FDIC Office of Inspector General

Semiannual Report to the Congress

April 1, 2022 - September 30, 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 5,640 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured $9.86 trillion in domestic deposits in 4,771 institutions, of which the FDIC supervised 3,080. The Deposit Insurance Fund balance totaled $124.5 billion as of June 30, 2022. Active receiverships as of September 30, 2022 totaled 156, with assets in liquidation of about $48.3 million.

Semiannual Report to the Congress

April 1, 2022 - September 30, 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 April 1, 2022 through September 30, 2022.

During this reporting period, we issued our report on the FDIC's Information Security Program, noting certain areas where the FDIC needs to focus its attention, including Supply Chain Risk Management, and its Plans of Action & Milestones. We also issued an Advisory Memorandum to the FDIC highlighting our concerns with respect to the FDIC's Background Investigations for Privileged Account Holders.

We continue to audit and evaluate other significant matters affecting the FDIC programs and operations, including the FDIC's examination program of Information Technology (IT) and cyber risks at banks; IT security of the FDIC's wireless networks; the Agency's supervision of Government-guaranteed loan programs; its Active Directory processes; contract oversight; consumer participation and inclusion in the banking system; strategies related to cryptocurrency and digital assets; and the FDIC's readiness to execute its Orderly Liquidation Authority, among others.

Our Investigations during the reporting period resulted in 56 indictments, 59 convictions, 43 arrests, and more than $47 million in fines, restitution ordered, and other monetary recoveries. In one of our cases, the former Chief Credit Officer of First NBC Bank pled guilty to conspiring with others to conceal material information and defraud the bank. The co-conspirators made false representations about certain substantial loans and concealed the financial condition of the Bank from its Board of Directors, auditors, and bank examiners. The FDIC estimates the cost of First NBC's failure to the Deposit Insurance Fund will be in excess of $900 million. In another case, an individual was sentenced to serve 46 months in prison for his role in a business email compromise scheme in which fraudulent emails from spoofed domains were used to trick numerous companies to unwittingly transmit funds from FDIC-insured institutions to accounts that the subject controlled.

Of note, our work in the area of pandemic-related fraud accounted for many judicial actions and monetary benefits during this period. To date, we have opened 181 cases associated with fraud in the CARES Act and American Rescue Plan programs. Prosecutions in these cases result in harsh sentences; ordered restitution; and seizures of cash proceeds, real estate, and luxury items from offenders who steal funds from Government programs intended for those most in need during the pandemic. In one of our cases this period, for example, a bank customer was sentenced to 125 months in prison, 5 years of supervised release, and was ordered to pay $1.2 million in restitution for his role in fraudulently obtaining Paycheck Protection Program funds.

We have also made significant investments in our Electronic Crimes Unit – to ensure that our Special Agents are equipped with the latest cutting-edge technology and tools to investigate financial crimes. We are focusing on cyber-crimes at banks, including computer intrusions, cryptocurrency, ransomware, and account takeovers. I was pleased to discuss these areas of focus recently at the Financial Fraud Conference sponsored by the Department of Justice and the FDIC as I looked to the future of our investigative work in the banking sector.

Throughout the reporting period, we have further developed our Data Analytics capabilities to use technology in order to cull through large datasets and identify anomalies that the human eye cannot ordinarily detect. We are developing tools and technology – to marshal our resources and harness the information. We are looking for red-flag indicators and aberrations in the underlying facts and figures, in order to proactively identify tips and leads for further investigation, detect high-risk areas at the FDIC, and recognize emerging threats to the banking sector. Another important project to leverage technology during the period relates to our external website. We updated the site, made it more user friendly, enhanced its functionality, simplified navigation, and strengthened its search features.

In addition, we are proud that two of our OIG teams received awards from the Council of the Inspectors General on Integrity and Efficiency for Excellence in Audits and Investigations. The IG Community recognized our work on the Sharing of Threat Information within the Agency, and a successful criminal case against a corrupt banker in Chicago. Three other members of our Office received awards for their contributions to investigations in the IG Community. I am especially grateful to the dedicated women and men of our Office who received these awards and for all who are carrying out the OIG mission.

We also welcomed talented new members to our OIG Team over the past 6 months, including an Assistant Inspector General for Investigations, Chief of Staff, Director of Management Services, and Data and Analytics Officer, and others with outstanding backgrounds and expertise.

Finally, we issued our first-ever Diversity, Equity, Inclusion, and Accessibility (DEIA) Strategic Plan. The Plan articulates four goals: We have a shared purpose. Each person is valued in our Office. Our processes are fair and equitable. We strive to mature our DEIA Program. This Plan demonstrates our steadfast commitment to the integration of these principles into our ongoing operations and functions.

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 of the FDIC.

Jay N. Lerner
Inspector General
October 2022

Table of Contents

Acronyms and Abbreviations

AEC	Audits, Evaluations, and Cyber
AIG	Assistant Inspector General
BSA/AML	Bank Secrecy Act/Anti-Money Laundering
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIOO	Chief Information Officer Organization
COVID-19	Coronavirus Disease 2019
DEIA	Diversity, Equity, Inclusion, and Accessibility
DHS	Department of Homeland Security
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOJ	Department of Justice
ECU	Electronic Crimes Unit
EIDL	Economic Injury and Disaster Loan
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FHFA	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
FRB	Federal Reserve Board
FSOC	Financial Stability Oversight Council
IG	Inspector General
IRS-CI	Internal Revenue Service-Criminal Investigation
IT	Information Technology
OC	Outside Counsel
OIG	Office of Inspector General
OM	Oversight Manager
OMB	Office of Management and Budget
POA&M	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
SME	Subject Matter Expert
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 (April 1, 2022–September 30, 2022)	
Audit, Evaluation, and Other Products Issued	**2**
Nonmonetary Recommendations	**1**
Investigations Opened	**44**
Investigations Closed	**55**
Judicial Actions:	
Indictments/Informations	**56**
Convictions	**59**
Arrests	**43**
OIG Investigations Resulted in:	
Fines of	**$71,300.00**
Restitution of	**$41,446,326.95**
Asset Forfeitures of	**$4,834,778.28**
Settlement	**$706,332.07**
Total	**$47,058,737.30**
Referrals to the Department of Justice (U.S. Attorney)	**67**
Responses to Requests Under the Freedom of Information/Privacy Act	**12**
Subpoenas Issued	**2**

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.

We are pleased to report that during the reporting period, we received the results of two peer reviews of our Audits, Evaluations, and Cyber (AEC) component conducted by IG community colleagues. In the case of audits, the Department of State OIG conducted a peer review of our audit organization's system of quality control in accordance with the Council of the Inspectors General on Integrity and Efficiency's (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). In the Department of State OIG's opinion, the system of quality control for the audit organization of the FDIC OIG in effect for the year ended March 31, 2022, had been suitably designed and complied with to provide the FDIC OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards and applicable legal and regulatory requirements in all material respects. Our Office received a rating of Pass.

Auditor-in-Charge Judith Hoyle accepted a CIGIE Award for Excellence on behalf of our FDIC OIG team for the audit of The FDIC's Sharing of Threat Information to Guide the Supervision of Financial Institutions. Pictured left to right are Audit Manager Joe Nelson; AIG for Audits, Evaluations, and Cyber, Terry Gibson; Judith Hoyle; and IG Jay N. Lerner.

Similarly, with regard to evaluations, the external peer review team from the Tennessee Valley Authority OIG assessed the extent to which the FDIC OIG complied with standards from CIGIE's *Quality Standards for Inspection and Evaluation* (Blue Book), January 2012. Specifically, the Review Team assessed quality control, planning, data collection and analysis, evidence, records maintenance, reporting, and follow-up. The assessment included a review of the FDIC OIG's internal policies and procedures implementing the seven covered Blue Book standards. It also included a review of selected inspection and evaluation reports issued between April 1, 2021 and March 31, 2022, to determine whether the reports complied with the covered Blue Book standards and the FDIC OIG's internal policies and procedures. The review team determined that our policies and procedures generally were consistent with the seven Blue Book standards addressed in the external peer review. Additionally, all three reports reviewed generally complied with the covered Blue Book standards and the FDIC OIG's associated internal policies and procedures.

Additionally, during the past 6 months, we issued our report on *The FDIC's Information Security Program—2022*, in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). We also issued a Memorandum to FDIC management on *Background Investigations for Privileged Account Holders* during the reporting period. Further, as a member of the Council of Inspectors General on Financial Oversight (CIGFO), we co-led the Working Group that issued a report on *Guidance on Preparing for and Managing Crises* and also provided input to CIGFO's Annual Report.

