and embezzlement and misappropriation of bank funds. Zilberberg was convicted by a jury of his peers following a week-long criminal trial. Zilberberg colluded with multiple co-conspirators to secure a fraudulent nominee loan in the amount of $1,400,000 from the Park Avenue Bank. At the time of Zilberberg's activities, the Park Avenue Bank was critically deficient according to FDIC bank examination records.

Between June 2009 and October 2013, Mendel Zilberberg conspired with multiple individuals to fraudulently obtain a $1,400,000 commercial bank loan from the Park Avenue Bank. Zilberberg facilitated successful processing of the loan contingent upon receiving one-third of the loan's proceeds upon disbursement. Between 2009 and 2013, Zilberberg met with several co-conspirators on several occasions to structure the loan. Loan records reflect that: 1) the loan's proceeds were to be used as working capital for the nominee co-conspirators' businesses, 2) that Zilberberg was the co-conspirators' attorney and 3) the co-conspirators' purported net worth qualified them for the loan. One of the co-conspirators later admitted that he had no intention of using the money, that he never met Mendel Zilberberg, and that his reported net worth was inflated by multiple other co-conspirators to secure the loan. On September 8, 2009, the nominee co-conspirator received a $1.4 million loan from Park Avenue Bank. On the same day, a transfer of $466,000 was made to Zilberberg's company, One World United.

The Park Avenue Bank loan became delinquent in January 2010. Two months later, Park Avenue Bank failed. Subsequently, Valley National Bank purchased the assets of Park Avenue Bank and assumed the delinquent loan. The loan eventually defaulted, and Valley National Bank recognized a loss of $213,370. Pursuant to the loss share agreement between the FDIC and Valley National Bank, the FDIC incurred a loss of $853,483.

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

Former Business President Pleads Guilty to Bank Fraud

Former Service Foods Inc., President Keith Kantor pled guilty to one count of conspiracy to commit bank fraud from an information filed in the Western District of Tennessee. Kantor was charged for his role in an asset-based loan fraud scheme in which he directed employees to fraudulently submit false financial information in support of a line of credit causing a loss of over $10 million to First Horizon Bank (First Horizon). Kantor's co-conspirator, former Service Foods Chief Financial Officer Stuart Kagan, previously pled guilty to one count of conspiracy to commit bank fraud in January 2023.

Beginning on or before July 2011 through June 15, 2015, Kantor conspired with Service Foods employees to defraud First Horizon. Beginning in at least 2012, Kantor began directing Kagan to falsify the level of accounts receivable to maintain Service Foods' borrowing base line of credit. Kagan directed employees to create fictitious customer orders to increase the level of accounts receivable. In June 2015, First Horizon discovered Service Foods was kiting checks and subsequently discovered the accounts receivable were overstated by over $10 million. Between June 2015 and August 2015, First Horizon charged off over $10 million on the Service Foods loan.

Source: Referral from the financial institution.
Responsible Agencies: FDIC OIG and United States Postal Inspection Service.
Prosecuted by the USAO, Western District of Tennessee.

Individual Pleads Guilty to Telemarketing Theft Scheme

Michael Zeto pled guilty to nine counts of bank fraud, four counts of wire fraud, and seven counts of aggravated identity theft in the District of Nevada.

Zeto, a purported technology executive and telecom operator, partnered with foreign telemarketers who claimed to sell various products, including medical discount plans, telemedicine services, and identity theft protection to American consumers. The foreign telemarketers acquired victim bank information and other personally identifiable information from list brokers. The victims, almost invariably elderly and otherwise vulnerable, often did not agree to purchase the products and had not authorized anyone to debit their bank accounts. The foreign telemarketers then provided the fictitious sale information to Zeto, and he distributed the information to his complex network of shell corporations so they could debit the accounts of these purported customers, totaling over $20 million in proceeds.

As banks repeatedly closed the accounts for Zeto's network of shell companies due to high rates of returns, Zeto continuously opened new bank accounts to deposit the fraudulent checks and take money from the victims' accounts. Zeto ultimately adapted to the banks' concerns by contracting with a Third-Party Payment Processor. In order to deceive the banks, the payment processor flooded the business accounts with meaningless transactions to disguise the true rates of returns. This effectively prevented the banks from identifying how high the rates of returns were, putting the banks at operational and reputational risk.

Source: This investigation was initiated as a spinoff of other FDIC OIG investigations involving similar schemes with DOJ's Consumer Protection Branch.
Responsible Agencies: FDIC OIG and U.S. Postal Inspection Service.
Prosecuted by DOJ's Consumer Protection Branch.

Former South Florida Regional Bank Manager and Co-Conspirator Sentenced for Participation in Scheme to Defraud Financial Institutions through COVID-19 Relief Programs

Daniel Hernandez, a former South Florida regional manager for a leading national bank was sentenced to 120 months in prison for participating in a conspiracy to defraud the PPP out of loan proceeds. Co-defendant Erich Javier Alfonso Barata (Alfonso) was sentenced to 48 months' imprisonment followed by 3 years of supervised release for his role in a conspiracy that involved defrauding financial institutions and the Small Business Administration by fraudulently obtaining proceeds from the COVID-19 relief programs. Hernandez and his co-conspirators attempted to defraud the PPP and EIDL programs out of approximately $25 million. The conspiracy caused approximately $15 million in losses.

