FDIC Office of Inspector General

Semiannual Report to the Congress

October 1, 2021 – March 31, 2022

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 5,670 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured $9.73 trillion in domestic deposits in 4,839 institutions, of which the FDIC supervised 3,122. The Deposit Insurance Fund balance totaled $123.1 billion as of December 31, 2021. Active receiverships as of March 31, 2022 totaled 188, with assets in liquidation of about $86.6 million.

Semiannual Report to the Congress

October 1, 2021 – March 31, 2022

Office of Inspector General

Federal Deposit Insurance Corporation

Inspector General's Statement

On behalf of the Office of Inspector General (OIG) at the Federal Deposit Insurance Corporation (FDIC), I am pleased to present our Semiannual Report for the period from October 1, 2021 through March 31, 2022.

During this reporting period, our audits and evaluations provided 77 recommendations to the FDIC to strengthen controls and improve efficiencies. Our reports covered such topics as the FDIC's Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders, Threat Information Sharing, Information Security, Whistleblower Rights and Protections for Contractors, Controls over Payments to Outside Counsel, and Supply Chain Risk Management.

Importantly, in February, we also issued our assessment of the Top Management and Performance Challenges Facing the FDIC, which helps to identify the most urgent risks on which policymakers should focus attention. We identified nine Top Challenges facing the FDIC:

- The FDIC's Readiness for Crises;
- Cybersecurity for Banks and Third-Party Service Providers;
- Supporting Underserved Communities in Banking;
- Organizational Governance at the FDIC;
- Information Technology Security at the FDIC;
- Security and Privacy at the FDIC;
- The FDIC's Collection, Analysis, and Use of Data;
- Contracting and Supply Chain Management at the FDIC; and
- Human Resources at the FDIC.

Of special note, in December 2020, our Office called attention to an issue regarding banks' reporting of cyber incidents. As a result of our work, the FDIC and other financial regulators proposed a rule requiring financial institutions and their service providers to promptly notify their primary Federal regulator if they experienced a destructive cyber incident. The rule was promulgated during the reporting period in November 2021 and now requires that a banking organization notify its financial regulator of a significant computer-security incident within 36 hours after the incident.

In addition, our OIG Special Agents and investigative support staff have continued to work closely with law enforcement partners to investigate criminal and administrative matters involving sophisticated, complex multi-million-dollar frauds. These schemes involve bank fraud, embezzlement, money laundering, currency exchange manipulation, and other crimes involving banks, executives, directors, officials, insiders, and financial professionals. We are also working to detect and investigate cyber-criminal cases that threaten the banks and banking sector.

During the past 6 months, our cases resulted in 90 indictments; 69 convictions; 58 arrests; and more than $939 million in fines, restitution ordered, and other monetary recoveries. In one such case, the former owner of DC Solar was sentenced to 30 years in prison and ordered to pay restitution of $790 million for his role in a Ponzi scheme involving investor losses totaling approximately $1 billion. According to the Department of Justice, this was the biggest criminal fraud scheme in the history of the Eastern District of California.

Our Office also continues to play a key role in the investigation of individuals and organized groups perpetrating fraud through the Paycheck Protection Program (PPP) under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) and American Rescue Plan (ARP). To date, we have opened 169 cases associated with fraud in the CARES Act and ARP programs. Over the past 6 months, our joint work in this area resulted in 51 criminal complaints, indictments, and informations; 35 arrests; 28 convictions; and more than $54 million in fines, restitution ordered, and forfeitures. We strongly support the Pandemic Response Accountability Committee's Fraud Task Force and the Department of Justice's COVID-19 Fraud Enforcement Task Force. The FDIC OIG will continue to work in close collaboration with our law enforcement partners.

I am especially grateful to the dedicated women and men of our Office. We appreciate the support of Members of Congress, and that of the FDIC Board of Directors and senior officials. We remain committed to serving the American people with our strong independent oversight.

Jay N. Lerner
Inspector General
April 2022

Table of Contents

Acronyms and Abbreviations

AEC	Audits, Evaluations, and Cyber
BSA/AML	Bank Secrecy Act/Anti-Money Laundering
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CFETF	Coronavirus Fraud Enforcement Task Force
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
COVID-19	Coronavirus Disease 2019
DATA Act	Digital Accountability and Transparency Act of 2014
DEIA	Diversity, Equity, Inclusion, and Accessibility
DIF	Deposit Insurance Fund
DOJ	Department of Justice
ECU	Electronic Crimes Unit
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FHFA	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
FMC	First Mortgage Company, LLC
IG	Inspector General
IMS	Information Management System
IRS-CI	Internal Revenue Service-Criminal Investigation
IT	Information Technology
MSG	Mobile Solar Generator
NIST	National Institute of Standards and Technology
OC	Outside Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
POAM	Plan of Action and Milestones
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
SAR	Suspicious Activity Report
SBA	Small Business Administration
SCRM	Supply Chain Risk Management
SSA	Social Security Administration
UNCF	United Negro College Fund
USAO	United States Attorney's Office
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, 2021–March 31, 2022)	
Audit, Evaluation, and Other Products Issued	**9**
Nonmonetary Recommendations	**77**
Investigations Opened	**54**
Investigations Closed	**18**
Judicial Actions:	
Indictments/Informations	**90**
Convictions	**69**
Arrests	**58**
OIG Investigations Resulted in:	
Fines of	**$2,500,685.00**
Restitution of	**$934,659,269.69**
Asset Forfeitures of	**$2,286,325.70**
Total	**$939,446,280.39**
Referrals to the Department of Justice (U.S. Attorneys)	**60**
Responses to Requests Under the Freedom of Information/Privacy Act	**7**

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 past 6 months, audit and evaluation work covered activities related to such topics as Termination of Bank Secrecy/Anti-Money Laundering Consent Orders, Threat Sharing, Information Security, Whistleblower Rights and Protections, Supply Chain Risk Management, and Payments to Outside Counsel. Audit and evaluation reports issued during the period resulted in 77 recommendations to management. Importantly, in February 2022, we also issued our report on the *Top Management and Performance Challenges Facing the FDIC* and provided it to FDIC management for inclusion in its Annual Report.

Of note during the reporting period, our Office of Audits, Evaluations, and Cyber (AEC) announced its **QUICK** Vision for AEC. This Vision stems from the FDIC OIG Vision of "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." QUICK represents the following attributes: **Q** – Quality-centric: Doing quality work and delivering quality products. Doing the right work, the right way, and communicating meaningful results for the FDIC, Congress, and the American people. **U** – Urgent-minded: Having the proper sense of urgency to keep things moving forward while not sacrificing quality. AEC views situations as opportunities and challenges rather than hurdles or struggles. **I** – Impact-oriented: Presenting AEC's results in the most compelling way. Focusing on impacts and effects and adding value for all of our stakeholders. **C** – Connected-together: Connecting with each other as people first. AEC works in a collaborative, unified, and supportive way toward the same goals and outcomes. **K** – Knowledge-seeking: Having a growth mindset and being a continuous learner. Understanding and consistently applying AEC policies and procedures.

AEC also brought on board a new Deputy Assistant Inspector General (DAIG) during the reporting period who will share leadership responsibilities with the AIG as the OIG carries out its audits, evaluations, and other reviews.

We also note that in addition to planned discretionary work that emanates largely from the Top Management and Performance Challenges, 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, there were no failed institutions requiring that we conduct either a Material Loss Review or a Failed Bank Review.

Results of the audits, evaluations, and other reviews completed during the reporting period are summarized below. Reports and accompanying videos can be found at www.fdicoig.gov.

Audits, Evaluations, and Other Reviews

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 policy-makers, 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 during the reporting period.

We found that the FDIC did not establish effective governance processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. Specifically, the FDIC:

- Did not establish a written governance structure to guide its threat information sharing activities;
- Did not complete, approve, and implement a governance Charter to establish a common understanding of the role for the FDIC's Intelligence Support Program, or to define an overall strategy and its requirements;
- Did not develop goals, objectives, or measures to guide the performance of its Intelligence Support Program;
- Did not establish adequate policies and procedures that defined roles and responsibilities for key stakeholders involved in the threat information sharing program and activities; and
- Did not fully consider threat information sharing in its Enterprise Risk Inventory and Risk Profile.

Further, we identified additional gaps in the FDIC's processes for acquiring, analyzing, and disseminating threat information, and in how the use of threat information could be improved. For example, the FDIC:

- Did not develop written procedures for determining its threat information requirements;
- Did not engage all relevant stakeholders when it developed its threat information needs;
- Did not establish procedures to guide its analysis of threat information; instead, the FDIC relied solely on the discretionary judgment of certain individuals to determine the extent to which threat information should be analyzed to support business and supervisory needs;
- Did not develop procedures for disseminating threat information;
- Had not established an infrastructure that would allow for the secure handling of classified information to certain senior FDIC officials; and
- Did not establish a procedure to obtain feedback from recipients of threat information to assess its utility and effectiveness.

Cyber Reporting Requirements by Banks

In April 2020, as part of our ongoing Threat Information Sharing review, the OIG identified an issue–that the banks were not required to report significant cyber incidents to the FDIC in a timely manner. After identifying this issue, we submitted a memorandum recommending that financial institutions be required to notify the FDIC of cyber incidents. As a result, in December 2020, the FDIC, the Federal Reserve Board, and the Office of the Comptroller of the Currency announced a proposed new regulation that would require all financial institutions and their service providers to promptly notify their primary Federal regulator if they experience a destructive cyber incident. This rule was made final in November 2021 and now requires that a banking organization notify its financial regulator of a significant computer-security incident no later than 36 hours after a cyber incident has occurred. This final rule reflects the great work and contributions of our OIG team, as well as the value and significance of the OIG's work in identifying critical issues for the FDIC.

We also found numerous gaps in the FDIC's management of threat information sharing, including: not having backup personnel for its Senior Intelligence Officer nor plans for an absence or departure; not establishing minimum training requirements for the Senior Intelligence Officer position; not obtaining required security clearances for certain senior FDIC officials; and not properly categorizing unclassified threat information.

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.

Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders

Money laundering is a serious crime that aims to conceal or disguise the illicit proceeds of another unlawful activity. The Bank Secrecy Act (BSA) has established recordkeeping and reporting requirements for financial institutions to implement -- in order to detect and prevent money laundering. The FDIC's examinations of banks for compliance with these requirements are essential elements in identifying potential weaknesses in a bank's BSA/Anti-Money Laundering (AML) program.

When a financial institution is not in compliance with such requirements, the FDIC may issue a Consent Order— which is a formal enforcement action against a bank. A BSA/AML Consent Order often contains several provisions for improvements to the bank's program, and FDIC examiners review a bank's progress in addressing these Consent Order provisions.

Our Office 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 the Federal Reserve Board and the Office of the Comptroller of the Currency. When Consent Orders are issued, all provisions requiring correction are published on the FDIC website; however, informal actions are not issued publicly. In some cases, the FDIC may terminate a Consent Order when provisions are in "substantial compliance" or "partially met." Therefore, in terminating an FDIC Consent Order, it will be removed from the website – even if not all of the provisions have been corrected. As a result, these website postings make it appear to the public, bank customers, and bank investors that all Order provisions have been corrected, although some previously-publicized Order provisions may not have been met.