We also note that in addition to planned discretionary work, our Office reviews the failures of FDIC-supervised institutions causing material losses to the Deposit Insurance Fund 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 (Dodd-Frank 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. A listing of ongoing assignments is also presented. Additionally, we discuss two unresolved recommendations from a report issued previously and other projects we have undertaken in connection with CIGFO and CIGIE, along with several key operational initiatives from the reporting period.

Audits, Evaluations, and Other Reviews

The FDIC's Information Security Program—2022

We issued our report on *The FDIC's Information Security Program—2022*. The audit evaluated the effectiveness of the FDIC's information security program and practices, as required by the Federal Information Security Modernization Act of 2014 (FISMA). The OIG engaged the professional services firm of Cotton & Company Assurance and Advisory, LLC to conduct this audit.

Department of Homeland Security (DHS) FISMA Reporting Metrics require OIGs to assess the effectiveness of their agencies' information security programs and practices using a maturity model. In Fiscal Year (FY) 2022, OIGs were required to evaluate a subset of 20 metrics. The FDIC's information security program was operating at a Maturity Level 4 (managed and measurable). The overall maturity level for FY 2022 was determined by a simple majority where the most frequent level (mode) across the 20 metric questions served as the overall rating. This mode-based scoring methodology does not fully capture the nature, scope, and magnitude of the risk posture of the agency's Information Technology (IT) security. As a result, an agency may still face significant risks even if its rating score is considered to be managed and measurable. We cautioned the FDIC against complacency since deficiencies remain in the information security program at the FDIC.

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

The FDIC's Supply Chain Risk Management (SCRM) Program Lacks Maturity: The FDIC is still developing its policies and procedures to address the SCRM finding from the FISMA report for 2021. Additionally, we found, in our OIG evaluation report of the FDIC's SCRM program (issued March 2022), that the FDIC had not implemented several objectives outlined in its SCRM Implementation Project Charter; did not conduct supply chain risk assessments in accordance with best practices; had not ensured that its Enterprise Risk Management processes fully capture supply chain risks; and FDIC Contracting Officers did not maintain contract documents in the proper system. We issued nine recommendations, five of which remained unimplemented.

The FDIC Did Not Adequately Oversee and Monitor Information Systems: The FDIC Chief Information Officer Organization (CIOO) had not completed the authorization in accordance with the National Institute of Standards and Technology Risk Management Framework for approximately 52 percent of its legacy systems and subsystems (as of May 19, 2022).

The FDIC Did Not Address Flaw Remediation Plans of Action and Milestones (POA&M) in a Timely Manner: The FDIC had 31 POA&Ms related to flaw remediation open past their estimated completion dates (as of June 21, 2022). These POA&Ms covered, for example, patch management, security updates for software products, and outdated versions or unapplied security updates for certain applications.

The FDIC Did Not Configure Privileged Accounts in Accordance with the Principle of "Least Privilege": We are currently conducting an audit of the FDIC's security controls over its Windows Active Directory. During the course of our work, we identified instances where accounts were configured with elevated account settings; however, there was no justification provided for such settings, and the elevated settings were no longer needed for administrators to perform their business roles. Additionally, we identified concerns relating to the Background Investigations for Privileged Account Holders at the FDIC and issued a Management Advisory Memorandum in June 2022.

The FDIC Did Not Fully Implement Its Document Labeling Guide: In our FISMA report dated October 2021, we recommended that the FDIC implement document labeling guide requirements across the organization. However, the FDIC had not yet fully implemented this recommendation and did not anticipate implementation until later this year.

The report contained a recommendation for the FDIC to address the 31 flaw remediation POA&Ms. It also contained a listing of three unimplemented recommendations from prior FISMA reports.

We also noted in the report that during the course of this audit, we learned that the FDIC process for emails included manual review by the FDIC (FDIC employees and/or contractors) of messages flagged by automated tools. This process presents security and privacy risks that FDIC employees and/or contractors could be inadvertently exposed to information that they would otherwise not be permitted to review. In addition, this process presents risks that emails relevant to urgent law enforcement matters are not received by the OIG in a timely manner, thus presenting security and safety concerns. As a result, on July 11, 2022, we issued a Memorandum to senior FDIC officials expressing our concerns regarding the FDIC's handling of OIG emails. The FDIC's CIOO responded that it intends to implement changes in technical and policy controls and IT infrastructure to mitigate the risks that we identified, and the FDIC OIG is currently working with FDIC IT personnel to address our concerns.

Background Investigations for Privileged Account Holders

While conducting an ongoing audit of security controls over the FDIC's Windows Active Directory, we identified concerns related to the FDIC's policies and procedures for ensuring that certain contractors and employees who require privileged access to FDIC information systems and data have background investigations commensurate with appropriate determinations of risk. A privileged account holder may have access and authority to control and monitor systems, and perform administrative functions that ordinary users are not authorized to perform. The Memorandum conveys our concerns to the FDIC regarding the need for controls to address associated risks.

The Office of Management and Budget Circular A-130 requires that agencies implement access control policies for information resources that ensure individuals have the appropriate background investigation conducted prior to granting access. We reviewed 144 privileged account holders to determine whether the FDIC conducted background investigations commensurate with position risk designation levels recorded in the FDIC's personnel system. We identified one exception and another case where a contractor had privileged access until the contractor's background investigation was unfavorably adjudicated. We also determined that the FDIC did not have policies or procedures in place to re-evaluate risk designations and background investigation levels for FDIC employees or contractors who transition from being non-privileged account holders to privileged account holders or whose privileged access is increased after they have already started work at the FDIC. Such controls can help ensure that the FDIC considers the risks resulting from a contractor or employee's change in privileged access and that the appropriate background investigation level is in place before granting the privileged access.

The FDIC agreed that procedures could be improved in this area and planned to perform follow-up work to further assess the extent of risk associated with our observations and make improvements to procedures and processes as warranted by the end of calendar year 2022.

Council of Inspectors General on Financial Oversight Guidance in Preparing for and Managing Crises

On June 30, a Working Group of CIGFO issued its *Guidance in Preparing for and Managing Crises*. Our Office, under the direction of our Assistant Inspector General (AIG) for AEC, co-led this effort on behalf of CIGFO member OIGs.

The Guidance is intended to be a compilation of lessons learned drawn from the experiences of Federal agencies during prior crises and any learned during the recent pandemic. The Guidance will facilitate effective crisis response as the Financial Stability Oversight Council (FSOC) fulfills its mission to identify threats to the financial stability of the country, promote market discipline, and respond to emerging threats to the stability of the U.S. financial system.

The crisis preparedness and management practices identified and summarized by the CIGFO Working Group OIGs were based upon agency planning documents to address market disruptions; contingency and crisis plans; stress tests; testing of market coordination procedures; retrospective analyses of regulator responses to prior crises; business resiliency management analyses; a prioritized supervision framework in response to the COVID-19 pandemic; crisis management plans; economic impact analyses following a crisis; plans for cyber incident response; lesson learned reviews; strategic plan initiatives to improve crisis management and response capabilities; audits of agency responses to emerging risks; international peer reviews of agency approaches to supervision and regulation following financial crises; and audits to assess regulatory activities under Presidential Policy Directive 21.

The guidance derived from these sources broadly falls into the following categories:

Collaboration and Pre-Crisis Planning Activities • Define agency mandates, roles, and responsibilities • Facilitate information sharing proactively • Strive for a shared view of market conditions • Implement continuous monitoring activities.

Agencies' Crisis Readiness Plan Elements • Establish individual roles and responsibilities related to plans • Describe triggering events • Identify relevant legal authorities and tools, and potential emergency actions • Develop communication plans and options • Prioritize system capacity, and cyber and information security (aligned with existing continuity capabilities) • Provide for testing, evaluation, review, revision, and training • Provide for reporting.

Agencies' Crisis Management • Implement leadership response • Coordinate among member agencies • Communicate to internal and external stakeholders • Assess resources • Supervise markets and regulated entities • Deploy response programs • Evaluate lessons learned.

CIGFO intends this guidance to assist FSOC and its member agencies, including the FDIC, with coordinating and planning for future crises in order to help identify and mitigate risks to the financial stability of the United States associated with potential gaps in crisis preparedness. CIGFO provided this guidance in support of FSOC and its member agencies' ongoing efforts, recognizing that some activities are already broadly in practice, while other activities presented in the report can promote new initiatives that enhance the wider crisis planning effort.

Top Management and Performance Challenges Drive Ongoing OIG Work

Our Top Management and Performance Challenges document summarizes the most serious challenges facing the FDIC and briefly assesses the Agency's progress to address them, in accordance with the Reports Consolidation Act of 2000 and Office of Management and Budget Circular A-136 (revised August 10, 2021). The Top Challenges document that we issued in February 2022 was based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities.