In or about March 2021, the USAO, Southern District of Florida, and FDIC OIG obtained information relating to CARES Act/PPP fraud being conducted by a bank executive and others. This investigation revealed an alleged scheme where numerous individuals conspired with recruiters/coordinators to obtain numerous PPP loans to be processed through two banks with the assistance of Daniel Hernandez and others.

In approximately April 2020, Alfonso was recruited by Hernandez to prepare and submit false and fraudulent PPP loan applications on behalf of companies that Alfonso controlled. Alfonso also agreed to prepare and submit false and fraudulent PPP loan applications on behalf of companies controlled by other co-conspirators. Hernandez informed Alfonso about the PPP program, instructed him on how to fill out the applications, and advised him on the type of supporting documentation to include. Alfonso and Hernandez agreed to charge each applicant a commission on every loan that was issued and share the proceeds.

Alfonso, at the request of Hernandez recruited over a dozen other applicants to submit false and fraudulent loans through himself and Hernandez. In each case, at Hernandez's direction, Alfonso prepared a false and fraudulent application that was submitted to financial institutions. For each co-conspirator, Alfonso received a commission of approximately 12 percent or 15 percent of the resulting loan that he shared with Hernandez.

Alfonso and Hernandez had a disagreement towards the end of 2020 and did not work together in furtherance of the conspiracy in 2021. Nonetheless, Alfonso, on his own, conspired with applicants to submit approximately 12 additional false and fraudulent PPP loan applications.

Source: Referral to the USAO, Southern District of Florida, and FDIC OIG.
Responsible Agencies: FDIC OIG, FBI, and SBA OIG.
Prosecuted by the USAO, Southern District of Florida, Money Laundering Section.

Tallahassee Couple Sentenced to Federal Prison for Wire Fraud Conspiracy, Money Laundering Conspiracy, and Making False Statements Relating to COVID-19 Relief Programs

Wilbert Jean Stanley, III and Felicia Jackson Stanley were sentenced, after previously pleading guilty to one count each of wire fraud conspiracy, money laundering conspiracy, and making false statements in connection with COVID-19 pandemic relief. Wilbert Stanley was sentenced to 40 months in Federal prison, and Felicia Stanley was sentenced to 24 months in prison.

Between March 1, 2020, and September 1, 2021, the Stanleys made false and fraudulent representations in applications to the SBA, financial institutions, and other lenders, for three different Federal COVID-19 relief programs: PPP loans, EIDLs, and Shuttered Venue Operators Grants. The false representations included inflated average monthly payroll expenses and the use of false tax forms as supporting documentation. The Stanleys submitted 166 false and fraudulent EIDL applications, of which 50 were funded, in their names for businesses that they owned and in the names of other individuals (whom they recruited). The Stanleys also submitted 20 false and fraudulent PPP loan applications, and 3 false and fraudulent grant applications in their names for businesses that they owned and in the names of other individuals (whom they recruited). For most of the applications that the Stanleys submitted (which were not in their names), the Stanleys had an arrangement with the named applicants to receive a kickback from the named applicants, which was paid from the PPP, EIDL, and grant proceeds.

Additionally, the Stanleys engaged in multiple monetary transactions that involved at least $10,000 of fraudulently obtained PPP loan, EIDL, or grant proceeds that they obtained through their scheme. Many of these transactions included payments for the purchase of real estate and to invest in virtual currency.

In total, through their false applications for Federal COVID-19 relief funds, the Stanleys attempted to obtain over $7 million for themselves and others, to which they were not entitled. The Stanleys were successful in fraudulently obtaining over $4.8 million in such funds.

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

Former Bank Vice President Pleads Guilty to Embezzlement

Angela Flippin, former Chief Operations Officer at People's Bank of Moniteau County entered a guilty plea to one count of embezzlement and one count of filing false tax returns. Flippin was the Vice President and Chief Operations Officer at the People's Bank of Moniteau County and admitted that she embezzled at least $550,000 from 2010 to 2017.

In January 2017, the Missouri Division of Finance discovered improper transactions involving Flippin. From 2010 through 2017, three areas of improper activity were identified: improper disbursements, improper expense reimbursements, and improper insurance premiums. Through their analysis, auditors determined Flippin received more than $550,000 in improper comp time disbursements and more than $8,000 in improper expense reimbursements.

Flippin personally held three separate bank accounts. Analysis of these bank accounts found Flippin made payroll deposits for $105,750. In addition to Flippin's payroll deposits there were other deposits that totaled $892,782. Analysis of expenditures from Flippin's bank accounts found $338,569 in PayPal online shopping transactions and other general debit card transactions.

Flippin also admitted that she failed to report the amounts that she embezzled from People's Bank of Moniteau County on her 2014, 2015, and 2016 Federal income tax returns. During those 3 years, she embezzled a total of $372,745, resulting in a total tax loss to the Federal government of $96,434.

Source: Missouri Division of Finance, FDIC Division of Risk Management Supervision.
Responsible Agencies: FDIC OIG, FHFA OIG, IRS, and FBI.
Prosecuted by the USAO, Western District of Missouri.