We further found that the FDIC did not provide guidance to its examiners in how to apply the terms, "substantial compliance" and "partially met," as a basis for terminating a Consent Order. The term, "partially met," provides extremely wide latitude to terminate a Consent Order when any portion of it is met. As a result, the FDIC could not be certain that some Consent Orders were terminated using a consistent interpretation of these terms.

In addition, we found that:

- Termination decisions were not centrally monitored, which would serve as an important internal control.
- The FDIC did not consistently prepare and maintain documentation in its systems of record to support the monitoring and termination decisions for BSA/AML Consent Orders.

Incorrect documentation of Consent Order terminations caused the FDIC to provide nine incorrect reports to the FDIC Board of Directors concerning enforcement actions; and caused the FDIC not to report three BSA/AML Consent Order terminations to the Financial Crimes Enforcement Network in the Department of the Treasury.

We made 10 recommendations to enhance the FDIC's BSA/AML Consent Order termination guidance and procedures.

Whistleblower Rights and Protections for FDIC Contractors

Whistleblowers play an important role in safeguarding the Federal Government against waste, fraud, abuse, and mismanagement. Their willingness to report wrongdoing can contribute to significant improvements in Government programs and operations. 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 did not consistently adopt or apply requirements intended to notify contractor and subcontractor employees about their whistleblower rights and protections. Specifically, the Whistleblower Rights and Notification Clause for contractors was not included in three of the nine FDIC contracts reviewed. Further, the FDIC's Legal Division, under its separate contracting authority, had not adopted any whistleblower rights notification provisions for contractors nor included any whistleblower clauses in its contracts.

In addition, the FDIC had not established any requirements for its officials to ensure that contractors carried out their obligations under the FDIC's Whistleblower Rights Notification Clause. Also, the FDIC had not verified that contractors informed their employees of whistleblower rights and protections, nor did the FDIC confirm that the contractors had inserted the clause in subcontracts exceeding $100,000.

We also found that the FDIC did not obtain Confidentiality Agreements from all of its contractors and contract personnel, as required. In addition, we reported that the guidance provided by the FDIC Legal Division may be unclear and confusing to contractor or subcontractor whistleblowers as to whom to report criminal behavior or allegations of fraud, waste, abuse, or mismanagement.

We made 10 recommendations aimed at ensuring that contractors and subcontractors are properly informed of their whistleblower rights and protections.

The FDIC's Implementation of Supply Chain Risk Management

The FDIC awarded more than $2 billion via 483 contracts in 2021, procuring products and services from many types of vendors, contractors, and subcontractors. The supply chain for each vendor, contractor, or subcontractor may present unique risks to the FDIC, including the installation of counterfeit hardware and software in the FDIC environment, or reliance on a malicious or unqualified provider. Supply chain threats could compromise the FDIC's Information Technology and data on its information systems and provide adversaries a means to exfiltrate sensitive information such as confidential bank examination information.

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, goals, and objectives; protect its sensitive and nonpublic information; and maintain the integrity of its operations. We conducted an evaluation to determine whether the FDIC developed and implemented its SCRM Program in alignment with the Agency's objectives and best practices.

We found that the FDIC had not implemented several objectives outlined in its SCRM Implementation Project Charter (November 2019) and was not conducting supply chain risk assessments in accordance with best practices. For example, the FDIC had not:

1. Identified and documented known risks to the Agency's supply chain;
2. Defined a risk management framework to evaluate risks to non-Information Technology procurements; or
3. Established metrics and indicators related to continuous monitoring and evaluation of supply chain risks.

We also found that the FDIC did not conduct supply chain risk assessments during its procurement process for Chief Information Officer Organization and other Division and Office contracts. In addition, the FDIC had not ensured that its Enterprise Risk Management processes fully captured supply chain risks. Further, FDIC Contracting Officers did not maintain contract documents in the Contract Electronic File system, as required.

We made nine recommendations to the FDIC to address the findings in our report and strengthen its SCRM Program.

Controls Over Payments to Outside Counsel

The FDIC's Legal Division relies on Outside Counsel (OC) to assist with legal matters. Between January 2018 and March 2021, the Legal Division paid approximately $94 million to OC to support the FDIC's interests in litigation and other legal matters. The FDIC must apply effective contract oversight in order to strengthen prudent management of FDIC resources and ensure that the FDIC receives goods and services as contracted.

Our Office conducted a review to determine whether the Legal Division's review and oversight of payments to OC can be improved. We found that the FDIC Legal Division should improve its review and oversight of payments to OC in four areas:

- Analyzing data to monitor and assess the effectiveness of program controls for reviewing invoices received from OC;
- Enhancing its policies and procedures by adding specific guidance in certain areas in order to ensure the consistent interpretation and applications of its requirements;
- Communicating the results of the Post-Payment Review Program to those involved in reviewing and approving OC invoices to improve their understanding of requirements and identify areas where revised guidance is needed; and
- Providing training to all FDIC personnel responsible for the review and approval process for OC invoices to ensure requirements are consistently understood among existing staff and new hires.

We made eight recommendations to the FDIC to address the findings in our report and improve the Legal Division's controls over payments to OC.

Reliability of Data in the FDIC Virtual Supervisory Information on the Net System
The Virtual Supervisory Information on the Net System (ViSION) contains information relating to the financial conditions, bank examinations, and supervisory matters involving FDIC-regulated financial institutions. It is considered by the FDIC to be a "mission-essential" system that supports its supervision and insurance responsibilities. There are more than 4,100 users of the ViSION system.

We conducted an evaluation to determine whether key supervisory information in the ViSION system was reliable: accurate, complete, and supported by source documentation. The FDIC guidance states that the ViSION system contains 19 key data elements that must be error free, with a required accuracy rate of 100 percent. Our evaluation focused on four of these data elements in the ViSION system: (1) Examination Ratings; (2) Examination Start Date; (3) Examination Completion Date; and (4) Examination Report Mail Date.

We found that two of the four key data elements tested were not reliable. Specifically, we found numerous errors for the Examination Completion Date (14 banks) and the Examination Report Mail Date (12 banks), because of weaknesses in the FDIC's quality control procedures and practices for these two key data elements. Unreliable Completion Dates may increase the risk of a late examination start and thereby noncompliance with statutory requirements for examination frequency, and similarly, unreliable Mail Dates may increase the risk of incorrect deposit insurance assessments, though we did not detect late examination starts or incorrect assessments in our sample. We did not find errors for the Examination Ratings and Start Date data elements. We also concluded that the risk-based assessment of the ViSION system data was outdated and not properly documented.

We made six recommendations for the FDIC to develop and implement standard guidance; conduct training; revise quality assurance procedures; correct errors in ViSION; conduct a risk assessment to identify key supervisory information in the ViSION system; and update the data reliability guidance based upon the results of the risk assessment.

The FDIC's Compliance under the Digital Accountability and Transparency Act of 2014
The Digital Accountability and Transparency Act of 2014 (DATA Act) expanded the reporting requirements of the Federal Funding Accountability and Transparency Act of 2006. Consistent with the DATA Act, the objectives of the audit we conducted were to assess the (1) completeness, accuracy, timeliness, and quality of the financial and award data submitted for the first quarter of Fiscal Year 2021 and published on USASpending.gov and (2) FDIC's implementation and use of the Government-wide financial data standards established by the Office of Management and Budget (OMB) and the Department of the Treasury.

We found that the FDIC's financial and award data submitted for the first quarter of Fiscal Year 2021 was timely, of higher quality, and accurate, but was not complete. We also found that the FDIC recorded the required transactions and events for the DIF during the proper period. However, the FDIC's submission that contained appropriation summary-level data excluded two Treasury Account Symbols (TAS) from which funds were obligated. As a result, obligation and outlay amounts for the two TASs were not available for display on USASpending.gov.

We further found that the FDIC had established controls to promote complete, accurate, timely, and quality reporting of the DIF data under the DATA Act. The FDIC will need to revise its procedures and processes in order to reflect the requirement to report on all TASs.

We made three recommendations for the FDIC to improve its processes and procedures for accurately recording its financial data.

The FDIC's Information Security Program - 2021

The OIG engaged a contractor firm to conduct the audit of the *FDIC's Information Security Program–2021*, which evaluated the effectiveness of the FDIC's information security program and practices, as required by the Federal Information Security Modernization Act of 2014 (FISMA).

IGs assess the effectiveness of the agency's information security programs and practices using a maturity model. This maturity model aligns with the five function areas in the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover. IGs assign maturity level ratings to each of the five function areas, as well as an overall rating, using a scale of 1-5. The audit determined that the FDIC's overall information security program was operating at a Maturity Level 4. The Department of Homeland Security FISMA Metrics indicated that the maturity ratings are determined by a simple majority where the most frequent level (mode) across the component questions serves as the domain rating, even where there are wide disparities among ratings.

The audit report also identified significant security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices, the most significant of which are described below:

High Number of Overdue and Unaddressed High- and Moderate-Risk Plans of Action and Milestones (POA&M). There were 176 high- and moderate-risk open POA&Ms, and the scheduled completion dates ranged from March 2010 to July 2021. Without consistently addressing control deficiencies timely, the FDIC will continue to face an increasing backlog of POA&Ms, leaving its data more vulnerable to security exploits from unmitigated threats.

The FDIC's Supply Chain Risk Management Program (SCRM) Lacks Maturity. The FDIC had not defined processes and procedures that support the underlying components of its SCRM directive. Without SCRM processes and procedures, the FDIC cannot be sure that its products, system components, systems, and services provided by external parties are maintained consistently with its cybersecurity requirements, thus placing it at increased risk of exploitation through its supply chain.

Administrative Account Management Needs Improvement. Administrative Accounts are highly sought-after targets by hackers and other adversaries who may wish to use the accounts to corrupt data, launch attacks, or conduct other malicious activities. We have reported weaknesses related to Administrative Account management in each of our past four FISMA audit reports issued since 2017. During FY 2021, the FDIC opened 10 additional POA&Ms related to privileged user access. Weaknesses in the FDIC's processes for managing Administrative Accounts increase the risk of unauthorized activity, such as individuals accessing, modifying, deleting, or exfiltrating sensitive information.

Inadequate Oversight and Monitoring of FDIC Information Systems. Historically, several systems, components, and services that should have been assessed according to the NIST Risk Management Framework (RMF) process were instead mischaracterized as subject to the now-rescinded Outsourced Solution Assessment Methodology. As a result, the FDIC did not subject these systems to a proper risk assessment, authorization to operate (ATO), or ongoing monitoring in accordance with the RMF. As of June 22, 2021, the FDIC had not completed ATOs for 10 operational systems. We noted that until the FDIC subjects all of its systems to the RMF, the FDIC cannot be sure it will identify and address security and privacy risks in a timely manner.

The audit report contained six recommendations for the FDIC to address the weaknesses we identified in order to strengthen its information security program and practices.

Top Management and Performance Challenges

The FDIC plays a unique and vital role in support of the U.S. financial system. At the time we issued our annual assessment, the FDIC insured approximately $9.5 trillion in bank deposits at over 4,900 banks, supervised and examined more than 3,200 banks, oversaw over $123 billion in the DIF that protects bank depositor accounts, and was responsible for resolving failed and failing banks.

