FDIC Office of Inspector General

Semiannual Report to the Congress

October 1, 2022 – March 31, 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 by insuring deposits, examining and supervising financial institutions, and managing receiverships. Approximately 5,612 individuals carry out the FDIC mission throughout the country.

According to the most current FDIC data, the FDIC insured $10.07 trillion in domestic deposits in 4,706 institutions, of which the FDIC supervised 3,032. The Deposit Insurance Fund balance totaled $128.2 billion as of December 31, 2022. Active receiverships as of April 30, 2023 totaled 118, with assets in liquidation of about $192.6 billion.

Semiannual Report to the Congress

October 1, 2022 – March 31, 2023

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 October 1, 2022 through March 31, 2023.

I have been honored to serve as the Acting Inspector General (IG) of the FDIC since January 27, 2023, when former IG Jay N. Lerner retired from Federal service. IG Lerner led our Office for more than 6 years, and we recognized his contributions as a public servant of more than 30 years at a retirement ceremony in January 2023.

This semiannual report highlights four audit and evaluation reports issued during the period. These reports addressed issues related to Information Technology (IT), Supervision, and Contracting. Specifically—we examined security controls over the FDIC's wireless network, security controls over the FDIC's Windows Active Directory, implementation of the FDIC's IT risk examination program, and the FDIC's oversight of a telecommunications contract with AT&T Corp. We made 56 recommendations to address needed improvements in these areas, and the FDIC is working to address them.

We also issued our annual report on the Top Management and Performance Challenges Facing the FDIC, which presents our assessment of the most significant risks on which policymakers should focus attention. We identified the following challenges:

- 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

Our investigations during the reporting period resulted in 50 indictments/informations; 56 convictions; 40 arrests; and more than $331 million in fines, restitution ordered, assessments, and other monetary recoveries.

In one of our cases, a rancher was sentenced to 132 months of imprisonment, 3 years of supervised release, and ordered to pay more than $244 million in restitution in the Eastern District of Washington. He orchestrated and carried out a massive, brazen, and long-term "ghost cattle" scheme where he fraudulently billed Tyson Foods and another company more than $244 million for the purchase and feeding of cattle that never existed. The rancher obtained fraudulent multi-million dollar loans from FDIC-regulated and insured institutions to facilitate the scheme, and also defrauded CME Group Inc., the world's largest operator of financial derivatives exchanges. In defrauding the CME Group Inc., the rancher caused potential losses to FDIC-regulated and insured institutions with direct or financed holdings. The scheme was the largest-ever criminal fraud scheme prosecuted in the Eastern District of Washington.

Our investigations involving pandemic-related fraud continued to account for many judicial actions and monetary benefits during this period. To date, we have opened 190 cases associated with fraud in the 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 steal funds from Government programs intended for those most in need during the pandemic. In one of our cases this period, for example, a former Florida State Representative pleaded guilty to wire fraud, money laundering, and making false statements in connection with COVID-19 relief fraud.

Our Electronic Crimes Unit (ECU) continues to ensure that our Special Agents are equipped with the latest cutting-edge technology and tools to investigate financial crimes that directly and indirectly impact FDIC programs and operations. We continue to focus on our ECU's ability to successfully ingest large amounts of evidentiary data and the successful investigation of cyber crimes at banks, including computer intrusions, cryptocurrency, ransomware, and account takeovers.

Throughout the reporting period, we have also further developed our 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 looking for red-flag indicators and aberrations in the underlying facts and figures, in order to proactively identify tips and leads for further investigation or audit, detect high-risk areas at the FDIC, and recognize emerging threats to the banking sector.

Our Office said farewell during the reporting period not only to former IG Lerner, but also to Deputy IG Gale Stallworth Stone. Gale retired after a Federal career of more than 37 years. We will miss her contributions to our OIG team. On a positive note, Michael McCarthy will serve as Acting Deputy IG and Stacey Luck will fill the role of Acting General Counsel. We also welcomed talented new members and enhanced our OIG leadership team over the past 6 months. We named Bronzwyn Palmer as our Assistant IG (AIG) for Management and Quenton Sallows as our Deputy AIG for Investigations. We have brought on a Director of Human Resources, other financial professionals, auditors, and special agents with outstanding backgrounds and expertise.

I am proud of the accomplishments of members of the OIG and am especially grateful for their unwavering pursuit of the mission of the OIG during a time of transition in our Office. In light of recent events in the banking sector, which saw the failure of Silicon Valley Bank and Signature Bank, the upcoming months will be challenging for our Office. We are reviewing issues related to those failures in coordination with our law enforcement and audit partners. Since the FDIC is the primary Federal regulator for Signature Bank, we have begun a statutorily-required Material Loss Review to evaluate the FDIC's supervision of the bank and the causes of the failure. I am confident that we are up to this complex task.

We appreciate the support of Members of Congress, and that of senior officials at the FDIC and its Board of Directors, including the two newest Members of the Board, Vice Chairman Travis Hill, and Director Jonathan McKernan. We remain committed to serving the American people with our strong independent oversight of the FDIC.

/s/

Tyler Smith
Acting Inspector General
April 2023

Table of Contents

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

Acronyms and Abbreviations

AD	Active Directory
AIG	Assistant Inspector General
BSA/AML	Bank Secrecy Act/Anti-Money Laundering
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
DHS	Department of Homeland Security
DIF	Deposit Insurance Fund
DOJ	Department of Justice
ECU	Electronic Crimes Unit
EIDL	Economic Injury Disaster Loan
FBI	Federal Bureau of Investigation
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
NDAA	National Defense Authorization Act for FY 2023
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
OM	Oversight Manager
OMB	Office of Management and Budget
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
SAR	Suspicious Activity Report
SBA	Small Business Administration
SCRM	Supply Chain Risk Management
USAO	United States Attorney's Office
USPIS	U.S. Postal Inspection Service
ViSION	Virtual Supervisory Information on the Net System

Introduction and Overall Results

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

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

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

Overall Results (October 1, 2022–March 31, 2023)	
Audit, Evaluation, and Other Products Issued	**5**
Nonmonetary Recommendations	**56**
Investigations Opened	**45**
Investigations Closed	**37**
Judicial Actions:	
Indictments/Informations	**50**
Convictions	**56**
Arrests	**40**
OIG Investigations Resulted in:	
Special Assessments	**$12,611.00**
Fines	**$30,600.00**
Restitution	**$307,124,816.14**
Asset Forfeitures	**$21,633,432.54**
Settlement	**$2,257,132.00**
Total	**$331,058,591.68**
Referrals to the Department of Justice (U.S. Attorney)	**69**
Responses to Requests Under the Freedom of Information/Privacy Act	**11**
Subpoenas Issued	**N/A**

Audits, Evaluations, and Other Reviews

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

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

During the reporting period, our work addressed key areas in information technology, supervision, and contracting. We issued reports on *Security Controls Over the FDIC's Wireless Networks*; *Implementation of the Information Technology Risk Examination (InTREx) Program*; *Security Controls Over Microsoft Windows Active Directory*, and *FDIC Oversight of a Telecommunications Contract*. Importantly, we also issued our report on the Top Management and Performance Challenges at the FDIC.

We note that in addition to planned discretionary work, our Office reviews the failures of FDIC-supervised institutions causing material losses to the Deposit Insurance Fund (DIF) if those occur. The materiality threshold is currently set at $50 million. If the losses are less than the material loss threshold outlined in the Dodd-Frank Wall Street Reform and Consumer Protection Act, 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. During the reporting period, on March 12, 2023, Signature Bank, an FDIC-supervised institution failed, with substantial losses to the DIF. Our Office will be conducting a Material Loss Review of this failure in the near future.

Results of the audits, evaluations, and other reviews completed during the reporting period are summarized below. A listing of ongoing assignments is also presented. Additionally, we discuss several unresolved recommendations from a report issued previously and provide an update on a matter that we have been addressing with the FDIC's Chief Information Officer Organization (CIOO) related to the security of OIG emails.

Audits, Evaluations, and Other Reviews

Security Controls Over the FDIC's Wireless Networks

The term, "Wi-Fi," refers to wireless technology that allows internet enabled devices (laptops, tablets, and smartphones) to connect to wireless access points and communicate through a wireless network. Wi-Fi technology offers benefits to organizations; however, it also introduces security risks to the confidentiality, availability, and integrity of FDIC data and systems because it is not bound by wires or walls. If not properly configured, Wi-Fi technology is susceptible to signal interception and attack.

We conducted a review to determine whether the FDIC has implemented effective security controls to protect its wireless networks.

We found that the FDIC did not comply or partially complied with five practices recommended by the National Institute of Standards and Technology and guidance from the FDIC and other Federal agencies in the following areas:

- Configuration of Wireless Networks: The FDIC did not properly configure its Policy Manager, which enforces security policies for wireless network connectivity. Also, the FDIC's CIOO Wi-Fi Operations Group did not have control or awareness of the set-up and configuration of numerous wireless devices operating in FDIC buildings and facilities.
- Wireless Signal Strength: The FDIC did not have processes to examine and modify the signal strength of wireless devices/networks broadcasting throughout its buildings and leaking outside of FDIC facilities.
- Security Assessments and Authorizations: The FDIC did not maintain a current Authorization to Operate for its wireless network and did not conduct sufficient continuous monitoring testing activities to support the Agency's ongoing authorization of its wireless network.
- Vulnerability Scanning: The FDIC did not include certain wireless infrastructure devices in its vulnerability scans. In addition, the FDIC did not use credentialed scans on wireless infrastructure devices.
- Wireless Policies, Procedures, and Guidance: The FDIC did not maintain policies and procedures addressing key elements of the FDIC's wireless networks, including roles and responsibilities for the CIOO's Wi-Fi Operations Group; procedures for remediating wireless equipment alerts; standards for configuration settings; updates of wireless inventory records; and detection of rogue access points.