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 64 judicial districts in 36 locations in the U.S.:

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

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 HSI Financial Fraud Working Group; Northern District of New York PPP Fraud Working Group.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force; Northern District of Georgia Mortgage Fraud Task Force; Eastern District of North Carolina Bank Fraud Task Force; Northern District of Alabama Financial Fraud Working Group; Northern District of Georgia SAR Review Team; Middle District of Georgia SAR Review Team; South Carolina Financial Fraud Task Force; Eastern District of North Carolina Financial Crimes Task Force; Western District of North Carolina Financial Crimes Task Force; Middle District of North Carolina Financial Crimes Task Force; 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; Financial Crimes Task Force, USAO District of Hawaii.
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 Acting 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.
- Issued a joint message from the FDIC Chairman and Acting IG recognizing the importance of Whistleblower Appreciation Day.
- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
- Presented at several of the FDIC's "One FDIC" forum for new staff members and shared information on the mission, goals, and accomplishments of the FDIC OIG.
- Continued to enhance our external website, videos, and other social media presence to provide stakeholders better opportunities to learn about the work of the OIG, the findings and recommendations our auditors and evaluators have made to improve FDIC programs and operations, and the results of our investigations into financial fraud. Established the FDIC OIG's first LinkedIn presence to further disseminate information to our stakeholders about the work and the mission of our Office.

- Helped organize and actively participated in the FDIC's Accounting and Auditing Conference. The The Assistant IG (AIG) for Audits, Evaluations, and Cyber (AEC) joined the Chief Risk Officer in presenting on the theme of *Partners in Accountability*. In a session on *Fighting Fraud and Ensuring Integrity*, the AIG for Investigations, a Desk Officer, and a Senior Special Agent presented an overview of OI's mission and several case studies illustrating the nature and impact of our fraud investigations.

- Coordinated with DOJ and USAOs throughout the country in the issuance of press releases announcing results of cases with FDIC OIG involvement and informed FDIC senior leadership and other members of FDIC management of such cases, as appropriate.

- Maintained congressional working relationships by communicating with various Committee staff on issues of interest to them; providing them our *Semiannual Report to the Congress*; notifying interested congressional parties regarding the OIG's completed audit and evaluation work; providing staff briefings as requested; monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the FDIC's Office of Legislative Affairs on any Congressional correspondence pertaining to the OIG.

- Briefed House Financial Services Majority and Minority staff and House Oversight and Accountability Majority staff on the FDIC OIG's ongoing and planned work related to the recent bank failures.

- Maintained the OIG Hotline to field complaints and allegations of fraud, waste, abuse, and mismanagement affecting FDIC programs and operations from the public and other stakeholders. The OIG's Whistleblower Protection Coordinator also helped educate FDIC employees who had made or were contemplating making a protected disclosure as to their rights and remedies against retaliation for such protected disclosures. Our web-based hotline portal at https://www.fdicoig.gov/oig-hotline integrates seamlessly with our electronic investigative management system and enhances the efficiency and effectiveness of OIG Hotline operations. It also increases transparency and reporting capabilities that support our efforts to engage and inform internal and external stakeholders. During the reporting period, we handled 442 Hotline inquiries, 16 of which led to our opening investigations.

- Participated at the National Organization of Black Law Enforcement Executives' 47th Annual Conference where several Special Agents and our Criminal Research Specialist conducted outreach and shared information with law enforcement colleagues.

- Presented at the Women in Federal Law Enforcement Leadership Conference. Our AIG for Investigations spoke on the work and mission of OIGs, our specific mission at the FDIC OIG, law enforcement careers as a member of OI, leadership, and professional development for women in Federal law enforcement considering a career as an 1811 in the IG community. One of our Desk Officers and a Special Agent also conducted outreach and shared information about the FDIC OIG's OI with law enforcement colleagues during the conference.

- Attended the 2023 FBI Bank Fraud Conference in Atlanta, GA, where our AIG for Investigations and one of our Desk Officers spoke about the OIG mission and financial crimes impacting the U.S. banking sector. One of our Atlanta Region's Special Agents and his case partners from the FBI and SBA OIG also presented at the conference.

- Supported several Council of the Inspectors General on Integrity and Efficiency (CIGIE) forums related to audits and evaluations: One of our AEC Managers and an AEC Auditor presented the results of the OIG's audit of the *FDIC's Security Controls Over Microsoft Windows Active Directory* during the CIGIE Cybersecurity Working Group meeting. Another AEC Manager presented at the CIGIE-sponsored Connect, Collaboration, and Learn Working Group's training event titled, *Effective Communication when Conducting Audits, Evaluations, and Inspections - Part II*. A third AEC Manager presented on the progress of the CIGIE Monetary Impact Work Group during the CIGIE Inspections and Evaluations Town Hall event.

- 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 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. Formed part of the CIGFO team examining FSOC's Response to the Executive Order on Climate-Related Financial Risk, with a report issued in August 2023, and provided input to the CIGFO Annual Report on the work of our Office with impact to the broader financial sector.

- 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 2023 budget and proposed budget for FY 2024.

- 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.
- Acknowledged our FDIC OIG law enforcement agents, our law enforcement partners, and all who serve in our Nation's law enforcement community during National Police Week in May 2023 by way of a posted expression of gratitude for their commitment to public service and dedication to our country.
- 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.