Our Top Management and Performance Challenges document summarizes the most serious challenges facing the FDIC and briefly assesses the Agency's progress to address them, in accordance with the Reports Consolidation Act of 2000 and Office of Management and Budget Circular A-136 (revised August 10, 2021). The Top Challenges document 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 document, we considered comments from the FDIC, and while exercising our independent judgment, we incorporated suggestions where appropriate. We acknowledged several instances where the FDIC had taken steps to address the Challenge, particularly where the Agency had implemented concrete actions that demonstrated a direct relationship towards achieving a desired outcome. We also recognized that there may have been other ongoing plans and intentions for future activities that may still have been under development at the time of our writing.

We identified nine Top Challenges facing the FDIC, as follows:

The FDIC's Readiness for Crises. The FDIC must be prepared for all crises, because of its unique role in overseeing and administering the DIF, which insures the bank accounts of millions of depositors and consumers. The FDIC faces Challenges in fully developing its plans to respond to an unfolding crisis. Further, the FDIC should consider climate-related risks with respect to the report issued by the Financial Stability Oversight Council, and whether it will take actions in response to the report's recommendations in preparing its supervisory and examination processes. The FDIC should also be ready to respond to evolving risks associated with the current pandemic and other crises, including supervising and examining Government-guaranteed loans at banks and related fraud risks.

Cybersecurity for Banks and Third-Party Service Providers. 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 appropriate 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 establish a process to receive, analyze, and act on reports of significant cyber incidents at banks in order to adjust supervisory strategies, policies, and training for bank examiners; to warn other banks of such threats; and to prepare for potential bank failures. 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. The FDIC also should assess the risks to banks presented by crypto assets, particularly with respect to the anonymous nature of these assets and the increased risk of money laundering and other wrongdoing.

Supporting Underserved Communities in Banking. The FDIC should ensure that its programs – including those that support Minority Depository Institutions and Community Development Financial Institutions – are effectively designed to foster financial inclusion and reduce the number of unbanked and underbanked individuals. Further, the FDIC's examinations should continue to ensure that banks are in compliance with regulations that combat discriminatory lending practices against low-income borrowers and minority populations. The FDIC also should ensure that its examiners have the skills, capabilities, and procedures to assess the effect of banks' use of artificial intelligence in decision-making and minimize any undue bias related to the algorithms or historical data used.

Organizational Governance at the FDIC. Effective governance allows FDIC Board members and senior FDIC officials to manage the affairs of the Agency and its risks, 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 towards achieving the FDIC's mission. The FDIC faces Challenges in providing clarity concerning the submission of motions presented to the Board of Directors for consideration and approval. Further, the FDIC should ensure that the Board, through its Audit Committee, can oversee and manage the risks identified and monitored through its Enterprise Risk Management Program. The FDIC also should clarify under what circumstances and which portions or provisions of Executive Branch policies or guidance are to be followed. In addition, the FDIC should ensure that weaknesses in FDIC programs are corrected and recommendations are addressed in a timely manner. FDIC rulemaking and guidance should also be aligned with other regulators to ensure that banks are not treated differently depending upon their primary regulator. FDIC internal guidance also should be clearly defined to ensure consistent application of FDIC program requirements. In addition, FDIC rulemaking should be a transparent process that analyzes the need for safety and soundness regulations and the compliance burden placed on banks.

Information Technology (IT) Security at the FDIC. The FDIC relies on its IT systems for day-to-day activities and especially during crises. 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 address its outstanding corrective actions related to IT security controls, management of privileged Administrative Accounts, and oversight and monitoring of information systems. Further, the FDIC should ensure that it establishes effective security controls for its mobile devices and for the automated systems that monitor and control critical building services at facilities.

Security and Privacy at the FDIC. The FDIC employs a workforce of approximately 5,800 employees and 1,600 contract personnel at 92 FDIC facilities throughout the country, and it is custodian of 76 IT systems and voluminous hard-copy records. The FDIC should continue to manage risks associated with its personnel security and suitability processes to ensure that employees and contractors undergo appropriate and timely investigations and re-investigations commensurate with their positions. As well, the FDIC should maintain its risk-based physical security program and ensure that its policies promote an FDIC work environment that is free from discrimination, harassment, and retaliation. Further, the FDIC should have effective programs to safeguard all forms of sensitive and personally identifiable information in its possession.

The FDIC's Collection, Analysis, and Use of Data. Data and information can enhance capabilities to mitigate threats against banks and the U.S. financial system. The FDIC faces Challenges in establishing effective processes to govern its sharing of threat information to guide the supervision of financial institutions. Effective sharing of threat information helps the FDIC to protect the DIF and the financial system by building situational awareness; supporting risk-informed decision-making; and influencing supervisory strategies, policies, and training. The FDIC should establish a written governance structure and implement a Charter to establish a common understanding of its Threat Information Sharing program and define an overall strategy and requirements for it. Further, the FDIC should develop goals, objectives, and measures to guide the performance of its Intelligence Support Program, and it should establish adequate policies and procedures to define roles and responsibilities. The FDIC faces Challenges in the four component functions of Threat Information Sharing – acquisition, analysis, dissemination, and feedback. Further, the FDIC should improve the reliability of its internal data to ensure that the FDIC Board and senior officials can depend upon the data to assess program effectiveness throughout the organization.

Contracting and Supply Chain Management at the FDIC. The FDIC awarded over $2 billion in contracts for goods and services in 2021 in support of its mission. 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. Further, the FDIC should have processes in place to identify and ensure heightened monitoring of contracts for Critical Functions, so that the Agency maintains control of its mission functions and prevents over-reliance on contractors. The FDIC also should have programs in place to manage and mitigate security risks associated with the supply chains for contracted goods and services. Further, the FDIC should ensure notifications to contractors and sub-contractor personnel, so that they are advised about and aware of their whistleblower rights and protections, and that they know how to report allegations of misconduct, violations, and gross mismanagement.

Human Resources at the FDIC. The FDIC relies on the talents and skills of its employees to achieve its mission, and it faces Challenges in managing its human capital lifecycle. At the present time, nearly 25 percent of the FDIC workforce is eligible to retire, and this figure climbs to nearly 40 percent by 2026. These figures include personnel in key divisions supporting the FDIC mission – including the Division of Resolutions and Receiverships (over 59 percent by 2026); Division of Finance (over 55 percent by 2026); Legal Division (over 51 percent by 2026); and Division of Administration (about 49 percent by 2026). Further, the FDIC should continue to improve its program for the retention of employees, as well as the collection and analysis of relevant personnel data. In addition, the FDIC should continue to ensure diversity and inclusion among its workforce. 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 work environment.

Ongoing Work

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

- *Examinations of Government-Guaranteed Loans*. The objective is to determine the effectiveness of the FDIC's examinations in identifying and addressing undue risks and weak risk management practices for banks that participate in government-guaranteed loan programs.
- *Security Controls Over the Windows Active Directory*. The objective is to assess the effectiveness of controls for securing and managing the Windows Active Directory to protect the FDIC's network, systems, and data.
- *Security Controls Over the FDIC's Wireless Networks*. The objective is to determine whether the FDIC has implemented effective security controls to protect its wireless networks.
- *Implementation of the Information Technology Risk Examination (InTREx) Program*. The objective is to determine the effectiveness of the InTREx program in assessing and addressing information technology and cyber risks at FDIC-supervised financial institutions.

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

Pandemic Response Accountability Committee Updates

March 27, 2022 was the 2-year mark of the enactment of the Coronavirus Aid, Relief, and Economic Security (CARES) Act. The Pandemic Response Accountability Committee (PRAC) was created as part of the CARES Act in March 2020. The PRAC is a Committee of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and is comprised of 22 Federal Inspectors General (IG), including the FDIC IG, who are working collaboratively to oversee more than $5 trillion in Federal pandemic-relief emergency spending. The PRAC's primary mission is to work with OIGs to ensure that taxpayer money is used effectively and efficiently to address the pandemic-related public health and economic needs that were funded through the various COVID-19 relief bills. Several of PRAC's noteworthy initiatives during the reporting period follow:

Virtual Roundtables with the National Academy of Public Administration: The PRAC held two roundtable events with the National Academy of Public Administration during the reporting period. The first event featured a panel of experts who examined the impact of housing and rental assistance relief programs on underserved communities. During the second roundtable, a panel of experts examined the effectiveness of pandemic relief programs in broadband assistance, and how local governments used pandemic funding to address broadband challenges.

Congressional Transparency Caucus Event: On October 20, 2021, the Congressional Transparency Caucus hosted a conversation with the PRAC to learn about its crucial role in overseeing $5 trillion in pandemic relief legislation. PRAC Chairman and Department of Justice IG Michael Horowitz, Liz Hempowicz of the Project on Government Oversight, former Chicago IG Joseph Ferguson, and Caryl N. Brzymialkiewicz, Deputy IG at the Department of the Interior participated on the panel. Panelists discussed the importance of transparency and oversight of the trillions of dollars the Federal government has spent fighting the COVID-19 pandemic and supporting Americans during this crisis and how the PRAC can help the administration, state and local government, and Congress to ensure effective use of these funds and fight fraud, waste, and abuse.

Webinar with The Levin Center: On March 15, 2022 the PRAC co-hosted a webinar with The Levin Center. The webinar for state legislators and staff featured the PRAC and Levin Center experts covering state pandemic response and oversight.

Testimony: *Pandemic Response and Accountability: Reducing Fraud and Expanding Access to COVID-19 Relief through Effective Oversight.* On March 17, 2022 the Chair of the PRAC testified before the Senate Committee on Homeland Security and Governmental Affairs about the PRAC's ongoing oversight work, achievements during its first 2 years, and the collaborative model it is providing in building a legacy for effective, coordinated government oversight.

Feature on NBC News' Investigative Series 'The Fleecing of America': The PRAC Chair was interviewed by NBC Nightly News Anchor Lester Holt to discuss COVID-19 relief fund scams and the efforts of the PRAC and Inspectors General to prevent the abuse of taxpayer dollars. The segment kicked off the return of the network's investigative series, *The Fleecing of America*.

Our Office supports these and other ongoing initiatives. Results of our investigative cases involving COVID-19 relief fraud are discussed in the *Investigations* section of this semiannual report. We look forward to continuing to work with others in the IG community and law enforcement to oversee the funds provided in the legislation and to keep the public informed as we address the challenges posed by the COVID-19 pandemic.

For ongoing efforts of the Committee, consult the PRAC website, pandemic.oversight.gov and its Twitter account, @COVID_Oversight.

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, money laundering, embezzlement, and currency exchange rate manipulation. Our cases often involve bank executives, officers, and directors; other financial insiders such as attorneys, accountants, and commercial investors; private citizens conducting businesses; and in some instances, FDIC employees.