As a result, the FDIC faced potential security risks based upon its wireless practices and controls, including unauthorized access to the FDIC networks and insecure wireless devices broadcasting WiFi signals. The FDIC had effective controls related to physical access controls of wireless devices, access control and encryption, monitoring of user internet destinations on its wireless networks, and disabling legacy wireless networks.

We made eight recommendations intended to strengthen the security controls over the FDIC's wireless networks and protect the confidentiality, availability, and integrity of FDIC systems and data. Management concurred with our recommendations. We engaged the professional services firm of TWM Associates, Inc. to conduct the technical aspects of this review.

Implementation of the Information Technology Risk Examination (InTREx) Program

Cyber risks present some of the greatest systemic threats facing the financial services sector – both domestically in the United States, and globally. The FDIC – along with the Federal Reserve Board (FRB) and Office of the Comptroller of the Currency – have all recognized that cybersecurity is a critical challenge facing the banking industry. These threats include ransomware attacks, denial of service, data breaches, phishing, and supply chain vulnerabilities. And they are increasing in both sophistication and frequency. Banks also may suffer cybersecurity incidents through their interconnections with third-party providers that deliver administrative or management services to financial institutions, such as accounting, human resources, and transaction processing.

The FDIC supervises banks to ensure that their operations function in a safe and sound manner, and comply with all laws and regulations. The FDIC examines institutions to assess their financial condition, management practices – as well as the banks' capabilities to identify and address Information Technology (IT) and cyber risks, and to maintain appropriate internal controls.

In June 2016, the FDIC implemented the InTREx program to guide examiners through the IT portion of a safety and soundness examination. We conducted an audit to determine whether the InTREx program effectively assesses and addresses IT and cyber risks at financial institutions.

We found that the FDIC needs to improve its InTREx program to effectively assess and address IT and cyber risks at financial institutions. Specifically, we found the following weaknesses in the program that limit the ability of examiners to assess and address IT and cyber risks at financial institutions:

- The InTREx program is outdated and does 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 has 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 does 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 does 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 is not fully utilizing available data and analytic tools to improve the InTREx program and identify emerging IT risks; and
- The FDIC has not established goals and performance metrics to measure its progress in implementing the InTREx program.

The weaknesses detailed above collectively demonstrated the need for the FDIC to take actions to ensure that its examiners effectively assess and address IT and cyber risks during IT examinations. We made 19 recommendations to address these weaknesses. Five of those 19 recommendations lacked management decisions as of the end of the reporting period. We are continuing to work with FDIC management to reach resolution of these recommendations.

Security Controls Over the Windows Active Directory

It is important for the FDIC to ensure that only individuals with a business need are allowed access to its many systems that contain sensitive information. 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.

We performed 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.

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 FDIC needed to improve controls in the following areas:

- *Password Management:* We identified weaknesses in how the FDIC managed passwords and password changes. In addition, multiple privileged users (a) reused their passwords; (b) shared their passwords across multiple accounts; and (c) did not change their passwords for over a year.
- *Account Configuration:* Privileged accounts were configured with excessive privileges. Such privileges were not justified as necessary and could allow attackers to inflict significant damage if these accounts were compromised.
- *Access Management:* The FDIC account deletion setting did not remove over 900 users after they exceeded the required thresholds related to account inactivity. In addition, the FDIC suspended its automated account inactivity setting for a month in late 2021 without compensating controls.
- *Privileged Account Management:* Three FDIC users held privileged access for almost a year after the access was no longer required for their positions.
- *Windows Operating System Maintenance:* Several servers and a workstation were running unsupported versions of the Windows or Windows Server Operating System.
- *AD Policies and Procedures:* The AD Operations Manual included inaccurate information about the FDIC's implementation of AD.
- *Audit Logging and Monitoring:* The FDIC did not enable performance monitoring on two domain controllers supporting its AD infrastructure.

The FDIC's ineffective AD security controls could pose significant risks to FDIC data and systems. In addition, the cumulative impact of these weaknesses could result in an attacker covertly obtaining administrative privileges to the FDIC's AD, potentially allowing the attacker to obtain, manipulate, or delete data across the network, causing serious damage to the FDIC and its mission and reputation. Moreover, account misconfigurations by the FDIC may provide FDIC employees and contractors unnecessary elevated privileges on the FDIC's network.

We found that the FDIC had effective controls in the remaining five control areas we assessed related to configuration management, contingency planning, patch management, vulnerability remediation, and defining key AD points of contact.

We made 15 recommendations to address the AD security control weaknesses in the 7 areas listed above. The FDIC concurred with all recommendations.

The FDIC's Oversight of a Telecommunications Contract

The FDIC procures goods and services from contractors in support of its mission. The FDIC Division of Administration awarded 2,633 contracts valued at $2.85 billion over the 5-year period 2017-2021, averaging $570 million annually. Of this amount, the FDIC CIOO contracted for goods and services totaling $1.5 billion, which represented 53 percent of FDIC contract funds awarded over this period.

The FDIC needs a strong culture of compliance and internal controls related to acquisition and procurement. These internal controls must include comprehensive acquisition policies and procedures, supervisory processes that promote compliance, and effective contract oversight management. Absent strong internal controls, the FDIC faces increased operational, monetary, legal, and reputational risks.

Over the past 6 years, since 2017, the FDIC OIG has identified Contract Management as a Top Management and Performance Challenge facing the FDIC. Additionally, the OIG issued two reports in October 2019 and March 2021 identifying that the FDIC needed to strengthen its contract oversight management and monitoring activities. Further, in both 2021 and 2022, the Government Accountability Office concluded, in its financial statements audit of the FDIC, that the FDIC had significant internal control deficiencies within its contract oversight and invoice review and payment processes.

In February 2014, the FDIC awarded a telecommunications service contract to AT&T Corp. (AT&T) in the amount of $12 million. The contract had a base period of 1 year, and four 1-year option periods, potentially resulting in a 5-year contract if all option years were exercised. However, the FDIC did not exercise the option years and allowed the contractor to continue to perform despite the fact that the base year period of performance ended in February 2015. On February 4, 2019, the FDIC modified the contract to extend the period of performance to February 2020 and increase the contract value to $13.2 million. On October 28, 2019, the FDIC again modified the contract to extend the period of performance to June 2022 and to increase the contract value to $18.3 million.

In May 2019, the FDIC CIOO approved a strategy to upgrade the bandwidth of AT&T's telecommunication services within the FDIC Field Offices. Although the contract provided the FDIC the option to upgrade its services, enacting this option required the FDIC and AT&T to process a formal contract modification. In March 2021, the FDIC CIOO notified the OIG of major internal control failures with the AT&T telecommunications contract and that:

- The FDIC had not completed a contract modification for the FDIC Field Office upgrades;
- The FDIC contract had already reached its funded ceiling; and
- The FDIC owed AT&T $2.2 million for unpaid invoices at that time.

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 found 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 personnel failed to fulfill their roles and responsibilities with regard to the AT&T contract.

As a result, the FDIC was subject to an unauthorized contractual commitment that cost the FDIC $4.2 million and a prolonged increase in operational, monetary, legal, and reputational risks. Further, we found that the FDIC incurred costs above the market price for similar services in the amount of at least $1.5 million. We included the $1.5 million in a recommendation that Funds Be Put to Better Use, and we are reporting this amount in this Semiannual Report to the Congress.

We made 14 recommendations to the FDIC, the Chief Information Officer, and the Chief Financial Officer. The recommendations included incorporating improvements into the FDIC CIOO's organizational culture, internal control environment, and internal controls; identifying the extent and significance of the FDIC CIOO's risk related to its procurement activities; and assessing whether management action related to employee or contractor performance or conduct is needed based on the facts presented in the report. The FDIC concurred with all recommendations.

Top Management and Performance Challenges Facing the FDIC

The FDIC plays a unique role in support of the U.S. financial system. At the time we issued our Top Management and Performance Challenges report in February 2023, the FDIC insured nearly $10 trillion in deposits at more than 4,700 banks, supervised over 3,200 banks, oversaw the $125 billion DIF that protects bank depositor accounts, and resolved failing banks. The readiness of the FDIC to execute all facets of its mission promotes confidence and stability in the Nation's financial system.

Our report noted that banks are facing a rising interest rate environment while the U.S. economy faces inflationary pressure and continued uncertainties remain resulting from Russia's invasion of Ukraine. Banks have also adopted new technologies and third-party partnerships to engage customers at a time of increasing cyber security breaches. Banks are also entering into markets for digital assets, which may increase money laundering and terrorist financing risks. The FDIC's operating environment is also changing. The FDIC moved to a hybrid working environment and faces increased retirements and resignations among FDIC personnel.

In light of these circumstances, our report summarized the most serious challenges facing the FDIC and briefly assessed the Agency's progress to address them, pursuant to the Reports Consolidation Act of 2000 and Office of Management and Budget Circular A-136 (revised August 27, 2020). Our report is 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. To compile this report, we received input and considered comments from the FDIC, and while exercising our independent judgment, we incorporated suggestions where appropriate and fair.

We identified nine Top Challenges facing the FDIC that could impact its capabilities to promote public confidence and financial stability:

Preparing for Crises in the Banking Sector. The FDIC has a unique mission to administer the DIF and insure Americans' bank deposits against losses during crises. The FDIC's effective maintenance of the DIF, supervision of banks, and resolution of failed banks provides financial stability to the United States. The FDIC faces crisis readiness challenges to fully develop its plans to respond to an unfolding crisis, including exercising the orderly liquidation of systemically important entities. Further, FDIC readiness and supervisory activities should take into account climate-related risks. FDIC supervisory processes should also be agile to respond to evolving risks such as fraud in crises-related Government-guaranteed loan programs and the evasion of US-imposed economic and trade sanctions.