- Carried out spending and hiring plans to make optimum use of the OIG's $47.5 million in requested funding for FY 2023. For FY 2024, the FDIC OIG proposed a budget of $49.8 million. The increase is necessary to sustain prior investments in IT and data analysis, and support critical OIG contractual audit services focused on cybersecurity and statutorily-mandated reviews of failed banks.
- Developed the OIG's Shutdown Plan and corresponding FAQs for a lapse in appropriations given a potential government shutdown after September 30. The OIG receives an annual appropriation in which Congress sets an amount that the FDIC is required to provide from the DIF for OIG operations. Absent the passage of a continuing resolution or enactment of an FY 2024 appropriations bill, our Office would have been required to shut down at that time.
- Issued an updated telework policy for the OIG. The main substantive change to this policy was that Managers should schedule in-office collaboration at least one day per pay period, effective on July 2. Indicated that if we did make changes to our policy to be consistent with new FDIC practices, those updates would not take effect any earlier than those for the FDIC--anticipated to be no sooner than January 2024. Coordinated staff space and equipment needs upon their return to the workplace.

- Held three in-person and three virtual training sessions on the use of Body Worn Cameras for our Special Agents in compliance with Executive Order 14074 - *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*.
- Held a 2-day All Hands Training in September in Charleston, South Carolina for our OI staff to collaborate and share investigative experiences. Special Agents refreshed their field techniques by participating in tactical entry training, active shooter and room clearing scenarios; control tactics training including ground control and handcuffing techniques; and emergency medical training.
- Developed a short survey to gauge OIG employees' overall impression of our Office of Management's operations, while also collecting ideas for how the Office can improve its services and support to all members of the OIG.
- Held a briefing by our IT staff to discuss and share thoughts on expanding the use of Microsoft Teams sites for more effective collaboration and other IT issues.
- 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 implementation of our Information Technology Strategic Plan and IT Road Map for 2021-2023, in coordination with the Division of Information Technology and the CIOO. The OIG's plan is designed to deliver robust and modern IT solutions to advance capabilities in supporting the OIG mission; support IT innovation and foster growth of technical skills and talent among OIG users; streamline and digitize information management workflows and processes; minimize development and operational costs; enhance the public relations of the OIG through the Internet-facing website; facilitate sharing of information and best practices; improve the OIG's overall security posture and disaster recovery capabilities; and enhance support for telework and the digital workplace. Kept staff fully apprised of steps they needed to take to ensure the ongoing security of OIG information systems, data, equipment, and electronic devices.
- Continued to refine, adjust, and leverage a new audit management platform, eCase. It creates a system of record to document the work performed and review of that work to support report findings consistent with applicable professional standards. It also allows us to build dashboards to track assignments relative to office benchmarks; monitor the FDIC's implementation of OIG report recommendations; and ensure that staff meet professional standards. Ensured that that the OIG's new platform complies with the FDIC's system security requirements and has the ability to adapt to new technical requirements and advancements.

- Leveraged the OIG's Electronic Crimes Unit's laboratory. The laboratory allows field Agents to remotely access a server-based lab environment which allows for the storage and processing of digital evidence into forensic reviewable data. This capability greatly increases the efficiency and effectiveness of the investigative process by allowing for much quicker actuation of data into e-discovery platforms. The build-out of the ECU has also facilitated financial fraud investigations, including cyber crimes at banks.

- Continued to pursue OIG data management strategies and solutions. Auditors, criminal investigators, and information technology professionals are seeking to ensure that we are leveraging the power of data analytics to inform organizational decision making and ensure we are conducting the most impactful audits, evaluations, reviews and investigations. Focused on establishing an OIG data governance framework, implementing a data analytics platform, establishing data integration technologies, and implementing an OIG data warehouse that integrates with the FDIC's data warehouse to facilitate OIG analysis and reporting of FDIC data.

- Advanced the OIG's data analytics project 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 OIG complied with legal and ethical standards, rules, principles, and guidelines; provide legal advice and counsel to teams conducting audits, evaluations, and other reviews; and support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.

- Continued to review and update a number of OIG internal policies related to audit, evaluation, investigation, operations, and administrative processes of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the Office. For example, updated and/or posted policies regarding such topics as Deconfliction of OIG Activities, OIG Petty Cash Policy, Records Management, Monitoring the Use of Information Technology, and External and Removable Media.

- 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 two Special Agents in Charge and the transfer of one Special Agent in Charge, Director of Human Resources, AEC Planning and Operations Manager, Desk Officers, and a Senior Human Resources Specialist.

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

Exercising leadership skills and promoting teamwork.

- Held a Town Hall meeting in April, during which the Acting IG and the Executives shared updates on the state of the Office, including summaries from OIG components about their ongoing work and how it relates to the OIG mission; telework; and upcoming office initiatives such as S-Drive migration, iPhone refresh, and other OIG projects.
- Encouraged use of 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. Provided all staff an opportunity to share their opinions about what the FDIC OIG is doing well and where improvements can be made.
- Held an OI leadership team meeting in the New York Regional Office for wide-ranging discussions on values, vision, culture, staff development, policy and procedures, training, investigative operations, and more.
- 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. Posted a video on our external website presenting the DEIA Plan to the public.
- 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.