The OIG's Electronic Crimes Unit (ECU) works closely with law enforcement and intelligence community partners to investigate and prosecute significant threats to the confidentiality, integrity, or availability of the FDIC's information systems, network, or data, and cyber crimes that may harm FDIC programs or operations and the Nation's banks. The ECU recognizes and adapts to emerging trends in the financial sector and is on the forefront to prevent fraud, waste, and abuse both internally and externally to the FDIC in the digital era. The ECU also conducts and provides effective and timely forensic accounting and digital evidence acquisition and analysis support for criminal investigative activity nationwide.

Since many of the programs in the 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 regularly coordinates with the supervisory and resolutions components within the FDIC to watch for developing patterns of crimes and other trends in light of the pandemic. Our Special Agents have been working proactively with other OIGs; USAOs; 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 169 such cases.

Notably, during the reporting period, the FDIC OIG's efforts related to the Federal government's COVID-19 pandemic response resulted in 51 criminal complaints, indictments, and informations; 35 arrests; and 28 convictions, involving fraud in the CARES Act Programs. Fines, restitution ordered, and asset forfeitures resulting from these cases totaled in excess of $54 million. Importantly, our Office's investments in data analytics have begun to enhance the efficiency of our audits, reviews, and investigations and will yield even greater dividends in the future. As one example, during the reporting period, data analytics efforts enabled direct support to several of our active criminal investigations of COVID-19 pandemic-related fraud, resulting in the identification of additional persons and business entities involved in the fraud scheme, as well as the uncovering of additional fraudulent loans.

Further, the OIG's data analytics effort is progressing in its collaboration with the 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 that will help to inform strategic planning within the OIG.

DOJ COVID-19 Fraud Enforcement Task Force (CFETF)

The FDIC OIG continues to support efforts of the task force as a key interagency partner for the Department of Justice. On March 10, 2022, IG Lerner and our Deputy AIGI attended a roundtable discussion with leadership from the member agencies and components of DOJ's CFETF. The roundtable was hosted by Attorney General Merrick Garland and focused on interagency collaboration and progress in identifying and fighting COVID-19-related fraud. The CFETF'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. During the roundtable, the Attorney General also announced the appointment of a Director for COVID-19 Fraud Enforcement to lead the department's criminal and civil enforcement efforts to combat COVID-19-related fraud, along with the latest results of criminal and civil enforcement actions that include alleged fraud related to over $8 billion in pandemic relief.

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 continued safety and soundness of the Nation's banks and help ensure integrity in the FDIC's programs and activities. Actions in cases involving COVID-19 relief fraud are also included in our discussion of cases from the reporting period.

First Person Charged for Fraudulently Seeking COVID Relief Business Loans Is Sentenced

On October 7, 2021, David Adler Staveley was sentenced to serve 56 months in Federal prison followed by 3 years of supervised release after pleading guilty to Conspiracy to Commit Bank Fraud and Failure to Appear in Court. Staveley was the first person in the country charged with fraudulently seeking forgivable pandemic relief small business loans guaranteed by the Small Business Administration (SBA) under the CARES Act. Staveley fled from prosecution after removing his electronic monitoring device and attempted to stage a suicide 3 weeks after being charged and appearing in U.S. District Court in May 2020. In order to further his ruse, Staveley left suicide notes with associates and left his wallet in his unlocked car that he parked along the ocean in Massachusetts. Further investigation determined that between May 26 and July 23, 2020, Staveley traveled to various states using false identities and stolen license plates. He was apprehended by the United States Marshals Service in Alpharetta, GA, on July 23, 2020.

Staveley and David Butziger conspired to file four fraudulent CARES Act Paycheck Protection Program (PPP) forgivable loan applications with a Rhode Island bank, falsely claiming they owned businesses with large monthly payrolls when, in fact, they did not own the businesses. Staveley admitted that as part of the scheme, he and Butziger filed fraudulent loan applications seeking $185,570 to pay employees at Top of the Bay restaurant in Warwick, RI; $144,050 for Remington House Inn restaurant in Warwick, RI; $108,777 for On The Trax restaurant in Berlin, MA; and $105,381 to pay employees at Dock Wireless, an unincorporated business. Staveley had no ownership interest in Top of the Bay, Remington House Inn, or On The Trax, which were closed at the time the loan applications were submitted and remain closed. Dock Wireless had no employees and no wages were ever paid by the business.

Source: USAO District of Rhode Island.
Responsible Agencies: FDIC OIG, FBI, Internal Revenue Service-Criminal Investigation (IRS-CI), and SBA OIG.
Prosecuted by the USAO, District of Rhode Island.

DC Solar Owner Sentenced to 30 Years in Prison for a Billion Dollar Ponzi Scheme

On November 9, 2021, Jeff Carpoff, owner of DC Solar, was sentenced to 30 years in prison and ordered to pay restitution of $790 million. Between 2011 and 2018, DC Solar manufactured mobile solar generator (MSG) units, which were solar generators that were mounted on trailers and were promoted as being able to provide emergency power to cellphone towers and lighting at sporting events. A significant incentive for investors was generous Federal tax credits due to the solar nature of the MSGs. The conspirators carried out an accounting and lease revenue fraud using Ponzi-like circular payments. Carpoff and others lied to investors about the market demand for DC Solar's MSGs and its revenue from leasing to third parties, then covered up these lies with techniques including false financial statements and fake lease contracts. Their fraud concealed a circular payment structure where Carpoff and others were simply using new investors' money to pay older investors the purported lease revenue that investors were expecting. As DC Solar lost vast sums of money with this fraudulent model, Carpoff and other conspirators stopped building the MSGs altogether, selling thousands of MSGs that did not even exist to investors. To carry out this part of the fraud, Carpoff and others made it appear that MSGs existed in locations that they did not, swapped vehicle identification number stickers on MSGs that had been built earlier, and attempted to deceive certain investors during equipment inspections. In reality, at least half of the approximately 17,000 MSGs claimed to have been manufactured by DC Solar did not exist. The fraud scheme resulted in investor losses totaling approximately $1 billion.

Source: USAO, Eastern District of California.
Responsible Agencies: FDIC OIG, FBI, and IRS-CI.
Prosecuted by the USAO, Eastern District of California, Sacramento.

Oklahoma Businessman Sentenced for Defrauding Multiple Financial Institutions and Fannie Mae in Mortgage Lending Scheme

On November 29, 2021, Ronald J. McCord was sentenced in the Western District of Oklahoma to serve 104 months in federal prison followed by 3 years of supervised release. McCord was ordered to pay $51,861,806 in restitution. On May 10, 2021, McCord pleaded guilty to three counts of bank fraud, one count of false statements to a financial institution, and one count of money laundering.

McCord was the Chairman and founder of First Mortgage Company, LLC (FMC), the largest independently owned mortgage lending and loan servicing company in Oklahoma. FMC had over $300 million in residential warehouse financing lines with subsidiaries of Citizens State Bank and SpiritBank. Beginning in the fall of 2016 through December 2017, FMC had drawn on its warehouse lines of credit with Citizens and SpiritBank to fund loans, then sold those loans to Fannie Mae, and resubmitted the loan documents to receive additional draws on its lines of credit. FMC also refinanced loans without sending payoff proceeds to the banks, drew on its warehouse line of credit to fund mortgages to borrowers, received payoffs from borrowers on the resulting loans that it serviced, and never repaid the banks. FMC also obtained loan funds from the banks for loans that never closed and failed to return the funds to the banks. Also, in December 2017, McCord authorized diversions from an escrow account for real estate taxes and mortgage insurance premiums which totaled approximately $28 million related to the sale of Mortgage Servicing Rights through Fannie Mae.

Source: USAO, Western District of Oklahoma.
Responsible Agencies: FDIC OIG, Federal Housing Finance Agency (FHFA) OIG, and FBI.
Prosecuted by the USAO, Western District of Oklahoma.

Former Chief Lending Officer of New Jersey Bank Sentenced

On December 1, 2021, James Bortolotti was sentenced to 18 months in prison, 3 years of supervised release, and ordered to pay $3.17 million in restitution for securing a federal guarantee on certain loans by making false statements to the SBA.

While serving as the chief lending officer of a New Jersey bank, Bortolotti became aware of a Small Business Administration lending program to incentivize lenders, including banks, to loan money to small businesses by providing a 75 percent SBA-backed guarantee on loans. When a lender applies for an SBA guarantee on a loan, the lender must disclose information related to the creditworthiness of the small business. Bank-1 hired a consulting firm to help the bank apply for SBA-backed guarantees.

On February 29, 2012, a consultant from the consulting firm submitted an application to the SBA for a guarantee of approximately $3.75 million on loans totaling approximately $5 million made to a small business located in Robbinsville, New Jersey. The application contained false information related to the creditworthiness of the business. Bortolotti knew the application contained false information, but he nevertheless reviewed and signed the application on behalf of the bank.

Source: USAO, District of New Jersey.
Responsible Agencies: FDIC OIG, SBA OIG, FHFA OIG, and FBI.
Prosecuted by the USAO, District of New Jersey.

Two Former Bank Employees Sentenced in Bank Embezzlement

On February 8, 2022, Raqeel Alsalam and Portia Jackson were sentenced in the U.S. Court for the District of South Carolina for their roles in an embezzlement scheme while employed as bank employees. Alsalam was sentenced to 1-month incarceration, 5 years of supervised release, and was ordered to pay $148,100 in restitution. Jackson was sentenced to time served, 5 years of supervised release, and was ordered to pay $94,493 in restitution.

On August 13, 2019, an internal bank audit of the bank's cash vault determined the individual drawers of tellers Alsalam and Jackson were short $27,000 and $67,000, respectively. The internal bank audit also revealed Alsalam embezzled 33 Social Security Administration (SSA) benefit deposits intended for an elderly customer account. The SSA benefits were direct deposited (via electronic funds transfer) to an account that was closed on September 23, 2016. Payments received between November 2016 and July 2019 were moved to the bank's Monthly NSF/Exceptions Report and were credited to the branch cash item account. Alsalam's duties required her to make contact with the accountholder to resolve the issues or return the money to SSA. However, bank records reflect Alsalam used her user ID number to convert the bank customer's SSA benefits each month to a cashier's check and then cash the checks written to the bank customer. Alsalam cashed 32 of the checks from her own teller window; 1 check was cashed through another teller's station, and Alsalam's name was noted on the transaction teller (transmittal) tape.

Source: The case was initiated based on a referral from the victim bank.
Participating Agencies: FDIC OIG, SSA OIG, and U.S. Secret Service.
Prosecuted by the USAO, District of South Carolina.

Extradited Fugitive Pleads Guilty to $20 Million Bank Fraud Scheme

On February 24, 2022, Ayreh Greenes pleaded guilty to a $20 million bank fraud scheme in U.S. District Court in Los Angeles, CA. Greenes was indicted on bank fraud charges in 2014 and subsequently fled to Israel. In September 2020, Israel's Supreme Court ruled that Greenes, a dual Israeli-American citizen, could be extradited back to the United States to stand trial. In March 2021, Greenes was extradited back to the United States from Israel.