Mitigating Cybersecurity Risks at Banks and Third Parties. Cybersecurity has been identified as the most significant threat to the banking sector and the critical infrastructure of the United States. The FDIC faces challenges to ensure that examiners have the skillsets and knowledge to conduct information technology examinations that adequately identify and mitigate cybersecurity risks at banks and their third-party service providers. Further, the FDIC should ensure that it has effective processes for the intake of banks' cybersecurity incident reports and uses these reports to mitigate identified risks, identify trends and patterns of nefarious activity, and adjust supervisory processes. Mitigating cybersecurity risk is critical, as a cyber incident at one bank or third-party service provider has the potential to cause contagion within the financial sector.

Supervising Risks Posed by Digital Assets. About 52 million Americans have invested in digital assets. According to FDIC data, as of January 2023, the FDIC was aware that 136 insured banks had ongoing or planned crypto asset activities. The FDIC should work with other regulators to provided clarity regarding the regulation of digital assets. The FDIC should also have examiners with appropriate skillsets and examination processes to assess the safety and soundness of banks' digital asset activities and identify consumer risks. Further, the FDIC should ensure that its examinations, policies, and procedures address consumer risks regarding digital assets, including the relationship of deposit insurance and digital assets.

Fostering Financial Inclusion for Underserved Communities. Federal statute mandates that the FDIC study the unbanked market in the United States and identify the primary issues that prevent unbanked individuals from establishing conventional accounts in financial institutions. Converting the information gleaned from the study of unbanked individuals into effective actions that banks can take to increase access to the financial system for unbanked individuals is a challenging endeavor for the FDIC. Further, the FDIC should also ensure that its examiners have the skills, capabilities, and procedures to assess the effect of banks' use of artificial intelligence in decision making. Artificial Intelligence can be beneficial by increasing the speed and reducing the cost of bank operations, but it can also result in biases against individuals when the algorithms or data used for these decisions are flawed.

Fortifying IT Security at the FDIC. The FDIC is custodian of about 1.8 petabytes of sensitive and Personally Identifiable Information relating to failed banks and more than 4,700 insured banks. The FDIC continues to face challenges to ensure that it has strong information security processes to guard against persistent and increasing cyber threats against Federal agencies. Security control weaknesses of FDIC systems limit the effectiveness of FDIC controls, which places the confidentiality, integrity, and availability of FDIC systems and data at risk. The FDIC should have robust personnel security and suitability program and privacy controls to safeguard IT access to sensitive information and guard against insider threats.

Managing Changes in the FDIC Workforce. A total of 21 percent of the FDIC workforce was eligible to retire in 2022, and that figure climbs to 38 percent within 5 years (2027). These retirements may have a significant impact on key Divisions involved in Crises Readiness efforts and for subject matter experts in areas such as consumer compliance and information technology. At the same time, the FDIC is experiencing increased resignations of its examiners-in-training. Absent effective human capital management, the FDIC may lose valuable knowledge and leadership skill sets upon the departure of experienced examiners, managers, and executives. Meeting these challenges is especially important as the FDIC shifts its operations to a hybrid environment.

Improving the FDIC's Collection, Analysis, and Use of Data. Data and information can enhance the FDIC's and its supervised banks' capabilities to mitigate threats to the U.S. financial system. The FDIC faces challenges in receiving and using reliable information. Specifically, the FDIC should establish processes to acquire, analyze, and disseminate threat information from Government partners, databases, and repositories. Such information informs senior FDIC officials and decision-makers, FDIC examiners and Regional personnel, its supervisory program officials, and banks. Further, the FDIC should improve the reliability of its internal data to ensure that the FDIC Board and senior management can confidently use the data to assess program effectiveness.

Strengthening FDIC Contracting and Supply Chain Management. The FDIC awards nearly $600 million in contracts every year. Over a 5-year period, the FDIC awarded more than 2,600 contracts valued at $2.85 billion. The FDIC faces challenges to establish an effective contract management program that ensures the FDIC receives goods and services according to contract terms, price, and timeframes. An effective FDIC procurement program is important because the FDIC relies on contractor services for day-to-day activities and especially during crises. The FDIC should also have programs in place to mitigate security risks associated with the supply chains for contracted goods and services. Weaknesses in contractor-provided software to Government agencies have exposed examples of these supply chain risks. Further, the FDIC should have whistleblower processes and provisions within FDIC contracts to protect contractor personnel who report allegations of contractor violations and gross mismanagement.

Implementing Effective Governance at the FDIC. Effective governance allows FDIC Board members and senior FDIC officials to proactively manage risk, formulate regulatory policy, and provide clear guidance to banks and FDIC Regional Offices. Through these processes, the FDIC can allocate resources, prioritize and improve the flow of risk information to decision makers, and work toward achieving the FDIC's mission. The FDIC should ensure that risks to the FDIC are identified and monitored through an effective Enterprise Risk Management Program. The FDIC should also ensure that OIG-identified program weaknesses are promptly resolved and remediated. FDIC program performance should be measured using outcome measures to assess whether the FDIC is meeting a program's strategic objectives. The FDIC should also clarify its implementation of Executive Branch best practices, ensure the validity of its rulemaking process, and promulgate rules based on rigorous cost benefit analyses.

The FDIC has taken certain concrete and measurable steps to address some of these Challenges, as noted in our Challenges report. We also recognized that there may have been other ongoing plans, inputs, intentions, or future activities that were still under development at the time of our issuance of the report.

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:

- *The FDIC's Examination of Government-Guaranteed Loans.* The objective is to determine the effectiveness of the FDIC's examinations in identifying and addressing undue risks and weak management practices for banks that participate in Government-guaranteed loan programs.
- *Sharing of Threat and Vulnerability Information Phase 2.* The objective is to determine whether the FDIC has implemented effective processes to ensure that financial institutions receive actionable and relevant threat and vulnerability information.
- *The FDIC's Readiness to Execute the Orderly Liquidation Authority.* The objective is to determine whether the FDIC has established key elements to execute the Orderly Liquidation Authority under the Dodd-Frank Wall Street Reform and Consumer Protection Act, including: (1) comprehensive policies and procedures; (2) defined roles and responsibilities; (3) necessary resources and skill sets; (4) regular monitoring of results; and (5) integration with the Agency's crisis readiness and response planning.
- *FSOC's Response to the Executive Order on Climate-Related Financial Risk.* The objective is to determine what actions the Financial Stability Oversight Council (FSOC) has taken, or planned, in response to Executive Order 14030, Climate-Related Financial Risk, as of November 30, 2021, and whether those actions are consistent with the policy, objectives, and directives set forth in the Executive Order.
- *The FDIC's Efforts to Increase Consumer Participation in the Insured Banking System.* The objective is 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.
- *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 Adoption of Cloud Services.* The objective is to determine if the FDIC has an effective strategy and governance processes to manage its cloud computing services.
- *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.

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

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.

Among our findings, we reported that the FDIC had not established the necessary infrastructure to enable dissemination or receipt of classified National Security Information in its Regional Office locations. As of the end of the prior semiannual period, management had not made a management decision on two of the recommendations in the report related to the finding. Specifically, we recommended that the FDIC:

- Establish and implement a means to share classified information with the Regional Offices in a timely manner so that it is actionable. (Recommendation 13)
- Establish a means for Regional Offices to handle classified information once it is shared, including the infrastructure (systems, facilities, and communications) to securely handle, transmit, discuss, store, and dispose of classified information. (Recommendation 14)

In our semiannual report for the period ending September 30, 2022, we reported that these 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. As explained on page 53 of this report, we took that action, and were awaiting the Follow-up Official's final determination on these recommendations as of the end of this current reporting period. We will continue to work with FDIC officials to reach a management decision on these recommendations.

Update on Earlier Issue Raised in FISMA Report October 2021

In our previous semiannual report, we noted that during the course of our 2021 audit under the Federal Information Security Modernization Act of 2014 (FISMA), we learned that the FDIC process for emails included manual review by the FDIC (FDIC employees and/or contractors) of messages flagged by automated tools. We pointed out that this process presented security and privacy risks that FDIC employees and/or contractors could be inadvertently exposed to information that they would otherwise not be permitted to review. In addition, this process presented risks that emails relevant to urgent law enforcement matters would not be received by the OIG in a timely manner, thus presenting security and safety concerns. We noted that on July 11, 2022, we issued a Memorandum to senior FDIC officials expressing our concerns regarding the FDIC's handling of OIG emails. The FDIC's CIOO responded that it intended to implement changes in technical and policy controls and IT infrastructure to mitigate the risks that we identified. We reported that the FDIC OIG was working with FDIC IT personnel to address our concerns.

On February 16, 2023, the CIOO provided our Office with a written plan for modernizing the OIG's email infrastructure. We subsequently met with the CIOO to provide feedback and suggested changes to the plan. Based on the OIG's feedback, the CIOO prepared an updated plan and provided it to the OIG on March 31, 2023. The CIOO communicated that it takes very seriously the security and proper handling of FDIC email. This includes implementing effective processes for ensuring the confidentiality and timely receipt of OIG email from complainants, whistleblowers, and law enforcement partners to meet the OIG's mission and maintain its independence. The revised plan outlines the challenges and the steps that the CIOO intends to take during 2023 and 2024 to modernize the FDIC and OIG email infrastructure. Successful implementation of the planned activities is critical to the independence of the OIG and its operations.