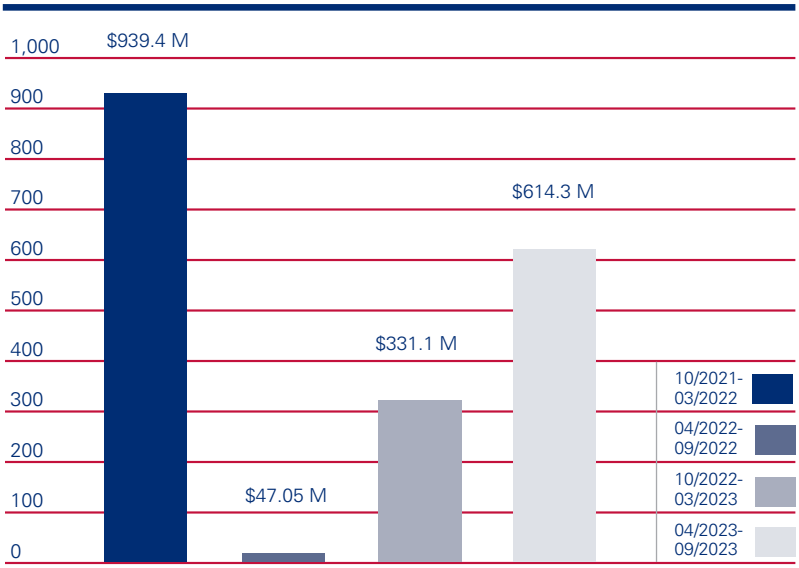
- Supported efforts of the Workforce Council. The Council hosted a forum exploring "A Day in the Life of the Acting Inspector General," and also sponsored its "Let's Move OIG" fitness challenge for all staff. The mission of this Council is to foster and support a workplace that engages employees, builds 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.
- Provided joint training by members of the OIG's Office of General Counsel and AEC to other Counsel and AEC colleagues on the process for redacting AEC published reports to protect sensitive information that is posted publicly on the OIG external website.
- Supported OIG staff pursuing professional training, banking schools, and certifications to enhance their expertise and knowledge. These included staff participation at the ABA Stonier Graduate School of Banking at the Wharton School of the University of Pennsylvania, and preparation to become a Certified Information Systems Auditor.
- Organized several social activities, including component-specific Coffee Chats, to promote community, teamwork, and collegiality among OIG staff.
- Held training sponsored by the Arbinger Group for OIG staff to explore approaches that move individuals, teams, and organizations from the default self-focus of an inward mindset to the results focus of an outward mindset. Followed up with additional sustainment discussion sessions for attendees.
- Continued a leadership role in a working group on behalf of CIGIE's Audit and Inspection and Evaluation Committees related to Monetary Impact. The FDIC OIG AIG for AEC and an Audit/Evaluation Manager have 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, book discussions, 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 OIG's Diversity, Equity, Inclusion and Accessibility Working Group. Hosted a series of events to highlight diversity, including to recognize Arab American Heritage Month, Jewish American Heritage Month, Asian American/ Native Hawaiian/Pacific Islander Heritage Month, LGBTQ+ Pride Month, Juneteenth, and Women's Equality Day.
- Hosted a virtual event presenting the National Aeronautics and Space Administration (NASA) Office of Inspector General's audit engagement, "NASA Efforts to Increase Diversity in its Workforce." The NASA team shared its best practices in performing oversight work in the area of DEIA.
- 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.
- Led efforts of the PRAC's Law Enforcement Coordination Subcommittee. Our AIG for Investigations served as Chair of this group through July 2023. 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.

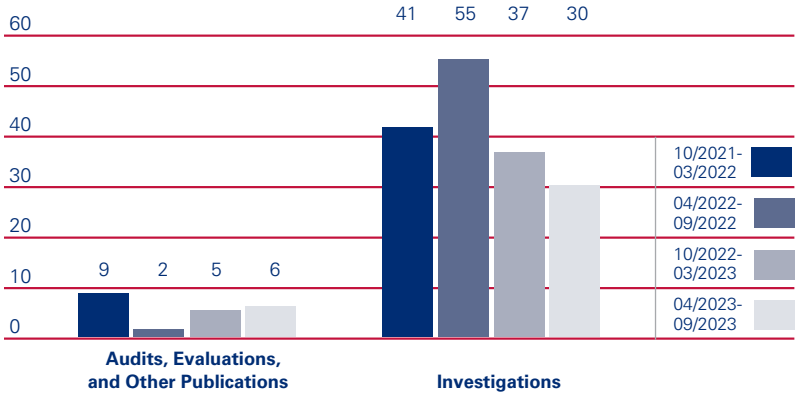
Cumulative Results (2-year period)

Recommendations	
October 2021 – March 2022	77
April 2022 – September 2022	1
October 2022 – March 2023	56
April 2023 – September 2023	71

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.	42
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.)	44-53
Section 5(a)(3): A summary of significant investigations closed during the reporting period.	18-27
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.	54
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.	55
Section 5(a)(7): The information described under section 804(b) of the Federal Financial Management Improvement Act of 1996.	56
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.	58-60