Greenes was the purported Chief Financial Officer of Los Angeles, CA, based companies New Electronic Inc., Tech Club Inc., New Electronic Inc., and Tech Club Inc., which operated as wholesalers of consumer electronics, including televisions and DVD players. Greenes and his co-defendant, Aviv Mizrahi, the owner and Chief Executive Officer of New Electronic Inc., and Tech Club Inc., used false financial records over several years to obtain over $20 million in financing from financial institutions. The scheme to utilize false financial records included fraudulent accounts receivable aging reports and false inventory records resulting in over $20 million of loss to the financial institutions. The financial institutions relied on these records provided by Greenes and Mizrahi to fund the various lines of credit for New Electronic Inc., and Tech Club Inc., respectively.

Responsible Agencies: FDIC OIG and FBI.
Prosecuted by the USAO, Central District of California.

Bank Fraud and Embezzlement by Public Servant

On March 29, 2022, Trenna Trice was sentenced in the Middle District of Georgia to 2 years of imprisonment and 3 years of supervised release after having previously admitted to utilizing bank accounts at an FDIC-regulated financial institution to facilitate a scheme to steal money from charitable organizations and a local dental office. Trice, a Georgia school teacher, defrauded money from several victim charitable organizations, such as the United Negro College Fund (UNCF) and the Samarc Foundation in order to fund a personal gambling addiction. Trice was ordered to pay restitution of $162,044 to the UNCF, $7,784 to the Samarc Foundation, $70,231 to a Columbus, GA dentist's office, and $200 to the Georgia Dental Society. The total loss amount was $240,259.

Trice worked as a volunteer campaign coordinator for the Columbus, GA Branch of the UNCF from 2005 to 2017. The UNCF is an organization that funds scholarships for African American students and historically Black colleges and universities. During her tenure with the UNCF, Trice organized and fundraised for the annual Columbus Mayors Masked Ball, the primary fundraising activity for the UNCF. A review of bank records revealed that Trice stole $162,044 in donations and ticket sales intended for the UNCF.

Trice had also collected donations for a nonprofit organization known as SAMARC run by two former NBA basketball players who ran an annual basketball camp for underprivileged youth in the Columbus area. Trice diverted a total of $7,784 in donations and basketball game ticket sales intended for SAMARC to her own personal use. Further investigation also revealed that Trice had been terminated as an employee from a Columbus doctor's office because she had taken funds intended for the Georgia Dental Society, outstanding patient balances, business utilities, and charities totaling $70,231.

Responsible Agencies: FDIC OIG and FBI.
Prosecuted by the USAO, Middle District of Georgia.

Former Seattle Doctor Sentenced for Defrauding Pandemic Relief Programs

On March 8, 2022, Eric Ryan Shibley was sentenced to 4 years in prison, 3 years of supervised release, and ordered to pay $1,438,000 in restitution after being convicted of fraudulently seeking over $3.5 million in PPP and Economic Injury Disaster Loan (EIDL) COVID-19 relief funds. Shibley was convicted by a Federal jury on November 15, 2021, on wire fraud, bank fraud, and money laundering charges.

According to evidence presented at trial, Shibley, a former medical doctor, submitted 26 fraudulent PPP and 13 EIDL loan applications to Federally-insured financial institutions, other SBA approved lenders, and the SBA, in the names of businesses with no actual operations or by otherwise misrepresenting the business's eligibility. In the applications, Shibley falsified the number of employees and payroll expenses and concealed his own criminal history. To support the fraudulent applications, Shibley submitted fake tax documents and the names of purported employees who did not, in fact, work for the businesses for which Shibley claimed they worked. In Shibley's testimony, he claimed to operate his multiple business entities on an all cash basis outside the banking system. Specifically, Shibley claimed to have a $1 million monthly payroll in which he paid his 156 employees at multiple worksites, in cash, on a daily basis. Shibley provided financial institutions with a list of employees that included at least one individual who died in 1987. In total, Shibley received over $2.8 million in COVID-19 relief funds as a result of the fraud scheme.

Source: DOJ - Criminal Division, Fraud Section and USAO, Western District of Washington.
Responsible Agencies: FDIC OIG, SBA OIG, FBI, Health and Human Services OIG, Treasury Inspector General for Tax Administration, Homeland Security Investigations, and IRS-CI.
Prosecuted by the USAO, Western District of Washington, Seattle, and the DOJ - Criminal Division, Fraud Section.

Former Personal Banker Sentenced to 24 Months in Prison for Defrauding Elderly

On March 23, 2022, Randy Mack, a former personal banker, was sentenced to 24 months in prison followed by 24 months of supervised release in the Eastern District of Virginia. Mack was ordered to pay full restitution of $256,400 along with a $100 special assessment for his role in defrauding an elderly client while employed at a financial institution. As a result of his conviction, Mack was also barred from working in the banking industry in the future as part of his sentence.

From November of 2017, through December of 2020, Mack conducted 167 fraudulent over the counter withdrawals and 39 fraudulent ATM withdrawals totaling $256,400 from several accounts held by one of Mack's elderly banking clients. These transactions were done without the knowledge or authorization of the client to whom Mack had a fiduciary responsibility. Mack conducted unauthorized transfers from a line of credit the client held at the financial institution in order to help conceal the withdrawals. Mack also fraudulently obtained 11 ATM cards linked to the client's account to help facilitate the ATM withdrawals.

Source: This case was based on a referral from the Fairfax County Police Department.
Responsible Agencies: FDIC OIG.
Prosecuted by the USAO, Eastern District of Virginia.

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 the following areas:

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

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; Bergen County New Jersey Financial Crimes Association; Long Island Fraud and Forgery Association; Connecticut USAO Bank Secrecy Act Working Group; Connecticut U.S. Secret Service Financial Crimes Task Force; 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.
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.
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; Financial Investigative Team, Milwaukee, Wisconsin; 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.
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; PRAC Fraud Task Force; PRAC Law Enforcement Coordination Subcommittee; PRAC Data Analytics Subcommittee; CIGIE COVID-19 Working Group; DOJ Stimulus Funds Fraud Working Group; District of Maryland SAR Review Task Force; Western District of Virginia SAR Review Task Force, Roanoke, Virginia; Western District of Virginia SAR Review Task Force, Abingdon, Virginia; Eastern District of Virginia SAR Review Task Force; Central Eastern District of Virginia SAR Review Task Force; Northern Virginia Eastern District of Virginia SAR Review Task Force; DOJ Foreign Corrupt Practices Act SAR Initiative; District of Columbia SAR Review Task Force; Southern District of West Virginia SAR Review Task Force; Northern District of West Virginia SAR Review Task Force.
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 former Chairman, FDIC Director and now Acting Chairman, other FDIC Board Members, Chief Operating Officer, Chief Financial Officer, and other senior FDIC officials through the IG's and senior OIG leadership's regularly scheduled meetings with them and through other forums. Attended FDIC Board Meetings and certain other senior-level management meetings to monitor or discuss emerging risks at the Corporation and tailor OIG work accordingly.
- Coordinated with the FDIC Acting Chairman, in his capacity as Chairman of the FDIC Audit Committee, to provide status briefings and present the results of completed audits, evaluations, and related matters for his and other Committee members' consideration. Presented the results of OIG audits, evaluations, and other reviews at monthly 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.
- Posted video summaries of OIG-issued audit and evaluation reports on our external website to provide stakeholders an additional opportunity to learn about the work of the OIG and the findings and recommendations our auditors and evaluators have made to improve FDIC programs and operations. These included our work on Whistleblower Rights and Protections for FDIC Contractors, Sharing of Threat Information to Guide the Supervision of Financial Institutions, and Supply Chain Risk Management. Also posted a video summary of our report on the Top Management and Performance Challenges Facing the FDIC.
- Coordinated with DOJ and USAOs throughout the country in the issuance of press releases announcing results of cases with FDIC OIG involvement and informed the former Chairman and FDIC Director and now Acting Chairman 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; monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the FDIC's Office of Legislative Affairs on any Congressional correspondence pertaining to the OIG. Briefed Minority staff from the House Financial Services Committee and Minority staff from the Senate Banking, Housing, and Urban Affairs Committee on the OIG's identification of the Top Management and Performance Challenges Facing the FDIC.

- 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 new web-based hotline portal at https://www.fdicoig.gov/oig-hotline integrates seamlessly with our electronic investigations 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. Updated the OIG's Hotline poster to better inform stakeholders on what to report and how.

- Supported the IG community by attending monthly CIGIE meetings and other meetings, such as those of the CIGIE Legislation Committee (of which the IG is the Vice Chair); the Diversity, Equity, Inclusion, and Accessibility (DEIA) Working Group (of which the IG is the Vice Chair); Audit Committee; Inspection and Evaluation Committee, Technology Committee; Investigations Committee; Professional Development Committee; Assistant IGs for Investigations; Assistant IGs for Management; and Council of Counsels to the IGs; responding to multiple requests for information on IG community issues of common concern; and commenting on various legislative matters through CIGIE's Legislation Committee.

- Supported efforts of the PRAC through active participation in its meetings, forums, and work groups and by playing a key role in collaboration with law enforcement partners in investigations of fraud in pandemic-relief programs. Also continued to adopt features of the PRAC's Agile Product Toolkit to provide our stakeholders a means of receiving more expedient information on results of oversight efforts, for example to convey emerging concerns identified during audits and evaluations.

- Participated on the Council of Inspectors General on Financial Oversight (CIGFO), as established by the Dodd-Frank Wall Street Reform and Consumer Protection Act, and coordinated with the IGs on that Council. This Council facilitates sharing of information among CIGFO member Inspectors General and discusses ongoing work of each member IG as it relates to the broader financial sector and ways to improve financial oversight.
- Shared information about the FDIC OIG on Federal News Network's "The Search for Accountability." The FDIC IG was interviewed regarding the oversight role of the OIG at the FDIC. During his interview, IG Lerner discussed our mission and the work of our Office, including summaries of some of our most recent audits and evaluations, and recent results from of our criminal investigations across the country.
- Participated in a panel discussion hosted by the Department of Veterans Affairs OIG on "DE&I Practices that Foster Community and High-Performance." IG Lerner was a panelist discussing ideas, innovations, challenges, successes, and the positive impact of sound Diversity, Equity, & Inclusion practices.
- Participated in a panel discussion on DEIA in the Federal Government, as part of the Association of Government Accountants' Spring Training session. IG Lerner joined the panel to discuss ongoing DEIA initiatives and navigating the DEIA landscape as an Inspector General.
- Produced and posted a video on our external website highlighting the work of the OIG's Office of Investigations as it conducts cases throughout the country to uncover financial fraud and help preserve the integrity of the banking sector.
- Participated in the FDIC's 15th Annual FDIC Accounting and Auditing Conference. The FDIC IG moderated a discussion by the Executive Director of the PRAC and SBA IG on *Fighting Fraud and Auditing in the Federal Pandemic Response*. The AIG for AEC and an AEC Program Manager spoke about The Independent *Audit and Evaluation Oversight Function at the FDIC*. This latter presentation included a brief history of the IG concept, the goals of AEC, FDIC Management and Performance Challenges, steps in the audit process, quality assurance efforts, standards guiding AEC's work, and highlights of recent reports.
- Issued two advisories reminding financial institutions and depositors to remain vigilant against cyberattacks, including recent information about steps to take to mitigate, prevent, and respond to cyber incidents.