Congressional Engagement

During the reporting period, our Office engaged with Congress on a variety of topics, including providing Congressional staff with summaries of our reports, holding briefings, and receiving correspondence related to recent activity in the banking sector. A brief discussion of these interactions follows:

Cryptocurrency: The FDIC OIG informed former-Senator Toomey, Senator Warren's and Senator Smith's staffs of the OIG's ongoing work related to cryptocurrency.

Top Management and Performance Challenges Facing the FDIC: In February, the FDIC OIG briefed Majority staff of the House Financial Services Committee and Majority staff of the Senate Committee on Banking, Housing, and Urban Affairs on the FDIC OIG's identification of the *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation*. In March, the FDIC OIG briefed Senator Warren's staff on the FDIC OIG's identification of the *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation*.

Congressional Budget Justification: In March, the FDIC OIG briefed Majority staff of the House Appropriations Subcommittee on Financial Services and General Government on the *OIG's Congressional Budget Justification for Fiscal Year 2024*.

Letter from Senator Warren and Representative Jayapal: On February 28, Senator Warren and Representative Jayapal sent a letter to the FDIC Acting Inspector General asking for the FDIC OIG to conduct a broad and meticulous review of financial conflicts of interest at the FDIC and the effectiveness of existing rules and laws to prevent such conflicts.

Letter from Senator Hagerty: On March 16, Senator Hagerty sent a letter to the FDIC Acting Inspector General urging that the FDIC OIG investigate whether the FDIC's Board of Directors and other employees complied with all legal responsibilities and duties, including those set forth in 12 U.S.C. § 1823, with respect to their actions concerning Silicon Valley Bank.

Letter from Representative Waters, Ranking Member of the House Committee on Financial Services: On March 17, Ranking Member Waters sent a letter to the Federal Reserve System, the FDIC (including the Acting IG), and the Securities and Exchange Commission requesting the agencies to fully exercise the maximum extent of their authorities to investigate and use available enforcement tools to hold senior executives and board members at Silicon Valley Bank and Signature Bank fully accountable for any unlawful activity.

Letter from Senator Warren: On March 18, Senator Warren sent the FDIC Acting Inspector General, Treasury Deputy Inspector General, and the Federal Reserve Board Inspector General a letter requesting an investigation of the causes of the bank management and regulatory and supervisory problems that resulted in the failure of Silicon Valley Bank and Signature Bank.

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, cyber crime, 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 50 indictments/informations; 56 convictions; 40 arrests or self-surrenders; and more than $331 million in fines, restitution ordered, and other monetary recoveries. We opened 45 cases and closed 37 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 already 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

The FDIC OIG continues to support efforts of DOJ's *COVID-19 Fraud Enforcement Task Force* as a key interagency partner for the Department of Justice.

The Task Force's goals include harnessing what the Federal law enforcement community has learned about COVID-19-related and other types of fraud from past efforts in order to better deter, detect, and disrupt future fraud wherever it occurs. Additionally, the Department of Justice has created Strike Force teams in key cities including Los Angeles, California; Sacramento, California; Miami, Florida; and Baltimore, Maryland. The FDIC OIG has started to work with the Miami Strike Force on these matters.

The FDIC OIG also continues to work with the Pandemic Response Accountability Committee (PRAC) and on December 1, 2022, we hosted a *Best Practices in Fraud Enforcement* meeting at the Headquarters level while also collaborating with the PRAC at the field level for joint investigations relating to pandemic relief fraud.

Pandemic-Related Financial Crimes

Since many of the programs in the Coronavirus Aid, Relief, and Economic Security (CARES) Act and related legislation are administered through banks and other insured institutions, our Office of Investigations has been actively involved in investigating pandemic-related financial crimes affecting the banks. In addition, our Office has regularly coordinated with the supervisory and resolutions components within the FDIC to watch for patterns of crimes and other trends in light of the pandemic. Our Special Agents have been working proactively with other OIGs; U.S. Attorney's Offices; and other law enforcement agencies on cases involving frauds targeting the $5 trillion in funds distributed through pandemic relief programs. Through these collaborative efforts, we have been able to identify, develop, and lead cases specific to fraud related to stimulus packages. We have played a significant role within the law enforcement community in combating this fraud, and since inception of the CARES Act, have been involved in 190 such cases.

Notably, during the reporting period, the FDIC OIG's efforts related to the Federal Government's COVID-19 pandemic response resulted in 32 indictments and informations; 20 arrests or self-surrenders; and 36 convictions, involving fraud in the CARES Act Programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases totaled in excess of $24.2 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 "Big 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 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.

Rancher Sentenced for Running $244 Million "Ghost Cattle" Scam

Cody Allen Easterday (Easterday) was sentenced to 132 months imprisonment, 3 years of supervised release, and ordered to pay $244,031,132 in restitution in the Eastern District of Washington. Easterday previously pleaded guilty to one count of wire fraud after having orchestrated and carried out a massive, brazen, and long-term "ghost cattle" scheme where he fraudulently billed Tyson Foods and another company more than $244 million dollars for the purchase and feeding of cattle that never existed. Easterday ultimately carried out the fraud in order to cover significant losses sustained in commodity trades through CME Group, Inc. and further used fraud proceeds for his personal use and benefit. The scheme was the largest-ever criminal fraud scheme prosecuted in the Eastern District of Washington.

Easterday is the owner of Easterday Ranches, Easterday Farms, and Easterday Farms Dairy. He used loan advances and accounts held at Rabobank, N.A. (now Mechanics Bank) and Rabo AgriFinance to facilitate and fund market manipulation in Live Cattle and Feeder Cattle commodity futures contracts. CME Group, Inc., the world's largest financial derivatives exchange, was defrauded when Easterday submitted falsified paperwork that resulted in CME exempting Easterday Ranches from otherwise-applicable position limits in live cattle futures contracts. In order to cover approximately $200 million in commodity futures contracts trading losses, Easterday created and submitted false and fraudulent invoices totaling more than $244 million to Tyson Foods and another company between approximately 2016 and November 2020. These false and fraudulent invoices sought and obtained reimbursement from Tyson Foods and the other victim company for the purported costs of purchasing and raising hundreds of thousands of cattle that neither Easterday nor Easterday Ranches ever purchased, and that did not actually exist. The remainder of the $244 million Easterday stole from Tyson and the other victim company was converted to Easterday's personal use and for the benefit of the Easterday farming empire – an empire that, by 2020, included more than 22,000 acres of farmland, 150 employees, revenues of over $250,000,000, and even a private plane and hangar. Easterday's conduct also led Easterday Ranches and Easterday Farms to default on a $45 million loan issued by Washington Trust Bank. It is also alleged that Easterday may have misrepresented his assets to lenders in connection with the purchase of a dairy farm in 2019.

Source: Fraud Section of the Criminal Division of DOJ.
Responsible Agencies: FDIC OIG and United States Postal Inspection Service (USPIS).
Prosecuted by the Fraud Section of the Criminal Division of DOJ and the USAO, Eastern District of Washington.

Former Florida State Representative Pleads Guilty to Wire Fraud, Money Laundering, and Making False Statements in Connection with COVID-19 Relief Fraud

Joseph Harding, a former Florida State Representative, pleaded guilty to wire fraud, money laundering, and making false statements in connection with COVID-19 relief fraud.

Between December 1, 2020, and March 1, 2021, Harding committed wire fraud by participating in a scheme to defraud the Small Business Administration (SBA) and obtaining Coronavirus-related small business loans by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme, causing wire communications to be transmitted in interstate commerce. Harding made and caused to be made false and fraudulent SBA Economic Injury Disaster Loan (EIDL) applications, and made false representations in supporting loan documentation, in the names of dormant business entities, submitted to the SBA. Harding also obtained fraudulently created bank statements for one of the dormant business entities that were used as supporting documentation for one of his fraudulent EIDL applications. By this conduct, Harding obtained and attempted to obtain more than $150,000 in funds from the SBA to which he was not entitled. Harding also engaged in illegal monetary transactions with funds derived from unlawful activity related to his transfer of the fraudulently obtained EIDL proceeds into two bank accounts. After obtaining the EIDL proceeds, Harding conducted monetary transactions involving more than $10,000 in fraudulently obtained funds: a transfer to his joint bank account, a payment to his credit card, and a transfer into a bank account of a third-party business entity.

Source: Referral from the USAO, District of Florida.
Responsible Agencies: FDIC OIG, FBI, IRS-Criminal Investigation (IRS-CI), and SBA OIG.
Prosecuted by the USAO, Northern District of Florida.

North-Central Florida Blimp Company Executive Sentenced to over 5 Years in Federal Prison for COVID-19 Relief Fraud

Patrick Walsh was sentenced after previously pleading guilty to one count of wire fraud and one count of money laundering in connection to COVID-19 pandemic relief. Walsh was sentenced to 66 months in Federal prison.

Between April 7, 2020, and January 21, 2021, Walsh submitted a total of 16 fraudulent applications to multiple Federally-insured financial institutions and other qualified lenders for Paycheck Protection Program (PPP) loans in the names of multiple businesses, including his blimp companies, which were headquartered in Levy County. Walsh's false PPP loan applications included several discrepancies: no record of some employees that were listed in Walsh's applications; the number of employees listed in multiple applications was more than previously listed in employer tax records; and some of the companies claimed in the applications were not even established businesses as of February 15, 2020 (the beginning of the COVID-19 pandemic relief programs). Additional investigation revealed that Walsh had used several of the same employees on PPP loan applications for different companies.