Reporting Requirements (continued)	Page
Section 5(a)(9): A list of any outstanding recommendations from any peer review conducted by another Office of Inspector General that have not been fully implemented, including a statement describing the status of the implementation and why implementation is not complete.	58-60
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.	58-60
Section 5(a)(11): Statistical tables showing, for the reporting period: • number of investigative reports issued during the reporting period; • the total number of persons referred to the Department of Justice for criminal prosecution during the reporting period; • the total number of persons referred to State and local prosecuting authorities for criminal prosecution during the reporting period; and • the total number of indictments and criminal informations during the reporting period that resulted from any prior referral to prosecuting authorities.	56
Section 5(a)(12): A description of metrics used for Section 5(a)(11) information.	56
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.	56
Section 5(a)(14): (A) A detailed description of any instance of whistleblower retaliation, including information about the official found to have engaged in retaliation; and (B) what, if any, consequences the establishment actually imposed to hold the official described in subparagraph (A) accountable.	56
Section 5(a)(15): Information related to interference by the establishment, including— (A) a detailed description of any attempt by the establishment to interfere with the independence of the Office, including— (i) with budget constraints designed to limit the capabilities of the Office; and (ii) incidents where the establishment has resisted or objected to oversight activities of the Office or restricted or significantly delayed access to information, including the justification of the establishment for such action; and (B) a summary of each report made to the head of the establishment under section 6(c)(2) during the reporting period.	56
Section 5(a)(16): Detailed descriptions of the particular circumstances of each - (A) inspection, evaluation, and audit conducted by the Office that is closed and was not disclosed to the public; and (B) investigation conducted by the Office involving a senior Government employee that is closed and was not disclosed to the public.	56

Appendix 1

Information Responding 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 and/or comment on enacted law or proposed legislative matters. Much of the FDIC OIG's activity considering and reviewing legislation and regulation occurs in connection with that Committee, on which the FDIC OIG is a member.

The 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 Permanent Data and Analytics Capability for the IG Community, Establishing Authority for IGs to Provide Continuous Oversight During a Lapse in Appropriations, Congressional Notification When Legislative Branch IGs Are Placed on Non-Duty Status, and Statutory Exclusion for Felony Fraud Convicts to Protect Federal Funds. Additionally, the Committee provided input to proposed legislation related to information security that would be covered under the Federal Information Security Management Act of 2023. The Committee also solicited feedback on draft proposed legislation to amend Section 5274 of the National Defense Authorization Act regarding submission of reports that specifically identify non-governmental organizations or business entities.

Table I: Unimplemented Recommendations from Previous Semiannual Periods*

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-20-001 **Contract Oversight Management** October 28, 2019	The FDIC relies heavily on contractors for support of its mission, especially for information technology, receivership, and administrative support services. Over a 5-year period from 2013 to 2017, the FDIC awarded 5,144 contracts valued at $3.2 billion. Our evaluation objective was 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. 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. The report contained 12 recommendations to strengthen contract oversight.	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	
EVAL-21-002 **Critical Functions in FDIC Contracts** March 31, 2021	The FDIC relies on contractors to provide services in support of its mission. Some of these services cover Critical Functions. We conducted an evaluation to determine whether one of the FDIC's contractors was performing Critical Functions as defined by guidance issued by the Office of Management and Budget (OMB); and if so, whether the FDIC provided sufficient management oversight of the contractor performing such functions. The FDIC did not have policies and procedures for identifying Critical Functions in its contracts, as recommended by OMB Policy Letter 11-01 and best practices. However, we determined that Blue Canopy performed Critical Functions at the FDIC, as defined by OMB Policy Letter 11-01 and best practices. These services are critical to ensuring the security and protection of the FDIC's information technology infrastructure and data. A breach or disruption in these services could impact the security, confidentiality, integrity, and availability of FDIC information. Therefore, the FDIC needed proper oversight of the Critical Functions performed by Blue Canopy to ensure such a breach or disruption of service did not occur. The FDIC, however, did not identify the services performed by Blue Canopy as Critical Functions during its procurement planning phase. Therefore, the FDIC did not implement heightened contract monitoring activities for Critical Functions as stated in OMB's Policy Letter 11-01 and best practices. The report contained 13 recommendations aimed at strengthening the FDIC's internal controls over Critical Functions to align with OMB Policy Letter 11-01 and best practices.	13	5**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-22-001 **The FDIC's Information Security Program – 2021** October 27, 2021	The FDIC OIG engaged the firm of Cotton & Company LLP to perform our annual audit under the Federal Information Security Modernization Act of 2014 (FISMA). The audit was planned and conducted based on the Department of Homeland Security's reporting metrics: Fiscal Year 2021 Inspector General Federal Information Security Modernization Act of 2014 (DHS FISMA) Reporting Metrics Version 1.1 (May 2021) (DHS FISMA Metrics). Inspectors General assign maturity level ratings to key security function areas and the overall security program, using a scale of 1-5. At the time of our audit, ratings were determined by a simple majority where the most frequent level (mode) across the component questions would serve as the domain rating. The FDIC's overall information security program was operating at a Maturity Level 4. The FDIC had established certain information security program controls and practices that were consistent with information security policy, standards, and guidelines. However, the audit report describes significant control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. The report contained six recommendations to address these weaknesses.	6	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	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. 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. 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. In addition, we determined that the FDIC had not established any requirements for FDIC officials to determine whether contractors have 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. The report contained 10 recommendations intended to ensure that contractors and subcontractors are informed of their whistleblower rights and protections.	10	1**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-22-003 **Sharing of Threat Information to Guide the Supervision of Financial Institutions** January 18, 2022	To fulfill its mission, the FDIC acquires, analyzes, and disseminates threat information relating to cyber and other threats to the financial sector and FDIC operations. Effective sharing of threat information enriches situational awareness, supports informed decision-making, and guides supervisory strategies and policies. Our audit objective was to determine whether the FDIC established effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. We found that the FDIC did not establish effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. The FDIC acquired and analyzed certain information pertaining to threats against financial institutions and disseminated some information to certain supervisory personnel. However, we identified gaps in each component of the Threat Sharing Framework-Acquisition, Analysis, Dissemination, and Feedback. The report contained 25 recommendations.	25	1**	NA
EVAL-22-003 **The FDIC's Implementation of Supply Chain Risk Management** March 1, 2022	In 2021, the FDIC awarded 483 contracts totaling over $2 billion for the acquisition of products and services. These products and services are 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. Our evaluation objective was to determine whether the FDIC developed and implemented its SCRM Program in alignment with the Agency's objectives and best practices. 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. In addition, the FDIC had not integrated Agency-wide supply chain risks into the its Enterprise Risk Management processes. We also determined that Contracting Officers did not maintain contract documents in the Contract Electronic File system, as required. The report contained nine recommendations to improve the FDIC's SCRM Program and retention of contract documents.	9	5**	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-22-004 **The FDIC's Information Security Program – 2022** September 27, 2022	The Federal Information Security Modernization Act of 2014 (FISMA), Public Law No. 113-283, requires Federal agencies, including the FDIC, to conduct annual independent evaluations of their information security programs and practices and to report the results to the Office of Management and Budget (OMB). FISMA requires the independent evaluations to be performed by the agency IG, or an independent external auditor as determined by the IG. Cotton & Company Assurance and Advisory, LLC performed this work on the OIG's behalf. The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. The audit found that the FDIC had established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and National Institute of Standards and Technology security standards and guidelines. In addition, the FDIC had completed certain actions to continue to strengthen its security controls since the prior year, such as prioritizing the remediation of Plans of Action and Milestones; remediating outdated baseline configurations; and finalizing an Identity, Credential, and Access Management Roadmap. However, the audit found security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. These control weaknesses could be improved to reduce the impact on the confidentiality, integrity, and availability of the FDIC's information systems and data. The report contained one recommendation for the FDIC to address the 31 flaw remediation Plans of Action and Milestones.	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	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. Our evaluation objective was to determine whether the FDIC has implemented effective security controls to protect its wireless networks. We engaged the professional services firm of TWM Associates, Inc. to conduct the technical aspects of this review. We found that the FDIC did not comply or partially complied with several practices recommended by the National Institute of Standards and Technology and Federal and FDIC guidance in the following five areas: 1. Configuration of Wireless Networks 2. Wireless Signal Strength 3. Security Assessments and Authorizations 4. Vulnerability Scanning 5. Wireless Policies, Procedures, and Guidance The report contained eight recommendations intended to strengthen the security controls over the FDIC's wireless networks.	8	6	NA