- Communicated with the Government Accountability Office (GAO) on ongoing efforts related to our oversight roles and issues and assignments of mutual interest.
- Coordinated with the Office of Management and Budget to address matters of interest related to our FY 2022 budget and proposed budget for FY 2023.
- Worked closely with representatives of the DOJ, including the Main Justice Department, FBI, and USAOs, to coordinate our criminal investigative work and pursue matters of mutual concern. Joined law enforcement partners in numerous financial, mortgage, suspicious activity report review, cyber fraud, and PRAC-related working groups nationwide.
- Promoted transparency to keep the American public informed through four main means: the FDIC OIG website to include, for example, summaries of completed work, 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; external video summaries of report findings; 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.
- Increased transparency of our work 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 (108 as of March 31, 2022) and those recommendations that have been closed.
- Gave a class lecture on the *Role of the Inspectors General* for the Missouri School of Journalism. FDIC OIG AIG for Audits, Evaluations, and Cyber discussed the mission of Federal Inspectors General; IG reporting requirements; audits, evaluations, inspections, and investigations components of IG offices; interagency coordination in the CIGIE community; and the audit and evaluation process of the FDIC OIG.
- Conducted outreach to stakeholders interested in our investigative operations, including through presentations by OIG investigative staff – for example through a training session on Cryptocurrency and the U.S. Financial System at the GAO/CIGIE 2022 Coordination Meeting. The presentation covered blockchain, types of cryptocurrencies, the cryptocurrency address investigation process, virtual asset service providers, and types of cryptocurrency exchanges.

Administering resources prudently, safely, securely, and efficiently.

- Developed spending and hiring plans to make optimum use of the OIG's FY 2022 enacted funding of $46.5 million. Finalized our request for $47.5 million in FY 2023. Full funding of the OIG request will enable us to make investments in data analytics and IT infrastructure that will have long-term benefits to the efficiency of the OIG and FDIC, as well as provide the OIG with the ability to rapidly respond to any changes in economic conditions and the stability of the banking sector.
- Formulated two OIG policies outlining the flexibilities available in the hybrid OIG work environment: the Flexible Work Options Program, and Work Schedules and Hours of Duty policies. These policies are designed to provide flexibility for OIG employees to accomplish the mission and support work-life balance as our Office enters Phase 2 of the Return to Office Plan.
- Continued pursuing component office Implementation Plans designed to achieve the OIG's Strategic Goals, Guiding Principles, and Vision for 2022.
- 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 (OIT) strategic plan and IT Road Map for 2021-2023, 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.
- Implemented the FDIC OIG's Information Management System (IMS), a new electronic case management system that replaces the predecessor electronic/paper file system and modernizes the OIG's investigative business practices. The new system automates business flows and includes electronic supervisory notifications and approvals, as well as an online evidence inventory. Another enhancement of the new system is the new Hotline portal. Complainants and whistleblowers can now fill out a new intake form that captures information and intake of complaints directly into IMS for assessment by the Hotline team. The new Hotline portal link is accessible on the OIG's website.

- Worked to stand up a new audit management platform that will allow AEC to perform its work efficiently and effectively. Staff will be trained on how to use the system consistently, and AEC and OIT will ensure that the system provides AEC staff with useful information for dashboarding and reporting.
- Entered the final implementation stage of build-out of the OIG's Electronic Crimes Unit's laboratory. The laboratory will allow field Agents to remotely access a server-based lab environment which will allow for the storage and processing of digital evidence into forensic reviewable data. This capability will greatly increase the efficiency and effectiveness of the investigative process by allowing for much quicker actuation of data into e-discovery platforms.
- Continued work of our multi-disciplinary Data Analytics Team of auditors, criminal investigators, and information technology professionals 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. This team made strides in efforts to: (1) identify data access needs and potential sources of new data in support of our work; (2) identify, pilot, and bring online the infrastructure and analytical tools needed for our auditors, investigators, and related professional staff; and (3) identify and build the necessary internal capacity to support proactive data analytics initiatives through training, talent recruitment, and strategic organizational planning for the future.
- Made progress on the OIG's data analytics project on Paycheck Protection Program fraud through collaboration with the Pandemic Response Accountability Committee, the FDIC, the Financial Crimes Enforcement Network, the Department of Justice, the Federal Bureau of Investigation, and private sector entities.
- Enhanced and 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.
- Maintained the "Helpful Resources During Pandemic" collaboration site for all of OIG, as a means to provide continuous updates on the pandemic and offer helpful information resources to OIG staff as the Office continued to operate under mandatory telework conditions and then prepared for Phase 2 of a Return to Office.
- Published *In the Know*—a bi-monthly 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 employee leave and telework policies, personnel benefits, administrative guidance, IT system updates, 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. Continued to move all policies to a central SharePoint site for easier access and updating capabilities.
- 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 Deputy Assistant Inspector General (DAIG) for Investigations, DAIG for AEC, Budget 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 use of MS Teams throughout our Office to promote virtual collaboration and communication, particularly during the period of the pandemic when mandatory telework for our Office was in place.
- Collaborated with the U.S. Postal Service OIG and CIGIE personnel to update and migrate the OIG's external website –fdicoig.gov – to the Oversight.gov platform, a move designed to achieve economy and effectiveness.

Exercising leadership skills and promoting teamwork.

- Held two Town Hall events for OIG staff to maintain a sense of community and foster teamwork. At the first Town Hall, the IG gave a brief update about the status of our Office's Return to Office plan, and the Office of Investigations field leadership introduced themselves and their teams, and provided highlights of their investigative operations. At the winter Town Hall event, leadership and managers from AEC discussed their accomplishments and ongoing work, and the Workforce Council discussed updates on planned initiatives.
- Produced and shared with all OIG staff *OIG Vision 2022: Unlock the Potential*, a video that lays out a vision for the Office to help achieve four main goals: Strategic Implementation, Proactive Innovation, Professional Development, and Building a Community Within the OIG. The video highlights how the day-to-day activities of each OIG employee align with our goals and contribute to the success of the whole organization.
- Maintained the OIG's Intranet site to promote teamwork by having the page launch as the opening home page for OIG staff and expanded content to include cross-cutting information of interest to staff.
- Continued biweekly OIG senior leadership meetings to affirm the OIG's unified commitment to the FDIC OIG mission and to strengthen working relationships and coordination among all FDIC OIG offices.
- Supported efforts of the Workforce Council as that group explored issues relating to the OIG's eventual Return to Office.
- Hosted the first "Day in the Life" of an IG Executive series, organized by the OIG Workforce Council, where our OIG executives informally discuss their daily work routines and interactions with staff, so that OIG staff gain a fuller understanding of OIG leadership priorities, challenges, and successes.
- 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 monthly *OIG Connection* newsletters, *In the Know* publications, and other communications.
- Enrolled OIG staff in several different FDIC and CIGIE Leadership Development Programs to enhance their leadership capabilities and promoted leadership through several mentoring pairings of senior OIG staff with more junior staff in the OIG.

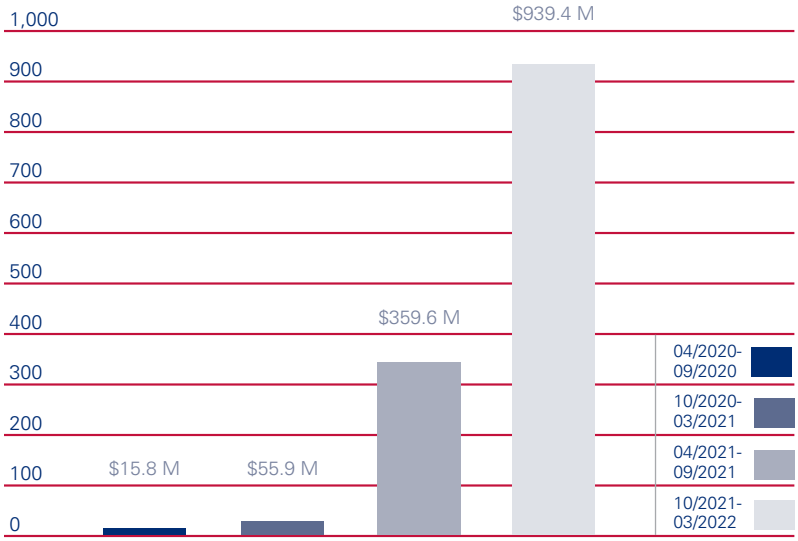
- Held the OIG's Distinguished Achievements Award Ceremony to recognize OIG staff in seven award categories: Leadership, Innovation, Business Support, Championing Diversity and Inclusiveness, Collaboration, New Staff Members, and the IG Awards for Excellence. Also used the occasion to celebrate career milestones and welcome 22 new staff members. Continued the OIG's ongoing awards and recognition program for staff across all component offices to acknowledge their individual and team contributions to the Office.
- Organized several activities, including a virtual Holiday celebration, Coffee Chats, a Guess Who in '22 presentation, and a Workforce Council-sponsored Let's Move Health and Wellness Challenge to promote community, teamwork, and collegiality among OIG staff.
- Implemented the OIG's 2022 Fellows Program for non-supervisory employees at the junior and senior levels to participate. Selected four OIG staff for the inaugural session. The program is designed to enhance fellows' understanding of the workings of all components of the OIG and the essential qualities for effective leadership.
- Held training sponsored by the Arbinger Group for all of AEC and others 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, and planned additional sessions to include staff from other component offices.
- Administered a survey instrument to members of our investigative staff to gauge team dynamics and effectiveness and establish a baseline that can be useful in highlighting areas of strength and opportunities for improvement.
- Assisted in organizing the 8th Annual CIGIE Leadership Forum: *The Digital Frontier: Engaging People, Navigating Change, and Leveraging Data*. This forum featured remarks from individuals from a wide variety of OIGs who shared their professional expertise with others in the IG community.
- Took a leadership role in a new working group on behalf of CIGIE's Audit and Inspection and Evaluation Committees related to Monetary Impact. The FDIC OIG AIG for AEC and an Audit/Evaluation Manager are leading a group comprised of representatives from 19 OIGs across the community. The purpose of the group is to assess how OIGs report and track monetary impacts from audits and evaluations. Also participated as a member of CIGIE's Connect, Collaborate, and Learn group. This working group holds technical training sessions for auditors and evaluators. The AIG for AEC moderated a session on IT audits.
- Carried out monthly coordination meetings for audit, evaluation, and investigation leadership to better communicate, coordinate, and maximize the effectiveness of ongoing work.