Walsh's fraudulent PPP loan applications sought a total of $11,950,439 in PPP loan funds, of which he received a total of $4,996,167. Further, between March 2020 and July 2020, Walsh submitted 18 fraudulent applications to the SBA for EIDLs in his own name and in the name of his wife. Walsh's false EIDL applications were approved and $2,822,000 was disbursed to him.

Additionally, Walsh engaged in multiple monetary transactions that involved at least $10,000 of fraudulently obtained PPP loan or EIDL proceeds that he obtained through his wire fraud scheme. Many of these transactions included payments for the purchase of real estate in Florida and Texas, oil leases, and to pay off his mortgage loans.

Walsh's imprisonment will be followed by 3 years of supervised release. Additionally, Walsh was ordered to pay restitution to the SBA in the amount of $7,818,167, and the Court entered an order of forfeiture in the same amount.

Source: Referral from the USAO, Northern District of Florida.
Responsible Agencies: FDIC OIG, FBI, IRS-CI, and SBA OIG.
Prosecuted by the USAO, Northern District of Florida.

Former Bank President and CEO Found Guilty of Fraud Resulting in the Failure of First NBC Bank

Former First NBC Bank President and Chief Executive Officer (CEO) Ashton J. Ryan, Jr. was convicted at trial by a Federal jury on 46 counts of bank fraud, conspiracy, and false bank entries.

From 2006 through April 2017, Ryan and others conspired to defraud First NBC Bank through a variety of schemes. Ryan was the President and CEO of the Bank for most of its existence. Ryan and others conspired to defraud First NBC Bank by disguising the true financial status of certain borrowers and their troubled loans, concealing the true financial condition of the Bank from the Board of Directors, auditors, and examiners.

When members of the Board or the Bank's outside auditors or examiners asked about loans to these borrowers, Ryan and others made false statements about the borrowers and their loans, omitting the truth about the borrowers' inability to pay their debts without getting new loans. As a result, the balance on these borrowers' loans continued to grow resulting, ultimately, in the failure of First NBC. The Bank's failure cost the FDIC's Deposit Insurance Fund slightly under $1 billion.

Source: This investigation was initiated from a complaint received by the FDIC.
Responsible Agencies: FDIC OIG, FBI, and FRB OIG.
Prosecuted by the USAO, Eastern District of Louisiana.

Former Bank Employee Convicted After Trial for Fraudulently Opening Bank Accounts

Diape Seck, of Rockville, Maryland, was convicted at trial for his role in a bank fraud scheme in which he and his co-conspirators obtained or attempted to obtain almost $2 million by fraud, including by stealing checks from the mail of churches and religious institutions.

From at least January 2019 to January 2020, Seck, a TD Bank employee, conspired with Mateus Vaduva, Marius Vaduva, Vlad Baceanu, Nicolae Gindac, Florin Vaduva, Marian Unguru, Daniel Velcu, Vali Unguru, and others to commit bank fraud. Specifically, the evidence showed that Seck fraudulently opened bank accounts in fake identities in exchange for cash bribes. Co-conspirators engaged in fraud involving rental cars and the deposit of checks stolen from the incoming and outgoing mail of churches and other religious institutions into the fraudulently opened bank accounts. The co-conspirators then withdrew the funds and spent the fraudulently obtained proceeds.

Diape Seck facilitated the opening of hundreds of bank accounts for his co-conspirators, who used purported foreign identity documents, often but not universally Romanian, to fraudulently open bank accounts with him, as well as bank accounts at other victim financial institutions. Seck opened accounts for co-conspirators without their presence in the bank, without verifying identity information, and opened accounts for co-conspirators who opened multiple accounts at a time under different identities. To conceal his improper activities, Seck opened accounts for the co-conspirators at the same time he conducted legitimate bank activities. The co-conspirators paid Seck cash in exchange for him opening the fraudulent bank accounts.

Seck violated numerous bank policies in opening approximately 412 checking accounts in a 1-year period from approximately January 2, 2019 through January 3, 2020, relying predominantly on purported Romanian passports and driver's license information. Checks payable to and written from churches and other religious institutions from around the country were deposited into many of the 412 checking accounts, which were not opened in the names of the churches.

The co-conspirators fraudulently negotiated the stolen checks by depositing them into the victim bank accounts, including the fraudulent accounts opened by Seck at Bank A, often by way of automated teller machine (ATM) transactions. After depositing the stolen checks into the bank accounts, the conspirators made cash withdrawals from ATMs and purchases using debit cards associated with the bank accounts.

Co-conspirators Vlad Baceanu, Daniel Velcu, Marian Ungur, and Vali Unguru, all of Baltimore, Maryland, previously pleaded guilty to conspiracy to commit bank fraud and wire fraud. Nicolae Gindac, of Dania Beach, Florida, was sentenced to 54 months in Federal prison and ordered to pay restitution of $1,096,660.11; Mateus Vaduva, of Baltimore was sentenced to 5 years in Federal prison and ordered to pay restitution of $1,320,885.84; Florin Vaduva, of Dania Beach, Florida, was sentenced to 51 months in Federal prison and ordered to pay restitution of $1,096,660.11; and Marius Vaduva, of Baltimore was sentenced to 42 months in Federal prison and ordered to pay restitution of $1,334,230.84, after they previously pleaded guilty to conspiracy to commit bank and wire fraud.

Source: USPIS.
Responsible Agencies: FDIC OIG, USPIS, Homeland Security Investigations (HSI), Montgomery County (MD) Police Department, Cary (NC) Police Department and Williamson County (TN) Sheriff's Office.
Prosecuted by the USAO, Maryland.

Hilo Man Receives 42 Months in Prison for Defrauding COVID-19 Relief Programs

Carey Mills, of Hilo, Hawaii, was sentenced to 42 months in Federal prison for wire fraud in connection with a scheme to defraud the Federal government of program funds intended for COVID-19-related relief. Mills pleaded guilty to a single-count information on May 17, 2022. In addition to a term of imprisonment, the Court also imposed a 5-year term of supervised release and ordered Mills to pay restitution to the SBA in the amount of $937,575.

From May to August 2020, Mills submitted multiple applications for PPP and EIDL funds on behalf of three businesses under his control, Kanaka Maoli Hookupu Center, New Way Horizon Travel, and Uilani Kawailehua Foundation, each time utilizing interstate wires. To support the applications, Mills submitted fraudulent payroll documents and IRS forms, which included false employee and wage payment records. As a result of these applications, Mills received $937,575 in the form of three forgivable PPP loans and one EIDL grant to which he was not entitled.

Mills used the Federal relief money to fund personal expenses, including the purchase of eight vehicles and two residential properties. The Mills case was the first COVID-19 program fraud sentencing in the District of Hawaii.

Source: This investigation was initiated from a referral from the USAO-Hawaii and U.S. Treasury Inspector General for Tax Administration (TIGTA).
Responsible Agencies: FDIC OIG, TIGTA, SBA OIG, and HSI.
Prosecuted by the USAO, Hawaii.

Former Wells Fargo Executive Agrees to Plead Guilty to Obstructing a Bank Examination Involving the Opening of Millions of Accounts Without Customer Authorization

Carrie L. Tolstedt, the former head of Wells Fargo Bank's retail banking division, agreed to plead guilty to obstructing a government examination into the bank's widespread sales practices misconduct, which included opening millions of unauthorized accounts and other products.

The Office of the Comptroller of the Currency (OCC), which investigated misconduct at Wells Fargo, also has reached a resolution with Tolstedt in a regulatory proceeding. As part of the consent order resolving that matter, Tolstedt agreed to a ban from working in the banking industry and to pay a $17 million civil penalty.

From approximately 2007 to September 2016, Tolstedt was Wells Fargo's senior executive vice president of community banking and was head of the Community Bank, which operated Well Fargo's consumer and small business retail banking business. The Community Bank managed many of the products that Wells Fargo sold to individual customers and small businesses, including checking and savings accounts, CDs, debit cards, bill pay, and other products.

Wells Fargo previously admitted that, from 2002 to 2016, excessive sales goals led Community Bank employees to open millions of accounts and other financial products that were unauthorized or fraudulent. In the process, Wells Fargo collected millions of dollars in fees and interest to which it was not entitled, harmed customers' credit ratings, and unlawfully misused customers' sensitive personal information.

Many of these practices were referred to within Wells Fargo as "gaming." Gaming strategies included using existing customers' identities – without their consent – to open accounts. Gaming practices included forging customer signatures to open accounts without authorization, creating PINs to activate unauthorized debit cards, and moving money from millions of customer accounts to unauthorized accounts in a practice known internally as "simulated funding."

Gaming also included opening credit cards and bill pay products without authorization, altering customers' contact information to prevent customers from learning of unauthorized accounts and to prevent Wells Fargo employees from reaching customers to conduct customer satisfaction surveys, and encouraging customers to open accounts they neither wanted nor needed.

According to the plea agreement, Tolstedt was aware of sales practices misconduct within the Community Bank and the fact that employees were terminated each year for gaming. By no later than 2006, Tolstedt was learning about the gaming practices from corporate investigations and, over time, learned that terminations for gaming in the Community Bank were steadily increasing, that the misconduct was linked in part to sales goals within the Community Bank, and that termination numbers likely underestimated the scope of the problem.

Although the Community Bank eventually took steps purportedly designed to proactively identify sales misconduct, the measures used by the bank flagged only a small portion of the potentially problematic activity for investigation. As of July 2014, only the most egregious .01 to .05 percent of employees engaging in activity considered a "red flag" for sales practices misconduct were investigated – with the remaining 99.95 to 99.99 percent left unexamined under this process.