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

- 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
- Human Resources at the FDIC

At the end of the current reporting period, we had a number of ongoing audits, evaluations, and reviews emanating from our analysis of the Top 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.

- *The FDIC's Administration and Oversight of the AT&T Telecommunications Contract.* The objective is to determine if the FDIC authorized and paid AT&T for services to upgrade bandwidth in FDIC field offices in accordance with its existing telecommunications contract and its policies and procedures.
- *Sharing of Threat and Vulnerability Information Phase 2.* The objective is to determine whether the FDIC has implemented effective processes to ensure that financial institutions receive actionable and relevant threat and vulnerability information.
- *The FDIC's Readiness to Execute the Orderly Liquidation Authority.* The objective is to determine whether the FDIC has established key elements to execute the Orderly Liquidation Authority under the Dodd-Frank Act, including: (1) comprehensive policies and procedures; (2) defined roles and responsibilities; (3) necessary resources and skill sets; (4) regular monitoring of results; and (5) integration with the Agency's crisis readiness and response planning.
- *FSOC's Response to the Executive Order on Climate-Related Financial Risk.* The objective is to determine what actions FSOC has taken, or planned, in response to Executive Order 14030, Climate-Related Financial Risk, as of November 30, 2021, and whether those actions are consistent with the policy, objectives, and directives set forth in the Executive Order.
- *The FDIC's Efforts to Increase Consumer Participation in the Insured Banking System.* The objective is to determine whether the FDIC developed and implemented an effective strategic plan to increase the participation of unbanked and underbanked consumers in the insured banking system.
- *FDIC Strategies Related to Crypto-Asset Risks.* The objective is to determine whether the FDIC has developed and implemented strategies that address the risks posed by crypto assets.
- *The FDIC's Adoption of Cloud Services.* The objective is to determine if the FDIC has an effective strategy and governance processes to manage its cloud computing services.

Ongoing reviews are listed on our website and, when completed, their results will be presented in an upcoming semiannual report. Additionally, the OIG's assessment of the Top Management and Performance Challenges currently facing the FDIC is ongoing and will be issued in February 2023.

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

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

Therefore, it is important that the FDIC develop policies, processes, and procedures to ensure that vital threat information is shared with its personnel – such as FDIC policymakers, bank examiners, supervisory personnel, and Regional Office staff – so that the data may be used in an actionable and timely manner. Our Office conducted a review to determine whether the FDIC had established effective and efficient processes to share threat information with its personnel. We identified several weaknesses in the FDIC's sharing of threat information and reported on those during the prior reporting period.

We made 25 recommendations to the FDIC to strengthen its governance processes for acquiring, analyzing, disseminating, and using relevant and actionable threat information to guide the supervision of financial institutions.

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

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

As explained more fully on page 57 of this report, we are reporting these two recommendations as unresolved and without management decisions as of the end of the current reporting period. We are continuing to work with FDIC management to reach a management decision on these recommendations.

CIGFO Annual Report

CIGFO published its annual report, dated July 2022. This report highlights CIGFO activities and presents write-ups from the member agency OIGs related to their work to help strengthen the financial system through their oversight of Federal programs. Coverage of the FDIC OIG's significant work over the past year includes discussion of Sharing of Threat Information to Guide the Supervision of Financial Institutions, Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders, the FDIC's Implementation of Supply Chain Risk Management, and the Top Management and Performance Challenges Facing the FDIC. Also included are highlights from several investigations that the FDIC OIG conducted to ensure integrity in the banking sector and address fraud in the Federal pandemic response.

CIGIE Monetary Benefits Working Group

The FDIC OIG's AIG for AEC and one of our Audit Managers are co-leading a working group on behalf of CIGIE related to identifying and reporting on the monetary impact of OIG audits and evaluations. The Monetary Impact Working Group was formed jointly by CIGIE's Audit Committee and Inspection and Evaluation Committee in March 2022. It is the largest working group, consisting of 42 members representing approximately 20 different OIGs, varying in size.

The short-term goal of the group is to identify best practices and any areas of inconsistency from across the IG community related to Monetary Impacts. Four sub-groups are at work addressing the following: (1) OIG Policies and Procedures; (2) Audit, Inspection, and Evaluation Reports; (3) Semiannual Reports to Congress; and (4) Survey Results from more than 51 OIGs.

The Working Group will brief the sponsoring committees on its results and identify next steps. The Working Group anticipates this might be guidance to the IG community on best practices and lessons learned related to monetary impact. The intent is to ensure that the monetary impact of OIG work is consistently captured and clear to the American public and Congress.

Other Noteworthy AEC Projects

IT Audit and Evaluation Strategic Plan: Another key initiative in AEC during the reporting period was the drafting of AEC's IT Audit and Evaluation Plan for Calendar Years (CY) 2023 through 2025. The plan is intended to provide both strategic and tactical direction for IT-related assignments. It will serve as a road map for AEC in reviewing IT operations and cybersecurity defenses. AEC has built in flexibility to address emerging technological issues, evolving cybersecurity threats, and changing FDIC priorities.

The Plan also speaks to recruiting and hiring IT auditors and specialists with strong IT audit and evaluation experience and technical skills, and enhancing the expertise of current IT auditors and specialists. We further plan to increase our use of data analytics in all AEC assignments to perform the highest risk assignments, increase efficiencies, and provide valuable insight to FDIC leadership. Additionally, longer term, we plan to build out a lab environment that will facilitate learning and enhance our staff's ability to perform technical testing during planned assignments.

New AEC Case Management System: In this semiannual period, AEC began to configure a new commercial-off-the-shelf case management system to align with the OIG's assignment management processes. AEC will be transitioning to the new system in fiscal year 2023. In addition to creating a system of record to document the work performed and review of that work to support report findings consistent with applicable professional standards, the new AEC Management Information System will allow us to build dashboards to track assignments relative to office benchmarks; monitor the FDIC's implementation of OIG report recommendations; and ensure that staff meet competency standards. Implementation of the new system will also ensure that the OIG complies with the FDIC's system security requirements and has the ability to adapt to new technical requirements and advancements.

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 work 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. Noteworthy PRAC initiatives during the reporting period include:

Report: On June 13, the PRAC issued its report on *Key Insights: Identity Fraud Reduction and Redress in Pandemic Response Programs*. This Insights Report is based on information gathered by the PRAC's Identity Fraud Reduction and Redress Working Group and other relevant partners. The report outlines challenges related to addressing identity fraud and highlights actions Government agencies can take to both reduce identity fraud and improve victim redress programs.

Testimony: ***Examining Federal Efforts to Prevent, Detect, and Prosecute Pandemic Relief Fraud to Safeguard Funds for All Eligible Americans.*** On June 14, 2022, the Chair of the PRAC testified before the House Select Subcommittee on the Coronavirus Crisis. In his testimony, Chair Michael E. Horowitz discussed the PRAC's ongoing oversight work and achievements over its first 2 years. He also emphasized the need to curtail identity fraud across Government programs and how pending legislative action will help watchdogs hold domestic and international fraudsters accountable.

Roundtable Event: ***What's It Like Applying for Pandemic Relief Funds?*** On June 15, the PRAC co-hosted a virtual panel discussion with the National Academy of Public Administration on the public's experience applying for financial assistance from different pandemic relief programs. In this virtual roundtable, a panel of experts discussed the barriers applicants faced trying to access benefits and what the Federal Government can do to reduce them.

Roundtable Event: ***How Can Local Governments Shed More Light on Pandemic Relief Spending in Their Communities?*** On June 29, the PRAC hosted a virtual panel discussion with panelists from local Governments and organizations that track Federal money to showcase examples of data dashboards and visualization tools that effectively display the use of pandemic funds in local communities. The panelists described their experiences collecting the data, challenges with reporting requirements, and recommendations for increasing transparency for the public.

Legislation Update: On August 5, President Biden signed H.R. 7334, the "COVID–19 EIDL Fraud Statute of Limitations Act of 2022," into law. This law establishes a 10-year statute of limitations for fraud by borrowers under the Small Business Administration's COVID-19 Economic Injury Disaster Loan (EIDL) Programs. The President also signed H.R. 7352, the "PPP and Bank Fraud Enforcement Harmonization Act of 2022," into law, which establishes a 10-year statute of limitations for fraud by borrowers under the Small Business Administration's Paycheck Protection Program (PPP).