- 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 (ELO) throughout the OIG to promote employee engagement, career development, and a positive workplace culture. The ELO provided training on the Neuroscience of Group Dynamics; arranged training from the NeuroLeadership Institute and Arbinger Group; and offered ELO 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 of the OIG's DEIA Working Group. Added new members to the group and hosted a series of events to highlight diversity, including a roundtable discussion with OIG staff to provide them an opportunity to share feedback and ideas for 2022 DEIA activities; presentations by the National President of Blacks in Government, who spoke on the Life and Legacy of Dr. Martin Luther King, Jr.; AbilityOne Vice Chair, who highlighted the benefits of hiring employees with disabilities and the mechanisms available to Federal agencies to do so; a Lieutenant Colonel and West Point graduate who shared his experiences as a leader in the military and practices in the Army to promote diversity, equity, and inclusion; and a panel of women leaders in the law enforcement community, moderated by the Special Agent in Charge of our Chicago Regional Office.
- Continued active involvement in CIGIE's DEIA Work Group, of which the FDIC IG is Vice Chair. Assisted in issuing the inaugural issue of *The Ally* newsletter to share information from the Work Group, which works to affirm, advance, and augment CIGIE's commitment to promote a diverse, equitable, and inclusive workforce and workplace environment throughout the IG Community. Also participated in CIGIE's DEIA Virtual Huddle, on which the Chair of the FDIC OIG's DEIA Working Group was a panelist. Topics included: the Evolution of DEIA; DEIA in the Workplace; and Leading DEIA from Where You Are.
- Continued our leadership role in the CIGFO joint working group on Crisis Readiness. The OIG's Assistant IG for AEC served as co-lead of the effort to compile forward-looking guidance for the Financial Stability Oversight Council and its members to consider in preparing for crises.
- Led efforts of the PRAC's Law Enforcement Coordination Subcommittee. Our Deputy 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.

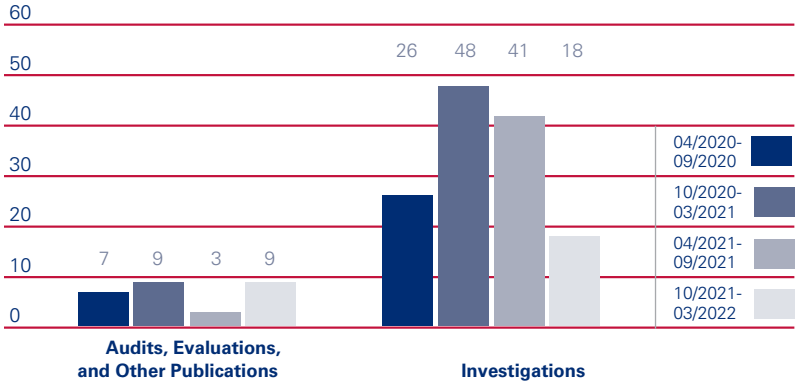
Cumulative Results (2-year period)

Nonmonetary Recommendations	
April 2020 – September 2020	44
October 2020 – March 2021	56
April 2021 – September 2021	12
October 2021 – March 2022	77

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



Products Issued and Investigations Closed



Reporting Requirements

Index of Reporting Requirements - Inspector General Act of 1978, as amended

Reporting Requirements (continued)	Page
Section 5(a)(10): Summary of each audit, inspection, and evaluation report issued before the commencement of the reporting period for which:	
• no management decision has been made by the end of the reporting period	55
• no establishment comment was received within 60 days of providing the report to management	55
• there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.	45-51
Section 5(a)(11): Significant revised management decisions during the current reporting period.	55
Section 5(a)(12): Significant management decisions with which the OIG disagreed.	55
Section 5(a)(14, 15, 16): An appendix with the results of any peer review conducted by another OIG during the period or if no peer review was conducted, a statement identifying the last peer review conducted by another OIG.	58-59
Section 5(a)(17): Statistical tables showing, for the reporting period:	
• number of investigative reports issued • number of persons referred to the DOJ for criminal prosecution • number of persons referred to state and local prosecuting authorities for criminal prosecution • number of indictments and criminal Informations.	55
Section 5(a)(18): A description of metrics used for Section 5(a)17 information.	55
Section 5(a)(19): A report on each OIG investigation involving a senior government employee where allegations of misconduct were substantiated, including:	
• the facts and circumstances of the investigation; and • the status and disposition of the matter, including if referred to the DOJ, the date of referral, and the date of DOJ declination, if applicable.	56
Section 5(a)(20): A detailed description of any instance of Whistleblower retaliation, including information about the official engaging in retaliation and what consequences the establishment imposed to hold the official responsible.	56
Section 5(a)(21): A detailed description of any attempt by the establishment to interfere with OIG independence, including with respect to budget constraints, resistance to oversight, or restrictions or delays involving access to information.	56
Section 5(a)(22): A detailed description of each OIG inspection, evaluation, and audit that is closed and was not disclosed to the public; and OIG investigation involving a senior government employee that is closed and was not disclosed to the public.	56

Appendix 1

Information Required by the Inspector General Act of 1978, as Amended

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. Inspector General Lerner is Vice Chair of the Council of the Inspectors General on Integrity and Efficiency's Legislation Committee. Much of the FDIC OIG's activity reviewing legislation and regulation occurs in connection with that Committee.

The CIGIE Legislation Committee provides timely information to the IG community about congressional initiatives; solicits the technical advice of the IG community in response to congressional initiatives; and presents views and recommendations to Congress and the Office of Management and Budget on legislative matters. The Legislation Committee seeks to provide technical assistance on legislative proposals that enhance the work of the IG community and ensure the independence of IGs and effective oversight of all Federal programs and spending.

During the semiannual period, the Legislation Committee provided input on proposed legislation to enhance IG independence and authorities, which included CIGIE legislative priorities such as Vacancies Act reform, testimonial subpoena authority, and notification to Congress if an IG is placed on non-duty status. FDIC OIG was a leader on another CIGIE legislative priority, ensuring that oversight of ongoing activities continues during any government shutdown, and we advised Congressional staff on proposed legislation.

Table I: Significant Recommendations from Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed

This table shows the corrective actions management has agreed to implement but has not completed, along with any associated monetary amounts. In some cases, these corrective actions may be different from the initial recommendations made in the audit or evaluation reports. However, the OIG has agreed that the planned actions meet the intent of the initial recommendations. The information in this table is based on (1) information supplied by the FDIC's Office of Risk Management and Internal Controls and (2) the OIG's determination of when a recommendation can be closed. The FDIC has categorized the status of these recommendations as follows:

Management Action in Process: (three recommendations from three reports)

Management is in the process of implementing the corrective action plan, which may include modifications to policies, procedures, systems or controls; issues involving monetary collection; and settlement negotiations in process.

Report Number, Title, and Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
Management Action in Process		
EVAL-20-001 **Contract Oversight Management** October 28, 2019	**2**	The FDIC developed a report to capture key data that will enhance the analyses and reporting to support the contracting program. Additional changes have since been made to the data in the report and to its format based on feedback received. The FDIC is assessing the need to add any additional information to the report.
AUD-20-003 **The FDIC's Privacy Program** December 18, 2019	**3**	The FDIC began a process in 2019 to ensure privacy plans are developed and approved for all systems containing personally identifiable information. The FDIC will fully implement this process over a 3-year period, with priority for new and changing authorizations over the next year.
EVAL-21-002 **Critical Functions in FDIC Contracts** March 31, 2021	**10**	The FDIC will consider and further study potential methodologies for assessing contractor overreliance, including how other agencies make such determinations. Based on its study, the FDIC will provide guidance to divisions and offices for assessing the potential for contractor overreliance and maintaining Federal control of essential functions or those necessary during a business continuity event.

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-17-001 **Audit of the FDIC's Information Security Program - 2016** November 2, 2016	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct a performance audit to evaluate the effectiveness of the FDIC's information security program and practices. This work is conducted in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). C&C found that the FDIC had established a number of information security program controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable National Institute of Standards and Technology standards and guidelines. However, C&C described security control weaknesses that impaired the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at elevated risk. C&C reported on 17 findings, of which 6 were identified during the current year FISMA audit and the remaining 11 were identified in prior OIG or Government Accountability Office reports. These weaknesses involved: strategic planning, vulnerability scanning, the Information Security Manager Program, configuration management, technology obsolescence, third-party software patching, multi-factor authentication, contingency planning, and service provider assessments. The report contained six new recommendations addressed to the Chief Information Officer to improve the effectiveness of the FDIC's information security program and practices.	6	1	NA
AUD-20-001 **The FDIC's Information Security Program - 2019** October 23, 2019	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct this audit. The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. C&C found that the FDIC established a number of information security program controls and practices that complied or were consistent with FISMA requirements and Federal information security policy, standards, and guidelines. However, C&C identified weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. C&C concluded that the FDIC's overall information security program was operating at a Maturity Level 3 (Consistently Implemented). The report contained three recommendations intended to ensure that (i) employees and contractor personnel properly safeguard sensitive electronic and hardcopy information and (ii) network users complete required security and privacy awareness training.	3	1	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-20-001 **Contract Oversight Management** October 28, 2019	The FDIC relies heavily on contractors for support of its mission, especially for information technology, receivership, and administrative support services. Over a 5-year period from 2013 to 2017, the FDIC awarded 5,144 contracts valued at $3.2 billion. Our evaluation objective was to assess the FDIC's contract oversight management, including its oversight and monitoring of contracts using its contracting management information system, the capacity of Oversight Managers (OM) to oversee assigned contracts, OM training and certifications, and security risks posed by contractors and their personnel. We concluded that the FDIC must strengthen its contract oversight management. Specifically, we found that the FDIC was overseeing its contracts on a contract-by-contract basis rather than a portfolio basis and did not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency. We also found that the FDIC's contracting files were missing certain required documents, personally identifiable information was improperly stored, some OMs lacked workload capacity to oversee contracts, and certain OMs were not properly trained or certified. The report contained 12 recommendations to strengthen contract oversight.	12	1	NA
AUD-20-003 **The FDIC's Privacy Program** December 18, 2019	The audit objective was to assess the effectiveness of the FDIC's Privacy Program and practices. We assessed effectiveness by determining whether the FDIC's Privacy Program controls and practices complied with selected requirements defined in eight of the nine areas covered by OMB Circular A-130. The significant amount of personally identifiable information held by the FDIC underscores the importance of implementing an effective Privacy Program that ensures proper handling of this information and compliance with privacy laws, policies, and guidelines. OMB Circular A-130, Managing Information as a Strategic Resource (OMB Circular A-130), organizes relevant privacy-related requirements and responsibilities for Federal agencies into nine areas. We found that the Privacy Program controls and practices we assessed were effective in four of eight areas examined. However, privacy controls and practices in the remaining four areas were either partially effective or not effective. The report contained 14 recommendations intended to strengthen the effectiveness of the FDIC's Privacy Program and records management practices.	14	3	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-20-003 **Cost Benefit Analysis Process for Rulemaking** February 4, 2020	The FDIC OIG conducted an evaluation of the FDIC's Cost Benefit Analysis Process for Rulemaking. Through the Banking Act of 1933, Congress provided the FDIC with the authority to promulgate rules to fulfill the goals and objectives of the Agency. A cost benefit analysis informs the agency and the public whether the benefits of a rule are likely to justify the costs, or determines which of various possible alternatives is most cost effective. Our evaluation objective was to determine if the FDIC's cost benefit analysis process for rules was consistent with best practices. We found that the FDIC's cost benefit analysis process was not consistent with widely recognized best practices identified by the OIG. Specifically, we found that the FDIC had not established and documented a process to determine when and how to perform cost benefit analyses. We also found that the FDIC did not leverage the expertise of its Regulatory Analysis Section economists during initial rule development; did not require the Chief Economist to review and concur on the cost benefit analyses performed, which is an important quality control; was not always transparent in its disclosure of cost benefit analyses to the public; and did not perform cost benefit analyses after final rule issuance. The report contained five recommendations to improve the FDIC's cost benefit analysis process.	5	5	NA
EVAL-20-004 **The FDIC's Readiness for Crises** April 7, 2020	The FDIC OIG conducted an evaluation of the FDIC's Readiness for Crises. We initiated this evaluation in 2018, and it covered the FDIC's readiness planning and preparedness activities up to early 2019. Our work was not conducted in response to the current pandemic situation, nor was the report specific to any particular type of crisis. Effective crisis readiness plans and activities can help the FDIC support the safety and soundness of insured depository institutions, as well as the stability and integrity of the Nation's banking system. Our evaluation objective was to assess the FDIC's readiness to address crises that could impact insured depository institutions. We identified best practices that could be used by the FDIC. Our review of these best practices identified seven important elements of a crisis readiness framework that are relevant to the FDIC – (i) Policy and Procedures; (ii) Plans; (iii) Training; (iv) Exercises; (v) Lessons Learned; (vi) Maintenance; and (vii) Assessment and Reporting. We reported that the FDIC should fully establish these seven elements of a readiness framework to address crises that could impact insured depository institutions. The report contained 11 recommendations to improve the FDIC's crisis readiness planning.	11	1	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-21-001 **The FDIC's Information Security Program – 2020** October 27, 2020	The FDIC OIG engaged the professional services firm of Cotton & Company LLP to conduct this audit. The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. Applying the FISMA metrics, the FDIC's overall information security program was operating at a Maturity Level 3 (Consistently Implemented). The FDIC established a number of information security program controls and practices that were consistent with FISMA requirements and Federal information security policy, standards, and guidelines. However, the FISMA report identified weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. The report contained eight recommendations intended to improve the effectiveness of the FDIC's information security program and practices.	8	3	NA
AUD-21-002 **Governance of the FDIC's Mobile Device Management Solution** December 21, 2020	The FDIC relies heavily on smartphones and tablets to support its business operations and communications. The FDIC uses a cloud-based mobile device management (MDM) solution to secure and manage these mobile devices. We conducted an audit to assess the adequacy of the FDIC's governance over a proposed MDM solution. We found that the FDIC's Chief Information Officer Organization did not identify elevated and growing risks associated with the project; resolve security concerns identified by the Office of the Chief Information Security Officer prior to procuring the proposed MDM solution; or establish roles and responsibilities for managing the use of Limited Authorizations to Operate. Further, the FDIC's Acquisition Services Branch did not engage the Legal Division to review the procurement of the proposed MDM solution, consistent with FDIC guidance. The report contained five recommendations intended to strengthen the FDIC's processes and governance for evaluating, authorizing, and procuring new technologies.	5	1	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
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	2	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-21-002 **Critical Functions in FDIC Contracts** March 31, 2021	The FDIC relies on contractors to provide services in support of its mission. Some of these services cover Critical Functions. We conducted an evaluation to determine whether one of the FDIC's contractors was performing Critical Functions as defined by guidance issued by the 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 II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods (continued)