In May 2015, Tolstedt participated in the preparation of a memorandum, which she knew would be provided to the OCC in connection with its examination of sales practice issues at Wells Fargo. To minimize the scope of the sales practices misconduct within the Community Bank, Tolstedt corruptly obstructed the OCC's examination by failing to disclose statistics on the number of employees who were terminated or resigned pending investigation for sales practices misconduct. She also failed to disclose that the Community Bank proactively investigated only a very small percentage of employees who engaged in activity flagged as potential sales practices misconduct.

Wells Fargo in 2020 acknowledged the widespread sales practices misconduct within the Community Bank and paid a $3 billion penalty in connection with agreements reached with the United States Attorneys' Offices for the Central District of California and the Western District of North Carolina, the Justice Department's Civil Division, and the Securities and Exchange Commission.

Responsible Agencies: FDIC OIG, FBI, Federal Housing Finance Agency OIG, FRB OIG, and the USPIS. The Office of the Comptroller of the Currency and the Securities and Exchange Commission provided additional investigative assistance.
Prosecuted by the USAO, Central District of California; USAO, Western District of North Carolina; and Major Frauds Section, DOJ.

Two Individuals Sentenced for Multimillion-Dollar Cattle-Trading Ponzi Scheme

Reva Joyce Stachniw and Ron Throgmartin were sentenced to 6 years in prison for their roles in a cattle-trading Ponzi scheme that resulted in millions of dollars in victim losses.

From late 2017 until early 2019, Reva Joyce Stachniw, of Galesburg, Illinois, and Ron Throgmartin, of Buford, Georgia, along with a co-conspirator, ran a Ponzi scheme by fraudulently representing to victims that their investments were backed by short-term investments in Stachniw and Throgmartin's cattle and marijuana businesses. The victim-investors gave the conspirators money based on false promises that their investments would be used for legitimate activities related to those businesses. In actuality, the funds were used to pay earlier investors.

In August 2022, Stachniw and Throgmartin were convicted at trial of one count of conspiracy to commit wire fraud, five counts of wire fraud, and one count of conspiracy to commit money laundering. In addition to their terms of imprisonment, Stachniw was ordered to pay $14,597,335.80 in restitution and to forfeit $6,013,370. Throgmartin was ordered to pay $14,597,335.80 in restitution and to forfeit $1,004,904.83. The restitution was ordered jointly and severally between the two.

Source: This investigation was predicated on a request from the USAO, Central District of Illinois.
Responsible Agencies: FDIC OIG and the FBI.
Prosecuted by the Fraud Section, DOJ.

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 over 63 judicial districts in 39 locations in the U.S.:

Arizona	Louisiana	North Carolina
Arkansas	Maryland	North Dakota
California	Massachusetts	Ohio
Colorado	Michigan	Oklahoma
District of Columbia	Minnesota	Pennsylvania
Florida	Mississippi	Rhode Island
Georgia	Missouri	South Carolina
Hawaii	Nebraska	South Dakota
Illinois	Nevada	Tennessee
Indiana	New Hampshire	Texas
Iowa	New Jersey	Virginia
Kansas	New Mexico	West Virginia
Kentucky	New York	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, 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 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.
- Reached out to the FDIC's newest Board Members, Vice Chairman Travis Hill and Director Jonathan McKernan following their appointment to the Board on January 5, 2023, to offer information about the mission, role, and work of the OIG at the FDIC.
- Coordinated with the former and current Chairmen 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.
- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
- 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.

- Added language to our publicly issued products in keeping with the National Defense Authorization Act (NDAA), advising relevant stakeholders that pursuant to Pub. L. 117-263, section 5274, non-governmental organizations and business entities identified in our OIG reports have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to comments@fdicoig.gov within 30 days of the report publication date as reflected on our OIG website. Any comments will be appended to the report and posted on our website. Submissions must be Section 508 compliant and free from any proprietary or otherwise sensitive information.
- Helped organize and actively participated in the FDIC and DOJ Financial Crimes Conference. Former IG Lerner delivered Keynote Remarks, focusing on our high-impact cases, our skilled Special Agents throughout the country, our law enforcement partnerships, the span of our investigations, the capabilities of our Electronic Crimes Unit, and our data analytics efforts. Other OIG Special Agents presented case studies of three successful financial 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. (See earlier section of this report entitled Congressional Engagement.)
- 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, IMS, 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 214 Hotline inquiries, 10 of which led to our opening investigations.

- Supported OIG staff conducting outreach to various audiences and stakeholders. For example, two OIG Special Agents Presented on Government Guaranteed Loan Fraud at the 2022 FDIC Accounting and Auditing Conference focusing on the case of United States vs. Banc-Serv Partners, LLP; one of our Audit Managers presented at CIGIE's 9th Annual Leadership Forum on the topic: "Reasonable Minds Can Disagree;" another Audit Manager presented on *Communications with the Auditee* during CIGIE's Connect, Collaborate, and Learn event; we briefed CIGIE's Audit Committee and Inspection and Evaluation Committee on the results of the Monetary Impact Working Group; and an Audit Manager and Special Agent from the ECU presented at CIGIE's Cybersecurity Working Group event on the topic of *Digital Assets: Legitimate Uses in the Traditional Financial System in Contrast to Nefarious Activities*.
- Attended the San Francisco Region Bank and Money Laundering Training Session for prosecutors, agents, and other law enforcement partners in Los Angeles, CA. The OIG's San Francisco Special Agent in Charge participated in a panel discussion to highlight the mission, priorities, and capabilities of the FDIC OIG Office of Investigations.
- Participated in the PRAC's Agile Oversight Forum. The forum focused on the strategies and approaches of agile oversight and how watchdogs can incorporate them into their work to provide relevant stakeholders with critical information more quickly. One of our OIG Audit Managers participated on a panel that discussed how Agile Products and Professional Standards Increase Innovation, Collaboration, and Opportunities. Other members of our Office of Audits, Evaluations, and Cyber helped research and identify forum topics.
- Hosted representatives from the PRAC, more than a dozen federal law enforcement agencies, and the DOJ at a meeting to discuss best practices in pandemic fraud enforcement. The discussions focused on challenges identified through the pandemic, fraud control recommendations, legislative proposals, data-sharing successes and challenges, and how to successfully position the law enforcement community to address future fraud challenges.
- Supported the IG community by attending monthly Council of the Inspectors General on Integrity and Efficiency (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.
- Hosted CIGIE's Quarterly Deputy Inspector General hybrid meeting. The former FDIC IG provided opening remarks during the meeting and the Deputy AIGI gave a presentation on the FDIC OIG's implementation of body-worn cameras. Other topics discussed included the Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, and presentations on DEIA.

- Shared information on CIGIE's DEIA efforts with the Federal News Network. During the interview, former IG Lerner and the Department of Education IG highlighted the issuance of the *Compendium of Office of Inspector General Reports Related to Diversity, Equity, Inclusion, and Accessibility*, and CIGIE's *Advancing Diversity, Equity, Inclusion, and Accessibility*: A Roadmap for Offices of Inspectors General.
- Supported efforts of the PRAC through active participation in its meetings, forums, and work groups and by playing a key role in collaboration with law enforcement partners in investigations of fraud in pandemic-relief programs. Also continued to adopt features of the PRAC's Agile Product Toolkit to provide our stakeholders a means of receiving more expedient information on results of oversight efforts, for example to convey emerging concerns identified during audits and evaluations.
- Participated on the Council of Inspectors General on Financial Oversight (CIGFO), as established by the Dodd-Frank Wall Street Reform and Consumer Protection Act, and coordinated with the IGs on that Council. This Council facilitates sharing of information among CIGFO member Inspectors General and discusses ongoing work of each member IG as it relates to the broader financial sector and ways to improve financial oversight. Formed part of the CIGFO team examining *FSOC's Response to the Executive Order on Climate-Related Financial Risk*.
- Joined IG community colleagues in warning consumers on *Slam the Scam Day* and re-issued an alert to inform the public about two types of impersonation scams: one purporting to be from the FDIC and the other from FDIC OIG personnel. The Alert also discussed tactics that scammers use in order to make their demands for funds appear to look legitimate, as well as information for contacting the FDIC OIG Hotline.
- Communicated with the Government Accountability Office on ongoing efforts related to our 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.
- Promoted transparency to keep the American public informed through three 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; Twitter communications to immediately disseminate news of report and press release issuances and other news of note; 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 including 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.
- Held two 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 briefing by our IT staff to discuss a variety of IT updates, including mobile device changes; upcoming data retention changes; and moving from SharePoint to Microsoft Teams to Team Channels.
- Made substantial 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 Office of Information Technology's 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. Shared updates on progress of the plan with OIG staff and kept them fully apprised of steps they needed to take to ensure the ongoing security of OIG information systems, data, equipment, and electronic devices.
- Launched our 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. The system ensures that the OIG 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. Going forward, our focus will be 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 to 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.

- Published *In the Know*—a bulletin for staff containing information to keep connected with the workforce and update all staff on happenings affecting their daily work in such areas as administrative and policy guidance, human resource matters, IT system updates, DEIA offerings, and professional development and training opportunities.

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

- Continued to review and update a number of OIG internal policies related to audit, evaluation, investigation, operations, and administrative processes of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the Office. For example, revised the OIG's *Travel and Relocation* policy to clarify certain practices, and issued two new policies: *Confidentiality and Disclosure* policy and *Review of Allegations, Discipline, and Adverse Actions Involving OIG Employees*.

- 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 the AIG for Management; Deputy AIGI; Senior Financial Management Analyst; Special Agents; and Auditors/Evaluators.
- 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.
- Held information session to inform OIG staff of the OIG's Emergency Preparedness and Continuity of Operations Programs.

Exercising leadership skills and promoting teamwork.