A New Way to Show Pandemic Funding by Individual Federal Agencies: In September, the PRAC announced a new way to view data on PandemicOversight.gov. The new agency funding profiles on the PRAC's website enable the public to see the total amount of pandemic relief money that nearly 40 Federal agencies received, and the specific programs funded. They also include relevant oversight work from Federal OIGs, whose audits and investigations alert the public and policymakers of any fraud, waste, and abuse.

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, embezzlement, money laundering, cybercrime, and currency exchange rate manipulation. Whether it is bank executives who have caused the failures of banks, or criminal organizations stealing from Government-guaranteed loan programs – these cases often involve bank directors and officers, Chief Executive Officers, attorneys, real-estate insiders, crypto-firms and exchanges, Financial Technology (FinTech) companies, and international financiers.

FDIC OIG investigations during the reporting period resulted in 56 indictments, 59 convictions, 43 arrests/self-surrenders, and more than $47 million in fines, restitution ordered, and other monetary recoveries.

Special Agent James Greczek (center) and his law enforcement partners were recognized with a CIGIE Award for Excellence for the investigation and prosecution of Stephen Calk, former Chairman and Chief Executive Officer of The Federal Savings Bank. Pictured with him are IG Jay N. Lerner (left) and AIG for Investigations, Shimon Richmond (right).

Electronic Crimes Unit

Our Electronic Crimes Unit (ECU) is an important component within our Office of Investigations. Over the past several years, the OIG ECU has been working to overhaul and revamp its Forensic Laboratory. During the reporting period, the OIG received an Authorization to Operate for the ECU's secure network. The ECU lab will help to analyze voluminous electronic records in support of complex financial fraud investigations nationwide. The ECU lab will also provide a platform for complex data analysis, eDiscovery, and forensic data services, and it will support the analysis of Electronically Stored Information.

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

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

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

The FDIC OIG continues to support efforts of DOJ's COVID-19 Fraud Enforcement Task Force (CFETF) as a key interagency partner for the Department of Justice. 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. Additionally, on September 15, the U.S. Attorney's Office for the Southern District of Florida announced that it has been selected to head one of three COVID-19 Fraud Strike Force Teams nationally. The district in the prior few weeks alone, had charged 23 COVID-19 relief fraud cases, with scheme amounts totaling over $150 million. The Strike Force Team will be comprised of dedicated prosecutors, the FDIC OIG, and other OIGs and law enforcement agencies. "These Strike Force Teams will build on the Department's historic enforcement efforts," said Attorney General Merrick B. Garland. "Since the start of this pandemic, the Justice Department has seized over $1.2 billion in relief funds that criminals were attempting to steal and charged over 1,500 defendants with crimes in federal districts across the country, but our work is far from over. The Department will continue to work relentlessly to combat pandemic fraud and hold accountable those who perpetrate it."

Pandemic-Related Financial Crimes

Since many of the programs in the Coronavirus Aid, Relief, and Economic Security (CARES) Act and related legislation are administered through banks and other insured institutions, our Office of Investigations has been actively involved in investigating pandemic-related financial crimes affecting the banks. In addition, our Office regularly coordinates with the supervisory and resolutions components within the FDIC to watch for patterns of crimes and other trends in light of the pandemic. Our Special Agents have been working proactively with other OIGs; U.S. Attorney's Offices; and other law enforcement agencies on cases involving frauds targeting the $5 trillion in funds distributed through pandemic relief programs. Through these collaborative efforts, we have been able to identify, develop, and lead cases specific to fraud related to stimulus packages. We have played a significant role within the law enforcement community in combating this fraud and since inception of the CARES Act, have been involved in 181 such cases.

Notably, during the reporting period, the FDIC OIG's efforts related to the Federal Government's COVID-19 pandemic response resulted in 41 indictments and informations; 30 arrests or self-surrenders; and 33 convictions involving fraud in the CARES Act Programs. Fines, restitution ordered, settlements, and asset forfeitures resulting from these cases totaled in excess of $27.8 million.

Leveraging Data Analytics

Importantly, our Office continues to develop its Data Analytics capabilities – to use technology in order to cull through large datasets and identify anomalies that the human eye cannot ordinarily detect. We are gathering relevant datasets, developing tools and technology, and hiring data-science experts – in order to marshal our resources and harness "Big Data." We are looking for red-flag indicators in the statistics and information – and searching for aberrations in the underlying facts and figures. And thus, we will be able to proactively identify tips and leads for further investigations and high-impact cases, detect high-risk areas at the FDIC, and recognize emerging threats to the banking sector.

Our data analytics efforts involve collaboration with the PRAC, the FDIC, Financial Crimes Enforcement Network (FinCEN), DOJ, FBI, and others. These efforts have resulted in: expanded access to investigative data tools and capabilities for OIG investigations; identification of potential data sets relevant to OIG efforts; new opportunities for collaboration with external partners; identification of additional data analytics pilot projects; and information sharing agreements to help inform strategic planning within the OIG.

The cases discussed below are illustrative of some of the OIG's investigative success during the reporting period. They are the result of efforts by FDIC Special Agents and support staff in Headquarters, Regional Offices, and the OIG's ECU. As noted, these cases reflect the cooperative efforts of OIG investigators, FDIC Divisions and Offices, other OIGs, USAOs, and others in the law enforcement community throughout the country. These working partnerships contribute to ensuring the safety and soundness of the Nation's banks, strengthen our efforts to uncover fraud in the Federal pandemic response, and help promote integrity in the FDIC's programs and activities.

Owners of Grand Rapids Trucking Company Plead Guilty to Bank Fraud Conspiracy and Pay $1,000,000 in Related Civil Case, in Connection with Covid-19 Relief Fraud

Semsi Salja and Anes Suhonjic, the owners of Grand Rapids-based trucking company DMR Transportation (DMR), pleaded guilty in Federal court on June 22, 2022 to conspiring to commit bank fraud in connection with a $290,855.00 loan under the Paycheck Protection Program (PPP). In a related civil case, DMR, Salja, and Suhonjic agreed to pay a total of $1,000,000.00, including a substantial civil monetary penalty under the Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA). FIRREA allows civil monetary penalties for any frauds involving or affecting certain types of financial institutions.

DMR knowingly and falsely certified that it qualified for the second draw PPP loan by falsely demonstrating that DMR sustained a 25-percent reduction in gross revenue in the second quarter of 2020 when compared to the second quarter of 2019. DMR also submitted falsified quarterly balance sheets and other false financial records that were signed by Salja and Suhonjic alongside the application. In September 2021, DMR sought forgiveness of its second-draw PPP loan by falsely certifying that its second-draw PPP loan proceeds were used to pay eligible business expenses when, in fact, DMR held that money in reserve.

The civil settlement includes the resolution of claims brought under the whistleblower provisions of the False Claims Act. Under those statutory provisions, a private party can file an action on behalf of the United States and receive a portion of the settlement or judgment proceeds.

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

Bank Customer Sentenced to 125 Months in Prison for Bank Fraud Related to PPP Funds

On April 12, 2022, Robert Williams was sentenced to 125 months in prison, 5 years of supervised release and was ordered to pay $1,227,491.87 in restitution for his role in fraudulently obtaining Paycheck Protection Program (PPP) funds.

Williams both directly applied for and assisted other individuals, and their associated entities, in applying for PPP loan funds and submitted applications containing material misrepresentations to Midwest Regional Bank and PNC Bank. Williams completed and submitted approximately 30 different PPP loan applications that contained materially false statements and false supporting documents related to the ownership of a business and the business' payroll, including the number of employees and monthly payroll expenses. Williams obtained Federal loans provided through the CARES Act that resulted in a loss of up to approximately $2.7 million. Williams applied for these loans at Midwest Regional Bank and PNC Bank and submitted false information to receive funding.

Williams did not use the PPP loan funds for any appropriate business expenses but used funds for his own personal benefit, including the purchase of vehicles such as a Maserati Levante and a Jaguar, F-Pace. During the investigation, the FBI seized approximately $466,000 and vehicles.

Source: Small Business Administration (SBA) OIG.
Responsible Agencies: This case is being investigated by the FDIC OIG, SBA OIG, and FBI.
Prosecuted by the USAO, Eastern District of Missouri.

Former Bank President and CEO of a Failed FDIC-Supervised Bank Sentenced

On May 10, 2022, Dennis Engle, the former President and Chief Executive Officer (CEO) of Harvest Community Bank (HCB), was sentenced to 2 years of probation in the District of New Jersey. Prior to sentencing, Engle pleaded guilty to one count of making false entries to deceive the FDIC and a financial institution, HCB, which failed on January 13, 2017.