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

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

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-23-002 **The FDIC's Security Controls Over Microsoft Windows Active Directory** March 15, 2023	The FDIC relies heavily on information systems containing sensitive data to carry out its responsibilities. To ensure that only individuals with a business need are allowed access, the FDIC uses Active Directory (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. 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. 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. The report contained 15 recommendations to improve AD security controls.	15	15	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	In February 2014, the FDIC awarded a telecommunications service contract to AT&T Corp. (AT&T) in the amount of $12 million for telecommunication services. In May 2019, the FDIC Chief Information Officer Organization (CIOO) approved a strategy to upgrade the bandwidth of AT&T's telecommunication services within the FDIC Field Offices. In March 2021, the FDIC CIOO notified the OIG of major internal control failures with the telecommunications contract. We conducted a review to determine if the FDIC authorized and paid AT&T for services to upgrade bandwidth in FDIC Field Offices in accordance with its policies and procedures and existing telecommunications contract. We determined that the FDIC did not authorize and pay AT&T for services to upgrade bandwidth in the FDIC Field Offices in accordance with its policies and procedures and existing telecommunications contract. The FDIC did not adhere to its acquisition policies and procedures because FDIC CIOO Executive Managers did not establish an accountable organizational culture or "tone at the top" for compliance with FDIC acquisition policies and procedures. FDIC CIOO Executive and Corporate Managers also did not implement proper internal controls for the AT&T contract. In addition, risks related to the FDIC CIOO's reliance on contractor services and the need to maintain an effective internal control environment for its contract oversight management activities were not included in the FDIC's Enterprise Risk Management Risk Inventory. Lastly, FDIC CIOO personnel failed to fulfill their roles and responsibilities with regard to the AT&T contract. The report contained 14 recommendations.	14	14	$1,500,000

*A current listing of each of our unimplemented recommendations is available here: https://www.fdicoig.gov/unimplemented-recommendations. This listing is updated monthly.

** Indicates recommendations that have been open for more than one year.

Table II: Audit and Evaluation Reports				
Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	Title*	Total	Unsupported	
EVAL-23-001 May 10, 2023	*FDIC Examinations of Government-Guaranteed Loans*			
AUD-23-003 July 25, 2023	*The FDIC's Adoption of Cloud Computing Services*			
EVAL-23-002 August 29, 2023	*Sharing of Threat and Vulnerability Information with Financial Institutions*			
EVAL-23-003 September 13, 2023	*FDIC Efforts to Increase Consumer Participation in the Insured Banking System*			
AUD-23-004 September 25, 2023	*The Federal Deposit Insurance Corporation's Information Security Program - 2023*			
EVAL-23-004 September 28, 2023	*The FDIC's Orderly Liquidation Authority*			
Totals for the Period		**$0**	**$0**	**$0**

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

Note: Other products issued:

• Members of our Office formed part of the CIGFO Working Group issuing the *Audit of the Financial Stability Oversight Council's Efforts to Address Climate-Related Financial Risk* on August 9, 2023. The OIG also provided input to the *CIGFO Annual Report*, issued on July 27, 2023.