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-21-004 **Security and Management of Mobile Devices** August 3, 2021	The FDIC deploys nearly 4,600 smartphones and more than 150 tablets to its employees and contractor personnel to support its business operations and communications. Although these mobile devices offer opportunities to improve business productivity, they also introduce the risk of cyber threats that could compromise sensitive FDIC data. The FDIC must implement proper controls to ensure that it effectively manages its inventory of mobile devices and the associated expenditures. We conducted an audit to determine whether the FDIC had established and implemented effective controls to secure and manage its mobile devices. We engaged the professional services firm of Cotton & Company LLP to conduct the audit. The audit found that the FDIC had not established or implemented effective controls to secure and manage its mobile devices in three of nine areas assessed, because the controls and practices did not comply with relevant Federal or FDIC requirements and guidance. The report contained nine recommendations intended to strengthen the FDIC's controls and practices for securing and managing its mobile devices.	9	5	NA
AEC-21-002 **The FDIC's Management of Employee Talent** September 1, 2021	We 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 (SME) were consistent with relevant OIG-identified criteria and (2) the FDIC's process for allocating examination staff and SMEs 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 SMEs and its process for allocating examination staff and SMEs 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 we issued a Memorandum to advise 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	3	NA

Table III: Audit and Evaluation Reports Issued by Subject Area

Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	**Title**	**Total**	**Unsupported**	
Supervision				
EVAL-22-002 December 1, 2021	*Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders*			
Information Technology and Cybersecurity				
AUD-22-001 October 27, 2021	*The FDIC's Information Security Program - 2021*			
AUD-22-002 November 3, 2021	*The FDIC's Compliance under the Digital Accountability and Transparency Act of 2014*			
EVAL-22-001 November 22, 2021	*Reliability of Data in the FDIC Virtual Supervisory Information on the Net System*			
AUD-22-003 January 18, 2022	*Sharing of Threat Information to Guide the Supervision of Financial Institutions*			
Resource Management				
REV-22-001 January 4, 2022	*Whistleblower Rights and Protections for FDIC Contractors*			
EVAL-22-003 March 1, 2022	*The FDIC's Implementation of Supply Chain Risk Management*			
REV-22-002 March 16, 2022	*Controls Over Payments to Outside Counsel*			
Totals for the Period		**$0**	**$0**	**$0**

Table IV: Audit and Evaluation Reports Issued with Questioned Costs

	Number	Questioned Costs	
		Total	Unsupported
A. For which no management decision has been made by the commencement of the reporting period.	0	$0	$0
B. Which were issued during the reporting period.	0	$0	$0
Subtotals of A & B	**0**	**$0**	**$0**
C. For which a management decision was made during the reporting period.	0	$0	$0
(i) dollar value of disallowed costs.	0	$0	$0
(ii) dollar value of costs not disallowed.	0	$0	$0
D. For which no management decision has been made by the end of the reporting period.	0	$0	$0
Reports for which no management decision was made within 6 months of issuance.	0	$0	$0

Table V: Audit and Evaluation Reports Issued with Recommendations for Better Use of Funds

	Number	Dollar Value
A. For which no management decision has been made by the commencement of the reporting period.	0	$0
B. Which were issued during the reporting period.	0	$0
Subtotals of A & B	**0**	**$0**
C. For which a management decision was made during the reporting period.	0	$0
(i) dollar value of recommendations that were agreed to by management.	0	$0
- based on proposed management action.	0	$0
- based on proposed legislative action.	0	$0
(ii) dollar value of recommendations that were not agreed to by management.	0	$0
D. For which no management decision has been made by the end of the reporting period.	0	$0
Reports for which no management decision was made within 6 months of issuance.	0	$0

Table VI: Status of OIG Recommendations Without Management Decisions
During this reporting period, there were no recommendations more than 6 months old without management decisions.

Table VII: Status of OIG Reports Without Comments
During this reporting period, there were no reports for which comments were received after 60 days of issuing the report.

Table VIII: Significant Revised Management Decisions
During this reporting period, there were no significant revised management decisions.

Table IX: Significant Management Decisions with Which the OIG Disagreed
During this reporting period, there were no significant management decisions with which the OIG disagreed.

Table X: Instances Where Information Was Refused
During this reporting period, there were no instances where information was refused.

Table XI: Investigative Statistical Information

Number of Investigative Reports Issued	18
Number of Persons Referred to the Department of Justice for Criminal Prosecution	60
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	1
Number of Indictments and Criminal Informations	69

Note: Description of the metrics used for the above information: Reports issued reflects case closing memorandums issued to FDIC management. With respect to the 60 referrals to DOJ, the total represents 59 individuals, no business entities, and 1 case where the subject is unknown at present. Our total indictments and criminal informations includes indictments, informations, and superseding indictments, as applicable.

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

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

Table XIII: Instances of Whistleblower Retaliation

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

Table XIV: Instances of Agency Interference with OIG Independence

During this reporting period, there were no attempts to interfere with OIG independence.

Table XV: OIG Inspections, Evaluations, and Audits That Were Closed and Not Disclosed to the Public; and Investigations Involving Senior Government Employees That Were Closed and Not Disclosed to the Public

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

Appendix 2

Information on Failure Review Activity

(Required by the Dodd-Frank Wall Street Reform and Consumer Protection Act)

FDIC OIG Review Activity for the Period October 1, 2021 through March 31, 2022 (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 National Aeronautics and Space Administration (NASA) OIG conducted a peer review of the FDIC OIG's audit organization and issued its report on the peer review on November 25, 2019. NASA OIG found the system of quality control for the FDIC OIG's Office of Program Audits and Evaluations and Office of Information Technology Audits and Cyber in effect for the period April 1, 2018, through March 31, 2019, to be suitably designed and implemented as to provide reasonable assurance that the audit organization's performance and reporting was in accordance with applicable professional standards in all material respects. NASA OIG's review determined the FDIC OIG should receive a rating of Pass.

NASA OIG communicated additional findings that required attention by FDIC OIG management but were not considered to be of sufficient significance to affect NASA OIG's opinion expressed in its peer review report.

This peer review report is posted on our website at www.fdicoig.gov.

Note: The Department of State OIG initiated an external peer review of our audit organization in April 2022 and expects to issue its results by September 30, 2022.

Inspection and Evaluation Peer Reviews

A CIGIE External Peer Review Team conducted a peer review of our Office of Program Audits and Evaluations (PAE) (recently re-named Audits, Evaluations, and Cyber) and issued its report on June 3, 2021. Members of the peer review team included participants from the Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection OIG, the U.S. Department of Education OIG, and the U.S. Nuclear Regulatory Commission OIG.

The team conducted the review in accordance with the CIGIE Inspection and Evaluation Committee guidance contained in the *CIGIE Guide for Conducting Peer Reviews of Inspection and Evaluation Organizations of Federal Offices of Inspector General* (Blue Book) issued in January 2017. The team assessed PAE's compliance with seven standards in CIGIE's Quality Standards for Inspection and Evaluation, issued in January 2012: quality control, planning, data collection and analysis, evidence, records maintenance, reporting, and follow-up.

The report found that PAE's policy and procedures sufficiently addressed the seven Blue Book Standards and that all three reports that the team reviewed met the standards and also complied with PAE's policy and procedures. The team also issued a separate letter of comment detailing its specific observations and suggestions and its scope and methodology.

Note: The Tennessee Valley Authority OIG initiated an external peer review of our evaluation organization in April 2022 and expects to issue its results by September 30, 2022.

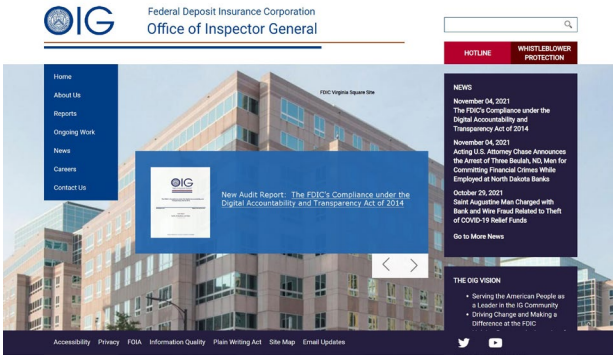
Investigative Peer Reviews

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.

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.

FDIC OIG
@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-workgroup**.

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**.