From 2010 to 2014, Engle devised a plan to hide approximately $13 million in non-performing loans in the names of nominee companies and a nominee investor. The delinquent loans were sold to nominee companies established in a straw buyer's name, therefore making it appear it was a legitimate sale. Engle provided false and fraudulent information to HCB's loan committee and concealed, in the books and records of HCB, the true nature, purpose, and terms of the loan, in order to circumvent FDIC regulations.

Source: Initiated by the FDIC OIG after HCB was closed.
Responsible Agencies: FDIC OIG.
Prosecuted by the USAO, District of New Jersey.

Iowa Businessman and Former Bank Vice President Sentenced for Defrauding the Small Business Administration

On April 22, 2022, Michael Slater, an Iowa businessman, was sentenced to 14 months in prison, 3 years of supervised release, and ordered to pay $4,528,191.26 in addition to an assessment of $100 for his role in defrauding the SBA as the President of Vital Financial Services.

On August 2, 2022, Andy Erpelding, former Vice President for Valley Bank, was sentenced to time served, 5 years of supervised release, ordered to pay a $100 assessment, and ordered to pay $2,102,150.19 in restitution to the SBA.

Erpelding, Slater, and other defendants fraudulently obtained loan guarantees from the SBA on behalf of Valley Bank borrowers, knowing that the loans did not meet SBA's guidelines and requirements for the guarantees. They did so by, among other things, fraudulently altering loan payment histories, renaming businesses, and hiding the fact that borrowers had previously defaulted on loans. When the fraudulently guaranteed loans defaulted, the defendants caused the submission of reimbursement requests to the SBA to purchase the defaulted loans from investors and lending institutions, thereby shifting the majority of losses on the ineligible loans to the SBA. In all, the defendants attempted to obtain guarantees on over $14 million in loans, were successful in obtaining guarantees on over $9 million in loans, and caused the SBA losses of over $4.5 million.

Source: The Valley Bank investigation was referred by the FDIC's Division of Risk Management Supervision. The Vital Financial Services investigation was initiated by the FDIC OIG and SBA OIG.
Responsible Agencies: FDIC OIG, SBA OIG, Federal Reserve Board (FRB) OIG, Federal Housing Finance Agency (FHFA) OIG, and FBI.
Prosecuted by the USAO, Southern District of Iowa.

District of Columbia Man Sentenced to 56 Months in Prison for Fraud, Money Laundering, and Identity Theft Schemes

On April 8, 2022, Jamar Skeete was sentenced to 56 months in prison followed by 36 months of supervised release for his role in a scheme to defraud SunTrust Bank (now known as Truist Bank). Skeete was also ordered to pay restitution in the amount of $486,256.19, a $400 special assessment, forfeiture of $169,807.36, and to complete 100 hours of community service. The restitution order was broken down as follows: Truist Bank - $35,442.90; IAC Group - $262,001.07; City of Flint, Michigan - $14,958.13; Ashbury Healthcare - $2,500.00; and CFC Insurance - $171,354.09.

Between September 2017 and June 2019, Skeete received and laundered the proceeds of at least four separate business e-mail compromise schemes targeting the City of Flint, Michigan; an Illinois-based company operating senior care facilities; and other businesses. Skeete used two stolen identities and multiple fraudulent shell company accounts to receive and launder the proceeds of the business e-mail compromise schemes in the District of Columbia and elsewhere. In one instance, Skeete established an account under a shell corporation and a stolen identity. Shortly thereafter, the victim, a company based in Michigan, received a series of fraudulent emails that appeared to be from a legitimate vendor. The emails deceived the victim into sending ACH transfers to the fraudulent account Skeete previously established. After receiving the ACH transfers, Skeete rapidly drained the account through a variety of transactions, including international wire transfers, cash withdrawals, and large cash advances at a casino. A secondary unrelated investigation in the Southern District of New York was being pursued and was transferred to the U.S. District Court, Washington DC, for plea and sentencing. Skeete was sentenced for both investigations at the same hearing.

Source: U.S. Postal Inspection Service.
Responsible Agencies: FDIC OIG, FBI, and the U.S. Postal Inspection Service.
Prosecuted by the USAO, District of Columbia.

Business Email Compromise Subject Sentenced

On September 2, 2022, Muhammed Naveed was sentenced to serve 46 months in prison for his role in a business email compromise scheme. Naveed was also ordered to pay restitution of $446,000 for his role in the operation of an unlicensed money transmitting business.

The investigation into suspected computer intrusion and business email compromise scheme identified fraudulent emails from spoofed domains that were used to trick numerous companies to unwittingly transmit funds from FDIC-insured institutions to the subject-controlled accounts rather than to accounts intended by the companies. During the course of the investigation, Naveed was identified as a money mule—that is, an individual who transfers money acquired illegally on behalf of others, and his business, Blacksmith Corporation, was identified as having received money as a result of this fraudulent scheme.

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

Beverly Hills Man Pleads Guilty to COVID-Relief Fraud

On September 22, 2022, Ramiro Mendes, of Beverly Hills, California, pleaded guilty to an information charging him with one count of wire fraud, arising out of fraudulent applications to obtain approximately $6.7 million in PPP funds and Economic Injury and Disaster Loan (EIDL) funds. Mendes' two adult children, Ammon Mendes and Mateus Mendes, previously pleaded guilty in related investigations. Mendes' sentencing is currently scheduled for December 12, 2022.

Specifically, from April 2020 to August 2020, Mendes schemed to fraudulently obtain Federal disaster relief funds distributed through the PPP and EIDL programs that were intended to help small businesses through the economic shock of the COVID-19 pandemic. Mendes claimed to own numerous fake businesses purportedly based in Beverly Hills, including One Wilshire Enterprises, Professional Music Services, and MB Property Management Group LLC. These companies were fake businesses that did not exist prior to the COVID-19 pandemic and did not have any operations or employees.

Mendes admitted to submitting 19 applications for PPP and EIDL loans that contained false and fraudulent information, including the purported existence of payroll expenses, phony tax forms, and the operational status of the businesses. For example, on June 24, 2020, Mendes submitted a fraudulent PPP loan application to a Florida-based bank, seeking a loan of $975,100. The loan application falsely stated that One Wilshire Enterprises employed 18 people, had an average monthly payroll of $390,040, and, according to a false tax form, earned $4,810,149 in revenue in 2019. Based on this false information, the bank approved and funded a PPP loan in the amount of $793,300. The loan amount was wired into a bank account that Mendes controlled.

Mendes admitted in his plea agreement to stealing the COVID-relief loans and misusing the proceeds for his own personal benefit, including the purchase of cryptocurrency. Mendes further admitted that the intended loss in this case was approximately $6,708,963, and the actual loss was at least approximately $2,228,302.

Source: FHFA OIG.
Responsible Agencies: FDIC OIG, FHFA OIG, Treasury Inspector General for Tax Administration, SBA OIG, Internal Revenue Service-Criminal Investigation (IRS-CI), FBI, and the U.S. Postal Inspection Service.
Prosecuted by the USAO, Central District of California.

Chief Credit Officer Pleads Guilty to Conspiracy to Defraud First NBC Bank

On September 13, 2022, William J. Burnell pleaded guilty to a superseding bill of information charging him with one count of conspiracy to commit bank fraud.

In or around 2006 through April 2017, Burnell was the First NBC Bank Chief Credit Officer. He was responsible for the overall quality of the bank's lending function, the bank's credit policies and administration, the bank's loan recovery and collection efforts, and the bank's monitoring and management of past due loans, which included the approval of the bank's internal list of past-due loans. Burnell was responsible for compiling month-end reports, including lists of overdrawn borrowers and past-due loans. These reports should have accurately shown the quality of the bank's assets, which included loans. Misrepresentations on these reports made a true assessment of the bank's overall financial well-being impossible. Burnell was also responsible for approving credit risk ratings before the bank decided to lend to its customers.

Nevertheless, Burnell conspired with the bank's President Ashton J. Ryan, Jr., Executive Vice President Robert B. Calloway, Senior Vice President Fred V. Beebe, and others to conceal material information and defraud the bank. For example, Burnell, Ryan, and Calloway knowingly concealed material information about borrower Gary Gibbs from the board, auditors, and examiners. Further, Burnell served as an additional approving officer for loans to borrower Warren Treme, who was Ryan's business partner. Beebe was Treme's loan officer. Burnell, Ryan, and Beebe made misrepresentations in Treme's loan documents and to the board, auditors, and examiners, in ways that financially benefited Ryan.

First NBC Bank was closed on April 28, 2017, by the Louisiana Office of Financial Institutions, which appointed the FDIC as Receiver. The FDIC estimates the cost to the Deposit Insurance Fund will be in excess of $900 million.