Table III: Status of Management Decisions on OIG Recommendations from Past Reporting Periods.
(Note: The information in this table relates to management decisions for recommendations made in a report issued in January 2022.)

During the last reporting period, there were three recommendations more than 6 months old without management decisions. In our report, *Sharing of Threat Information to Guide the Supervision of Financial Institutions (AUD-22-003)*, dated January 18, 2022, we found that the FDIC had not established the necessary infrastructure to enable dissemination or receipt of classified National Security Information in its Regional Office locations.

On March 21, 2023, we elevated the three recommendations to the Audit Follow-up Official for a final Management Decision. We received a response from the Audit Follow-up Official on May 30, 2023. The Audit Follow-up Official committed the FDIC to conducting reevaluations no less frequently than biannually of its decision to share information with Regional Directors and other Regional Office personnel in unclassified form only. Further, the Audit Follow-up Official committed the FDIC to obtain the necessary security clearances and provide the necessary procedures, infrastructure, and security clearances if any reevaluation – or information arising in between these biannual evaluations – indicates that sharing information with the Regional Offices at a classified level would materially improve supervision activities. We reviewed the final agency decision pertaining to management's actions to address the three recommendations of the subject report and concluded that the final agency decision was responsive. Therefore, the recommendations are now closed.

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	30
Number of Persons Referred to the Department of Justice for Criminal Prosecution	67
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	None
Number of Indictments and Criminal Informations	100

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

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

During this reporting period, there were no investigations involving senior government employees where allegations of misconduct were substantiated.

Table VII: Instances of Whistleblower Retaliation

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

Table VIII: Instances of Agency Interference with OIG Independence

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

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

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

During this reporting period, there were no audits or evaluations involving senior Government employees that were closed and not disclosed to the public. There were no investigations of senior government officials that were closed and not disclosed publicly.

Appendix 2

Information on Failure Review Activity

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

FDIC OIG Review Activity for the Period April 1, 2023 through September 30, 2023 (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 did not issue any Failed Bank Reviews during the reporting period, and 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 as well. 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.

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 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 FDIC OIG's associated internal policies and procedures.

Investigative Peer Reviews

Quality assessment peer reviews of investigative operations are conducted on a 3-year cycle. Such reviews result in a determination that an organization is "in compliance" or "not in compliance" with relevant standards. These standards are based on *Quality Standards for Investigations* and applicable Attorney General Guidelines, and Section 6(e) of the Inspector General Act of 1978, as amended.

The Department of the Treasury OIG conducted a peer review of our investigative function and issued its final report on the quality assessment review of the investigative operations of the FDIC OIG on May 9, 2019. The Department of the Treasury OIG reported that in its opinion, the system of internal safeguards and management procedures for the investigative function of the FDIC OIG in effect for the year ending October 31, 2018, was in compliance with quality standards established by CIGIE and the other applicable Attorney General guidelines and statutes noted above. These safeguards and procedures provided reasonable assurance of conforming with professional standards in the planning, execution, and reporting of FDIC OIG investigations and in the use of law enforcement powers.

The next peer review of our investigative operations was scheduled for Fall 2023 and was to be conducted by the Department of Veterans Affairs OIG. As of the end of the reporting period, this review was in process.

Congratulations and Farewell

During the reporting period, we congratulated and said farewell to Mary Carmichael and Sandra Moses, highly esteemed members of the OIG's Office of Audits, Evaluations, and Cyber. Ms. Carmichael, Planning and Operations Manager, retired after a career of more than 37 years of Federal service. Ms. Moses, a Senior Audit Specialist, served for more than 34 years in the Federal government.

Both of these individuals made immeasurable contributions in carrying out the OIG mission and realizing the vision of our Office: *Serving the American people as a recognized leader in the Inspector General 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.*

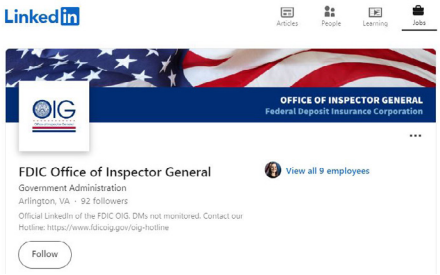
Throughout their tenure in the OIG, they fostered constructive working relationships within our Office, with the FDIC's senior leadership and Division and Office management, and other OIGs. We thank them for their dedication and commitment to our Office and its mission. We wish them all the best in their future endeavors.

DESIGN: FDIC/OCOM/GRAPHIC DESIGN AND PRINTING UNIT

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

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

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



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

OVERSIGHT.GOV
ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE

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

PANDEMIC RESPONSE ACCOUNTABILITY COMMITTEE

www.pandemicoversight.gov

★**Learn more about the IG community's commitment to 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

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

FDIC-019-2023