- Held two OIG-wide Town Hall Meetings for FDIC OIG leadership to discuss the state of the Office, OIG initiatives for the future, and the transition of leadership of the OIG to the Acting IG, following former IG Jay Lerner's retirement on January 27, 2023.
- Conducted "New Agent Training" for OI Special Agents who joined the Office. Presentations included case studies; legal topics; Audits, Evaluations, and Cyber overview; FDIC overview; and other law enforcement-related topics.
- Implemented features of the OIG's DEIA Strategic Plan, consisting of four components: *Purpose*: ways in which we strive to inspire each OIG team member to feel connected to our OIG Mission and Vision. This is accomplished through maintaining a diverse workforce in which all are engaged and can bring their authentic selves to the workplace in an environment of safety and acceptance and contribute to the success of the Office. *People*: in order to create a space of belonging in which we foster trusting relationships, invite opinions, and engage in relationship building, recognizing that our accomplishments are not possible without the hard work and dedication of the OIG team. *Processes*: to ensure that we uphold the OIG principles in our recruitment, hiring, promotion, recognition, awards, training, developmental opportunities, operations, procedures, workflows, policies, and technology. *Progress*: to hold ourselves accountable to these strategic goals, we will monitor progress as we mature our DEIA program.
- Held OIG senior leadership coordination meetings to affirm the OIG's unified commitment to the FDIC OIG mission and to strengthen working relationships and collaboration among all FDIC OIG offices.

- Participated in an interview with the CIGIE Professional Development Committee as part of its new spotlight series on leaders in the IG community. In the interview, former IG Lerner discussed and reflected on his career journey and leadership lessons.
- Organized and led the development of a training program for attorneys new to the OIG community. This effort by one of the FDIC OIG's attorneys was recognized by the Council of Counsels to the Inspectors General with a 2022 Outstanding Service Award.
- Supported efforts of the Workforce Council as that group added its new members. The mission of this Council is to foster and support a workplace that engages employees, builds trust, and identifies improvements and best practices for the OIG. The goal of the Council is to facilitate an engaged workplace culture by providing a mechanism where OIG employees can share input and have their input fairly considered, addressed, and become part of constructive solutions.
- 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 issuance of OIG *Connection* newsletters, an *In the Know* publication, and other communications.
- Enrolled OIG staff in several different FDIC, CIGIE, and other Leadership Development Programs to enhance their leadership capabilities.
- Participated in a panel during CIGIE's DEIA Shop Talk: *Women in Federal Law Enforcement*. The former Special Agent in Charge of our Chicago Office was part of the panel of 14 female leaders in Federal law enforcement who explained challenges they have overcome in their rise to leadership roles.
- Held the OIG's Annual Distinguished Achievement Awards Ceremony to recognize OIG staff in seven award categories: Inspector General Awards for Leadership, Innovation, Business Support, Championing Diversity and Inclusiveness, Collaboration, New Staff Member, and IG Awards for Excellence. Also administered the OIG's ongoing awards and recognition program for staff across all component offices to acknowledge their individual and team contributions to the Office throughout the year.
- Organized several activities, including component-specific and OIG-wide 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 Audits, Evaluations, and Cyber and an Audit/Evaluation Manager led a group comprised of representatives from 20 OIGs across the community. The purpose of the group is to assess and help ensure consistency in how OIGs report and track monetary impacts from audits and evaluations. Shared results with others in the IG community.

- Continued to support members of the OIG pursuing professional training, banking schools, and certifications to enhance the OIG staff members' expertise and knowledge.

- 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; arranged training from the NeuroLeadership Institute and Arbinger Group; 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 DEIA Working Group. Hosted a series of events to highlight diversity, including Diversity in Employment Awareness Month, National Native American Heritage Month, Veterans Day observance, January event to commemorate the life and legacy of Dr. Martin Luther King, Jr., two programs to commemorate Black History Month, and an event honoring Women's History Month.

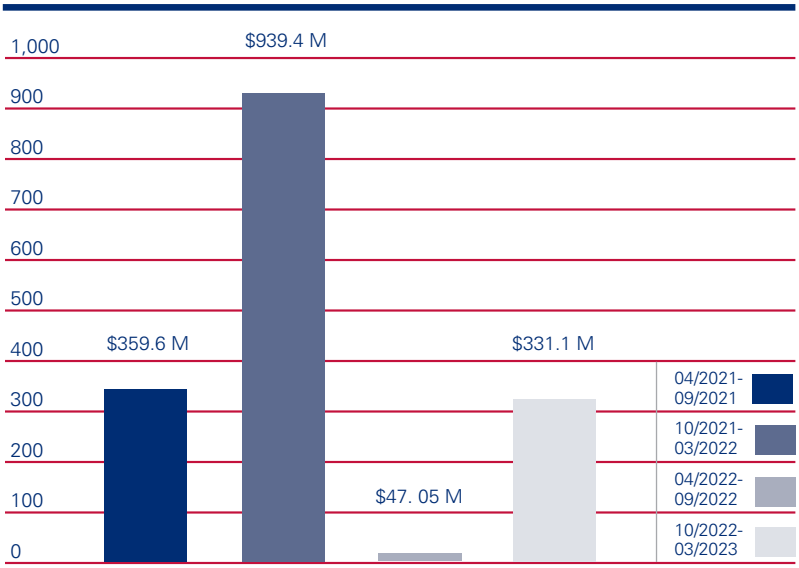
- Continued involvement in CIGIE's DEIA Committee, of which the former FDIC IG was Vice Chair. Supported issuance of *The Ally* Newsletter to share information from the Committee, which works to affirm, advance, and augment CIGIE's commitment to promote a diverse, equitable, and inclusive workforce and workplace environment throughout the IG Community.

- Led efforts of the PRAC's Law Enforcement Coordination Subcommittee. Our AIG for Investigations is Chair of this group. 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.

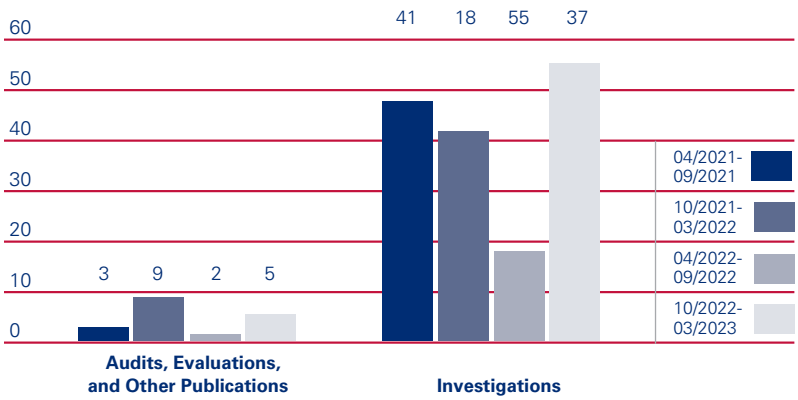
Cumulative Results (2-year period)

Nonmonetary Recommendations	
April 2021 – September 2021	12
October 2021 – March 2022	77
April 2022 – September 2022	1
October 2022 – March 2023	56

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.	5-9
Section 5(a)(2): An identification of each recommendation made before the reporting period, for which corrective action has not been completed, including the potential costs savings associated with the recommendation.	44-51
Section 5(a)(3): A summary of significant investigations closed during the reporting period.	20-27
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.	52
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.	53
Section 5(a)(7): The information described under section 804(b) of the Federal Financial Management Improvement Act of 1996.	54
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.	56-57

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.	56-57
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.	56-57
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.	54
Section 5(a)(12): A description of metrics used for Section 5(a)(11) information.	54
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.	54
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.	54
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.	54
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.	54

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. Former FDIC IG Lerner served as Vice Chair of the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Legislation Committee until his retirement in January 2023. Much of the FDIC OIG's activity considering and reviewing legislation and regulation occurs in connection with that Committee.

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 FDIC OIG took steps, in keeping with Section 5274 of the National Defense Authorization Act (NDAA) for FY 2023, to notify non-governmental organizations and business entities identified in our OIG reports that they have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Additionally, along with OIG colleagues across the government, we monitored changes in Semiannual Reporting requirements, as indicated in Section 5273 of the NDAA, which amended the IG Act, and we modified our reporting of required information in this semiannual report accordingly.