Source: FDIC Legal Division.
Responsible Agencies: FDIC OIG, FBI, and FRB OIG.
Prosecuted by the USAO, Eastern District of Louisiana.

Liberian National Sentenced to 10 Years for $23 Million COVID-19 Relief Fraud

On April 21, 2022, Steven Jalloul was sentenced to 120 months in prison followed by 3 years of supervised release. Jalloul was ordered to pay $486,493.90 in restitution to Celtic Bank, $384,222.26 in restitution to Cross River Bank, $76,345 to PNC Bank, and $25,052.84 to Funding Circle for a total of $972,114 in restitution. Jalloul was also ordered pay a $100 special assessment.

Jalloul is currently in prison serving a 6-year sentence for preparing false tax returns. The 120-month sentence will be served consecutively to the 6-year sentence that Jalloul is currently serving. From at least May 7, 2020, through at least July 28, 2020, Jalloul, owner and operator of Royalty Tax and Financial Services, LLC (Royalty Tax), Farmers Branch, Texas, submitted approximately 170 materially false loan applications for Royalty Tax clients seeking over $23 million in PPP funds through financial services companies, including BlueVine, Redwood City, California. Approximately 97 loans were approved and disbursed by participating lenders, including Celtic Bank and Cross River Bank, totaling over $12 million. Jalloul required Royalty Tax clients to pay a fee between 2 percent and 20 percent of the PPP loan proceeds and received at least $972,114 in fees between May 21, 2020, and July 6, 2020. Jalloul also laundered funds he received from a PPP loan he obtained using a stolen identity by wiring approximately $100,000 from the business account where the funds were deposited into Royalty Tax's business account. In addition, Jalloul received a PPP loan in the amount of $76,345 from PNC Bank (formerly known as BBVA USA) in April 2020 for his business, Amical Investment, Inc., which was not in operation as of February 15, 2015. Jalloul committed these offenses while released on bond awaiting sentencing for preparing false tax returns.

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

Former Bank President Pleads Guilty to Bank Fraud

On August 30, 2022, Brady Torgerson, former President of First Security Bank-West (FSB-W), Beulah, North Dakota, pleaded guilty to two counts of bank fraud. Torgerson was previously indicted on November 3, 2021, along with Brent D. Torgerson and Kelly M. Huffman by a Federal grand jury in the District of North Dakota for engaging in financial crimes while employed at financial institutions.

Torgerson, while employed at two separate North Dakota financial institutions, engaged in a scheme to defraud both financial intuitions by issuing bank funds to individuals not entitled to these funds, failing to register banking transactions, creating fraudulent loan obligations, and taking actions to conceal his activities.

As President of FSB-W, Torgerson issued 20 Bank Money Orders against the FSB-W general ledger account without properly crediting and funding the transactions, ultimately creating an overdraft of approximately $724,558.48 on FSB-W's general ledger account. In January 2021, Torgerson became employed at The Union Bank, Glenn Ullin, North Dakota, and created, between January 25, 2021, and January 29, 2021, fraudulent loan obligations against two separate individuals, in the approximate amount of $225,487.45, and the approximate amount of $225,487.44, when these individuals were neither responsible for these loan obligations nor received the proceeds and benefits of these fraudulent loan obligations. Proceeds from these loans were used to remedy, in part, the out-of-balance general ledger account at FSB-W.

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

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 we partnered with USAOs in over 69 judicial districts in 37 locations in the U.S.:

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

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; Connecticut Digital Assets Working Group; South Jersey SAR Task Force; Pennsylvania Electronic Crimes Task Force; NJ COVID-19 Fraud Task Force; Newark HSI Financial Fraud Working Group; Northern District of New York PPP Fraud Working Group.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force; Northern District of Georgia Mortgage Fraud Task Force; Eastern District of North Carolina Bank Fraud Task Force; Northern District of Alabama Financial Fraud Working Group; Northern District of Georgia SAR Review Team; Middle District of Georgia SAR Review Team; South Carolina Financial Fraud Task Force; Eastern District of North Carolina Financial Crimes Task Force; Western District of North Carolina Financial Crimes Task Force; Middle District of North Carolina Financial Crimes Task Force; COVID Working Groups for: Southern District of Florida, Middle District of Florida, Northern District of Florida; SAR Review Groups for: Miami, Palm Beach, Treasure Coast Financial Crimes Review Team, Key West/Monroe County; DOJ-COVID-19 Fraud Strike Force-Miami.
Kansas City Region	Kansas City SAR Review Team; St. Louis SAR Review Team; Minnesota Inspector General Council; Minnesota Financial Crimes Task Force; Nebraska SAR Review Team; Southern District of Iowa SAR Review Team.
Chicago Region	Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Central District of Illinois Financial Fraud Working Group; Northern District of Illinois SAR Review Team; Northern District of Illinois Bankruptcy Fraud Working Group; Cook County Region Organized Crime Organization; FBI Milwaukee Area Financial Crimes Task Force; FBI Northwest Indiana Public Corruption Task Force; Eastern District of Wisconsin SAR Review Team; Western District of Wisconsin SAR Review Team; Western District of Wisconsin Bankruptcy Fraud Working Group; Indiana Bank Fraud Working Group; Northern District of Indiana SAR Review Team; FBI Louisville Financial Crime Task Force; U.S. Secret Service Louisville Electronic Crimes Task Force; Western District of Kentucky SAR Review Team; Eastern District of Kentucky SAR Review Team; Southern District of Ohio SAR Review Team; Michiana Loss Prevention Working Group, AML Financial Institution/LE Networking Group, FBI Chicago Financial Crimes Task Force, Eastern District of Michigan SAR Review Team, Western District of Michigan SAR Review Team, Northern District of Ohio SAR Review Team, Southern District of Indiana SAR Review Team.
San Francisco Region	Fresno Mortgage Fraud Working Group for the Eastern District of California; Sacramento Mortgage Fraud Working Group for the Eastern District of California; Sacramento SAR Working Group; Orange County Financial Crimes Task Force-Central District of California; Orange County SAR Review Team; Northern District of California Money Laundering SAR Review Task Force; San Diego Financial Investigations and Border Crimes Task Force; Northern Nevada Financial Crimes Task Force; Financial Services Roundtable coordinated by the USAO of the Northern District of California; Los Angeles Complex Financial Crimes Task Force – Central District of California; Los Angeles Real Estate Fraud Task Force – Central District of California; Homeland Security San Diego Costa Pacifica Money Laundering Task Force; DOJ National Unemployment Insurance Fraud Task Force; California Unemployment Insurance Benefits Task Force; Nevada Fight Fraud Task Force; Las Vegas SAR Review Team; COVID Benefit Fraud Working Group, USAO District of Oregon; Financial Crimes Task Force, USAO District of Hawaii.
Dallas Region	SAR Review Team for Northern District of Mississippi; SAR Review Team for Southern District of Mississippi; Oklahoma City Financial Crimes SAR Review Working Group; Austin SAR Review Working Group; Houston High Intensity Drug Trafficking Area SAR Team.
Mid-Atlantic Region	Virginia Crime Analysts Network; Northern Virginia Financial Initiative SAR Review Team; Pandemic Response Accountability Committee (PRAC) Fraud Task Force; PRAC Law Enforcement Coordination Subcommittee; PRAC Data Analytics Subcommittee; Council of the Inspectors General on Integrity and Efficiency (CIGIE) COVID-19 Working Group; DOJ Stimulus Funds Fraud Working Group; District of Maryland SAR Review Task Force; Western District of Virginia SAR Review Task Force, Roanoke, Virginia; Western District of Virginia SAR Review Task Force, Abingdon, Virginia; Eastern District of Virginia SAR Review Task Force; Central Eastern District of Virginia SAR Review Task Force; Northern Virginia Eastern District of Virginia SAR Review Task Force; DOJ Foreign Corrupt Practices Act SAR Initiative; District of Columbia SAR Review Task Force; Southern District of West Virginia SAR Review Task Force; Northern District of West Virginia SAR Review Task Force.
Electronic Crimes Unit	Washington Metro Electronic Crimes Task Force; High Technology Crime Investigation Association; FBI Northern Virginia Cyber Task Force; DOJ Civil Cyber-Fraud Task Force; CIGIE Information Technology Committee; CIGIE Forensic Accountant Networking Group; CIGIE Financial Cyber Working Group; National Cyber Investigative Joint Task Force; FBI Headquarters Money Laundering, Forfeiture & Bank Fraud Unit; FBI Washington Field Office Cyber Task Force; FBI Las Vegas Cyber Task Force; FBI Los Angeles' Orange County Cyber Task Force; Secret Service Cyber Task Force, Newark, New Jersey; Secret Service Miami Cyber Fraud Task Force; Council of Federal Forensic Laboratory Directors; and International Organized Crime Intelligence and Operations Center (IOC-2).

Other Key Priorities

In addition to the audits, evaluations, investigations, and other reviews conducted during the reporting period, our Office has emphasized other priority initiatives that complement our efforts. Specifically, in keeping with our Guiding Principles, we have focused on **strengthening relations with partners and stakeholders, efficiently and effectively administering resources**, and **promoting leadership and teamwork**. A brief listing of some of our key efforts in these areas follows.

Strengthening relations with partners and stakeholders.

- Communicated with the 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.
- Redesigned and migrated our external website to a new platform to provide stakeholders enhanced opportunities to learn about the work of the OIG, the findings and recommendations our auditors and evaluators have made to improve FDIC programs and operations, and the results of our investigations into financial fraud.
- 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 Acting Chairman and other members of FDIC management of such cases, as appropriate.

- Maintained congressional working relationships by communicating with various Committee staff on issues of interest to them; providing them our *Semiannual Report to the Congress*; notifying interested congressional parties regarding the OIG's completed audit and evaluation work; 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.

- Maintained the OIG Hotline to field complaints and allegations of fraud, waste, abuse, and mismanagement affecting FDIC programs and operations from the public and other stakeholders. The OIG's Whistleblower Protection Coordinator also helped educate FDIC employees who had made or were contemplating making a protected disclosure as to their rights and remedies against retaliation for such protected disclosures. Our web-based hotline portal at https://www.fdicoig.gov/oig-hotline integrates seamlessly with our electronic Investigations Management System and enhances the efficiency and effectiveness of OIG Hotline operations. It also increases transparency and reporting capabilities that support our efforts to engage and inform internal and external stakeholders. During the reporting period, we opened 179 Hotline inquiries and closed 171. In total, during FY 2022, we opened 582 inquiries and closed 571.

- Supported OIG staff conducting outreach to various audiences and stakeholders. For example, the OIG's Chicago SAC spoke on a panel at the Women in Criminal Justice Conference. Additionally one of our Special Agents presented to a group of Forensic Accounting students at Northern Illinois University and at a local high school regarding the FDIC OIG and its mission. Two of our AEC staff spoke at a GAO Financial Management and Assurance Data Analytics Working Group meeting and at a CIGIE Connect, Collaborate, and Learn event on *Data Analytics Lessons Learned and Strategies for Finding the Right Data and Doing the Right Analysis*.

- Participated in several international outreach events. A Special Agent in our Electronic Crimes Unit joined co-case agents from the FBI in Germany and worked with law enforcement partners in support of an ongoing investigation into hacking by cyber criminals to buy and sell stolen bank account, credit card, and Personally Identifiable Information impacting FDIC institutions, among other illicit goods and services. Another of our Special Agents joined prosecutors from the U.S. Attorney's Office in Chicago, in conjunction with DOJ's Office of Overseas Prosecutorial Development, Assistance and Training, to train law enforcement and prosecutorial counterparts in Slovakia.

- Supported the IG community by attending monthly Council of the Inspectors General on Integrity and Efficiency (CIGIE) meetings and other meetings, such as those of the CIGIE Legislation Committee (which the FDIC IG Co-Chairs); the Diversity, Equity, Inclusion, and Accessibility (DEIA) Work 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; 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.

- Hosted the CIGIE Deputy Inspector General Working Group and discussed Operationalizing Diversity, Equity, Inclusion, and Accessibility; Return to the Office issues; and CIGIE/Legislation Updates. The training was attended by 41 leaders who collaboratively discussed challenges and solutions to a wide range of issues facing the community.
- Contributed to the CIGIE DEIA Work Group's Roadmap publication, *Advancing Diversity, Equity, Inclusion, and Accessibility: A Roadmap for Offices of Inspectors General*. The Roadmap includes routes and actions for OIGs to use in advancing diversity, equity, inclusion, and accessibility in the following areas: continuous education; staffing, recruitment, and hiring; promotions and professional development; performance, recognition, and awards; business supplier diversity; stakeholders and partners; safe, inclusive, and harassment-free workplaces; and data collection, assessment, and reporting.
- 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. Co-led CIGFO's report on *Preparing for and Managing Crises* and provided input to the CIGFO Annual Report.
- Acknowledged July 30 as National Whistleblower Appreciation Day. Invited a featured speaker, the Legal Director at the Government Accountability Project, to present his perspectives as an advocate for Federal whistleblowers over the past 43 years, during which he formally and informally assisted over 7,000 whistleblowers in defending themselves against retaliation and in making real differences on behalf of the public.
- Issued a joint announcement from the FDIC Inspector General and Acting FDIC Chairman addressing whistleblower protections for FDIC employees. Whistleblowers are the eyes and ears of the Agency, and they play a vital role in uncovering waste, fraud, abuse, and mismanagement.

- Shared information on CIGIE DEIA Efforts in a Government Executive article. The FDIC IG and Department of Education IG discussed the release of the CIGIE DEIA Work Group's Roadmap titled: *Advancing Diversity, Equity, Inclusion, and Accessibility: A Roadmap for Offices of Inspectors General*, and the Work Group's *Compendium of Office of Inspector General Reports Related to Diversity, Equity, Inclusion, and Accessibility*. The Compendium Project was led by one of the FDIC's Deputy IGs.
- Issued an Alert to inform the public about two types of impersonation scams: one purporting to be from the FDIC and the other from FDIC OIG personnel. The Alert also discussed tactics that scammers use in order to make their demands for funds appear to look legitimate, as well as information for contacting the FDIC OIG Hotline.
- Communicated with the Government Accountability Office (GAO) on ongoing efforts related to our oversight roles, risk areas at the FDIC, and issues and assignments of mutual interest.
- Coordinated with the Office of Management and Budget to address matters of interest related to our FY 2023 budget and proposed budget for FY 2024.
- Worked closely with representatives of the DOJ, including the Main Justice Department, FBI, and USAOs, to coordinate our criminal investigative work and pursue matters of mutual concern. Joined law enforcement partners in numerous financial, mortgage, suspicious activity report review, cyber fraud, and PRAC-related working groups nationwide.
- Promoted transparency to keep the American public informed through three main means: the FDIC OIG website to include, for example, 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; and presence on the IG community's Oversight.gov website, which enables users to access, sort, and search thousands of previously issued IG reports and other oversight areas of interest.
- Ensured transparency of our work for stakeholders on Oversight.gov by including press releases related to investigative cases and related actions, in addition to posting our audits and evaluations, and updated on an ongoing basis the status of FDIC OIG recommendations remaining unimplemented (73 as of September 30, 2022) and those recommendations that have been closed.

Administering resources prudently, safely, securely, and efficiently.

- Carried out spending and hiring plans to make optimum use of the OIG's $47.5 million in requested funding for FY 2023. For FY 2024, proposed a budget of $49.8 million. The increase is necessary to sustain prior investments in IT and data analysis, and support critical OIG contractual audit services focused on cybersecurity and statutorily-mandated reviews of failed banks.
- Implemented two OIG policies providing 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 entered Phase 3 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 strategic plan and IT Roadmap 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.
- Leveraged the FDIC OIG's Investigations Management System, the electronic case management system that replaced a predecessor electronic/paper file system and modernized 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 Hotline portal. Complainants and whistleblowers can now fill out a new intake form that captures information and intake of complaints directly into the system for assessment by the Hotline team. The Hotline portal link is accessible on the OIG's website.

- Continued efforts to stand up a new audit management platform that will further allow AEC to perform its work efficiently and effectively. Provided preliminary information to staff on how to use the system consistently, and coordinated with others in the IG community to ensure that the system will provide AEC staff and management with useful information for conducting audits and evaluations, dashboarding, and reporting.
- Completed build-out of the OIG's Electronic Crimes Unit's laboratory. The laboratory allows field Agents to remotely access a server-based lab environment which allows for the storage and processing of digital evidence into forensic reviewable data. This capability greatly increases the efficiency and effectiveness of the investigative process by allowing for much quicker actuation of data into e-discovery platforms. The build-out of the ECU will also facilitate financial fraud investigations, including cyber-crimes at banks.
- 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.
- Brought on board a Data and Analytics Officer to the OIG to coordinate office-wide data analytics activities and establish strategic direction for the OIG's efforts in this area.
- Advanced the OIG's data analytics project related to 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.
- Held Return to Office (RTO) information sessions for all OIG staff as a means to provide updates on transitioning from a period of mandatory telework to a hybrid working environment under the FDIC's Phase 3 of RTO.
- 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.
- 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 Assistant IG for Investigations; Director, Management Services; Special Agent in Charge of Headquarters Operations; Data and Analytics Officer; Chief of Staff; Special Agents; and Auditors/Evaluators.
- Oversaw contracts to qualified firms to provide audit, evaluation, IT, and other services to the OIG to provide support and enhance the quality of our work and the breadth of our expertise as we conduct audits, evaluations, and investigations, and to complement other OIG functions, and closely monitored contractor performance.
- Continued to integrate and leverage the use of MS Teams throughout our Office to promote virtual collaboration and communication, particularly during the period of the pandemic when mandatory telework for our Office was in place and recently during Return to Office Phase 3.
- 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 cost savings and ease of navigation for users.