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 (OMs) 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
AUD-21-003 **Security of Critical Building Services at FDIC-owned Facilities** March 29, 2021	The FDIC relies heavily on critical building services to perform its mission-essential business functions and ensure the health and safety of its employees, contractors, and visitors. Critical building services include electrical power; heating, ventilation, and air conditioning (HVAC); and water. We conducted an audit to determine whether the FDIC had effective controls and practices to protect electrical power, HVAC, and water services at its Virginia Square facility. The audit also assessed compliance with key security provisions in the FDIC's Facilities Management Contract. We found that the FDIC did not subject the three information systems we reviewed to the National Institute of Standards and Technology's Risk Management Framework as required by Office of Management and Budget policy. The FDIC also did not maintain signed Confidentiality Agreements for EMCOR and its subcontractor personnel working at the Virginia Square facility. In addition, the FDIC did not ensure that all EMCOR and its subcontractor personnel had completed required information security and insider threat training. The report contained 10 recommendations intended to strengthen the FDIC's controls and practices to protect critical building services.	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
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	12	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AEC-21-002 **The FDIC's Management of Employee Talent** September 1, 2021	The FDIC OIG conducted an evaluation of the FDIC's allocation and retention of its examination staff. Our objectives were to determine whether (1) the FDIC's activities for retaining safety and soundness examination staff and subject-matter experts were consistent with relevant OIG-identified criteria and (2) the FDIC's process for allocating examination staff and subject matter experts to safety and soundness examinations was consistent with relevant OIG-identified criteria. We found that the FDIC's activities for retaining safety and soundness examination staff and subject matter experts and its process for allocating such resources were consistent with relevant criteria, and thus we concluded our evaluation. In conducting our evaluation, however, we identified broader concerns regarding the FDIC's overall management of employee talent, and this Memorandum advised the FDIC of our concerns in this area. While the FDIC employs certain talent management activities, the FDIC's retention management strategy did not have clearly defined goals, a process for collecting and analyzing data, and a process for measuring the effectiveness of its retention activities. The report contained three recommendations to improve the FDIC's management of employee talent and for the FDIC to measure the effectiveness of its retention efforts and activities.	3	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-22-001 **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 (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. Ratings are determined by a simple majority where the most frequent level (mode) across the component questions will 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	3	NA
EVAL-22-001 **Reliability of Data in the FDIC Virtual Supervisory Information on the Net System** November 22, 2021	The FDIC maintains the Virtual Supervisory Information on the Net (ViSION) system, which supports FDIC supervision and insurance responsibilities. We conducted an evaluation to determine whether key supervisory information in the ViSION system was reliable, which was defined as accurate, complete, and supported by source documentation retained in the FDIC system of record. Among the four key ViSION system data elements tested, we found that two were not reliable. Specifically, we found an error for the Completion Date for 14 banks and an error for the Mail Date for 12 banks. We determined that the unreliable data resulted from weaknesses in the FDIC's procedures and practices for identifying and ensuring the quality of the ViSION system Completion Date and Mail Date data elements. We did not find errors for the Examination Ratings and Start Date data elements. We also found that the FDIC's risk-based assessment of ViSION system data was undocumented and outdated. The report contained six recommendations intended to strengthen the reliability of data in the FDIC ViSION system.	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	
EVAL-22-002 **Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders** December 1, 2021	The Bank Secrecy Act (BSA), and subsequent laws and regulations, established anti-money laundering (AML) recordkeeping and reporting requirements for financial institutions. When a financial institution is not in compliance with BSA/AML requirements, the FDIC may issue a Consent Order. We conducted an evaluation to determine whether the FDIC (i) considered factors similar to other Federal bank regulators in terminating BSA/AML Consent Orders; (ii) terminated BSA/AML Consent Orders in accordance with FDIC-established guidance; (iii) monitored FDIC Regional Office termination decision-making to ensure consistency across the Regions; and (iv) documented its actions. We found that the factors considered by the FDIC to terminate Consent Orders differed from the factors used by other Federal bank regulators. In addition, we found that FDIC guidance did not address how to apply the terms "substantial compliance" and "partially met." We also found that termination decisions were not centrally monitored, which would serve as an important internal control. Further, the FDIC did not consistently prepare and maintain documentation to support the monitoring of, and termination decision-making for, BSA/AML Consent Orders. The report contained 10 recommendations intended to enhance the FDIC's BSA/AML Consent Order termination-related guidance and procedures.	10	4	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
REV-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
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 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	9	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-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, FDIC had not integrated Agency-wide supply chain risks into its Enterprise Risk Management processes. We also determined that Contracting Officers did not maintain contract documents in the Contract Electronic File system, as required. The report contained nine recommendations to improve the FDIC's SCRM Program and retention of contract documents.	9	6	NA
REV-22-002 **Controls Over Payments to Outside Counsel** March 16, 2022	The FDIC's Legal Division relies on Outside Counsel to assist with legal matters. Between January 2018 and March 2021, the Legal Division paid approximately $94 million to Outside Counsel. We conducted a review to determine whether the Legal Division's review and oversight of payments to Outside Counsel could be improved. We found that the FDIC Legal Division should improve its review and oversight of payments to Outside Counsel in four areas: (1) increasing the analysis of FDIC data; (2) providing clear guidance in specific areas; (3) sharing the results of post-payment reviews with those involved in the invoice review process; and (4) providing a periodic training program to reinforce expectations and requirements. The report contained eight recommendations designed to improve the FDIC Legal Division's review and approval of payments to Outside Counsel, ensure consistency and conformance with the FDIC's procedural requirements, and promote the FDIC's efforts to reduce and recover disallowed costs.	8	1	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-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. 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 NIST security standards and guidelines. In addition, the FDIC completed certain actions to continue to strengthen its security controls since last 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 can be improved to reduce the impact of the confidentiality, integrity, and availability of the FDIC's information systems and data. The report contained one recommendation for the FDIC to address 31 flaw remediation Plans of Action and Milestones.	1	1	NA

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

Table II: Audit and Evaluation Reports				
Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	Title	Total	Unsupported	
REV-23-001 December 13, 2022	*Security Controls Over the FDIC's Wireless Network*			
AUD-23-001 January 31, 2023	*Implementation of FDIC's Information Technology Risk Examination (InTREx) Program**			
AUD-23-002 March 15, 2023	*The FDIC's Security Controls Over Microsoft Windows Active Directory*			
REV-23-002 March 31, 2023	*FDIC Oversight of a Telecommunications Contract*			$1,500,000
Totals for the Period		**$0**	**$0**	**$1,500,000**

*Management decisions were not made for 5 of 19 recommendations in this report as of the end of the reporting period. Management decisions were made for all other reports listed.

Other products issued:

- *Top Management and Performance Challenges Facing the FDIC, February 16, 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 two recommendations made in a report issued in a prior reporting period.)

During this reporting period, there were two 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.

We made three recommendations related to this finding. Recommendations 13 and 14 do not have management decisions, and both of these recommendations rely on the completion of Recommendation 15. Specifically, we recommended that the FDIC:

- Establish and implement a means to share classified information with the Regional Offices in a timely manner so that it is actionable. (Recommendation 13)
- Establish a means for Regional Offices to handle classified information once it is shared, including the infrastructure (systems, facilities, and communications) to securely handle, transmit, discuss, store, and dispose of classified information. (Recommendation 14)
- Evaluate and document whether additional Regional Office personnel should be required to hold a security clearance based on business needs. (Recommendation 15)

At the time we issued our report, the FDIC concurred with Recommendation 13 and 15, and did not concur with Recommendation 14. The FDIC conducted a Regional Security Clearance Evaluation and documented the results of the evaluation in an FDIC Memorandum. Based on its evaluation, the FDIC reversed its longstanding position of maintaining security clearances for its Regional Directors. The FDIC stated it would eliminate the security clearances for Regional personnel (except for the Regional Directors in New York and Dallas, for the limited purposes of "business continuity"). However, we determined that the FDIC Memorandum did not provide sufficient support for its decision to eliminate security clearances for Regional personnel. Specifically, based on the information included in the FDIC Memorandum, the FDIC did not conduct a thorough assessment of the benefits and value of sharing classified threat information with its Regional personnel.

In our Semiannual Report to the Congress for the period April 1, 2022 through September 30, 2022, we reported that if resolution of the recommendations was not reached by February 2023, we would elevate the recommendations to the Audit Follow-up Official for final management decision. We were unable to reach resolution of the recommendations by February 2023 and, therefore, on March 21, 2023, we elevated the three recommendations to the Audit Follow-up Official for a final Management Decision.

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	37
Number of Persons Referred to the Department of Justice for Criminal Prosecution	69
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	None
Number of Indictments and Criminal Informations	50

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, we conducted an investigation involving the Misuse of a Government Computer by a Senior FDIC Employee. We initiated this investigation upon the receipt of an allegation that a senior FDIC employee had misused the employee's FDIC-issued electronic equipment. The OIG investigation found the employee downloaded and/or stored a significant number of sexually explicit, sexually oriented, and/or indecent images and files on the employee's FDIC-issued laptop in violation of FDIC policy. The OIG completed its investigation and provided its report to the FDIC in December 2022 for appropriate action. The employee retired shortly after the OIG provided its report to the FDIC.

Table VII: Instances of Whistleblower Retaliation

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

Table VIII: Instances of Agency Interference with OIG Independence

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

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

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

During this reporting period, there were no audits or evaluations involving senior Government employees that were closed and not disclosed to the public. As noted in Table VI above, the OIG conducted one investigation of a senior government official that was closed and that was 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 October 1, 2022 through March 31, 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 is scheduled for Fall 2023 and will be conducted by the Department of Veterans Affairs OIG.

Congratulations and Farewell

During the reporting period, we congratulated and said farewell to several OIG leaders and staff upon their retirements. IG Jay N. Lerner retired after more than 30 years of Federal service. Deputy IG Gale Stallworth Stone also ended her Federal career after serving more than 37 years. Kathleen Enstrom, our Special Agent in Charge of the OIG's Chicago Region retired following more than 27 years in Federal law enforcement. Special Agent Lance Endy from the OIG's Electronic Crimes Unit also concluded his Federal service after a 30-year career. Special Agent Joe Moriarty retired following a Federal career of more than 32 years. And finally, Gary Sherrill, Senior Investigative Advisor, retired from the OIG following an outstanding 47-year Federal career.

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 Board and most senior leadership, FDIC Division and Office management, and our law enforcement partners 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.

Retirement Reception for Jay N. Lerner

January 12, 2023

FDIC Chairman Martin J. Gruenberg presenting IG Jay N. Lerner with an FDIC Board Resolution.

IG Jay N. Lerner delivers remarks during his retirement reception.

IG Jay N. Lerner with current and former Federal Inspectors General.

DESIGN: FDIC/OCOM/GRAPHIC DESIGN AND PRINTING UNIT

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

Follow us on Twitter: @FDIC_OIG.

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

Office of Inspector General
Federal Deposit Insurance Corporation

HOTLINE

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

For example:

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

Make a Difference and Contact Us:

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

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

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

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

OIG
Office of Inspector General

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

FDIC-013-2023