Exercising leadership skills and promoting teamwork.

- Held the OIG's first Leadership Forum. This two-afternoon event featured a variety of presentations, panels, and discussions focused on leadership. Topics included Followership, a panel with the OIG Fellows, Being an Authentic Leader, Psychological Safety in the Workplace, leadership perspectives from OIG Managers, TEDTalks on leadership and performance, and an Executive leadership panel moderated by the Chair of the OIG's Workforce Council.
- Conducted training for OIG Special Agents hired since April 2020 to inform and orient them to the FDIC and the OIG. The IG, Deputy IGs, AIGI, and Deputy AIGI shared their vision and priorities. Other presentations included case studies; legal topics; Audits, Evaluations, and Cyber (AEC) briefing; FDIC programs overview; and other law enforcement-related topics.

- Finalized the OIG's first DEIA Strategic Plan, consisting of four components: *Purpose*: ways in which we strive to inspire each OIG team member to feel connected to our OIG Mission and Vision. This is accomplished through maintaining a diverse workforce in which all are engaged and can bring their authentic selves to the workplace in an environment of safety and acceptance and contribute to the success of the Office. *People*: in order to create a space of belonging in which we foster trusting relationships, invite opinions, and engage in relationship building, recognizing that our accomplishments are not possible without the hard work and dedication of the OIG team. *Processes:* to ensure that we uphold the OIG principles in our recruitment, hiring, promotion, recognition, awards, training, developmental opportunities, operations, procedures, workflows, policies, and technology. *Progress*: to hold ourselves accountable to these strategic goals, we will monitor progress as we mature our DEIA program.
- Maintained the OIG's Intranet site to promote teamwork 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 fielded questions from OIG staff and explored issues relating to the OIG's Federal Employee Viewpoint Survey results, mentoring and training, and plans for the OIG's eventual Return to Office in Phase 3.
- Hosted two events in the "Day in the Life" of an IG Executive series, organized by the OIG Workforce Council, where our OIG executives informally discussed their daily work routines and interactions with staff, so that OIG staff could 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.
- Shared expertise of the OIG's Engagement and Learning Officer who discussed Neurodiversity in Leadership, as part of the 2022 FedTalks! Speakers Series presented by American University's Key Executive Leadership Programs.

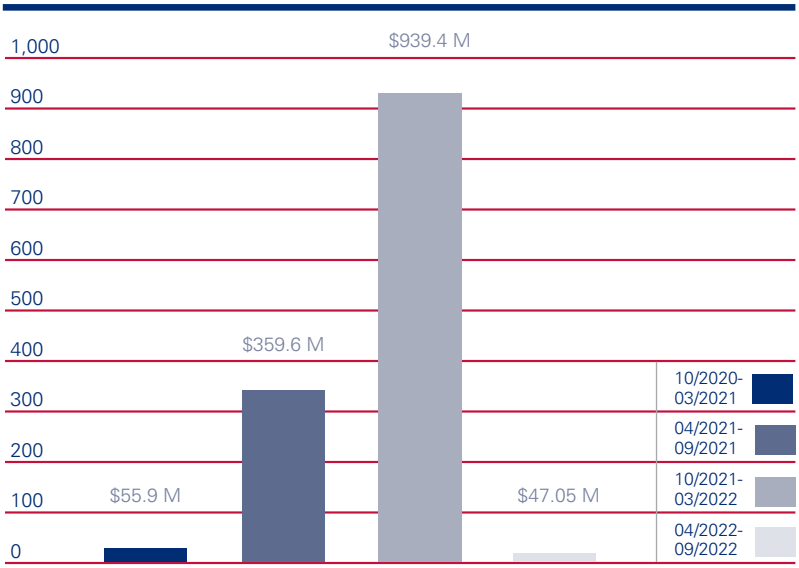
- Supported the OIG's Director of Management Services, who graduated from the African American Federal Executive Association Fellows class of 2022. These fellows represent a group of high-performing Federal leaders who participate in a rigorous developmental program designed to prepare them to compete for senior and executive leadership positions in the Federal Government.
- 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 component-specific and OIG-wide Coffee Chats, to promote community, teamwork, and collegiality among OIG staff.
- Conducted the OIG's 2022 Fellows Program for non-supervisory employees at the junior and senior levels. Four OIG staff completed the inaugural session and reported out at a September 2022 Managers Conference. 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.
- Took a leadership role in a working group on behalf of CIGIE's Audit and Inspection and Evaluation Committees related to Monetary Impact. The FDIC AIG for AEC and an Audit/Evaluation Manager led a group comprised of representatives from 20 OIGs across the community. The purpose of the group is to assess and help ensure consistency in how OIGs report and track monetary impacts from audits and evaluations. Shared results with others in the IG community. Also actively participated and made presentations as a member of CIGIE's Connect, Collaborate, and Learn group.
- 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. Hosted a series of events to highlight diversity, including Asian American, Native Hawaiian, and Pacific Islander Heritage Month; Jewish American Heritage Month; LGBTQI+ PRIDE Month; Hispanic Heritage Month; and Women's Equality Day.
- Continued active involvement in CIGIE's DEIA Work Group, of which the FDIC IG is Vice Chair. Supported issuance of *The Ally* Newsletter to share information from the Work Group, which works to affirm, advance, and augment CIGIE's commitment to promote a diverse, equitable, and inclusive workforce and workplace environment throughout the IG Community.
- Participated as a panelist during the CIGIE Professional Development Committee's event titled: "So You Want to Be Chief of Staff." The panelists, including the FDIC IG, discussed their unique journeys, including how to prepare and seek out opportunities for a leadership role and career as a chief of staff.
- Continued our leadership role in the CIGFO joint working group on Crisis Readiness. The OIG's AIG for AEC co-led the effort to compile and issue 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 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.

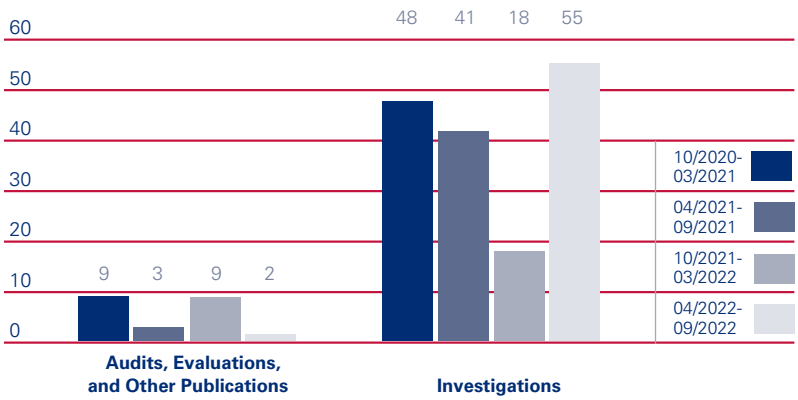
Cumulative Results (2-year period)

Nonmonetary Recommendations	
October 2020 – March 2021	56
April 2021 – September 2021	12
October 2021 – March 2022	77
April 2022 – September 2022	1

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	Page
Section 4(a)(2): Review of legislation and regulations.	41
Section 5(a)(1): Significant problems, abuses, and deficiencies.	4-9
Section 5(a)(2): Recommendations with respect to significant problems, abuses, and deficiencies.	4-12
Section 5(a)(3): Significant recommendations described in previous semiannual reports on which corrective action has not been completed.	42-43
Section 5(a)(4): Matters referred to prosecutive authorities.	58
Section 5(a)(5): Summary of each report made to the head of the establishment regarding information or assistance refused or not provided.	58
Section 5(a)(6): Listing of audit, inspection, and evaluation reports by subject matter with monetary benefits.	55
Section 5(a)(7): Summary of particularly significant reports.	4-9
Section 5(a)(8): Statistical table showing the total number of audit, inspection, and evaluation reports and the total dollar value of questioned costs.	55
Section 5(a)(9): Statistical table showing the total number of audit, inspection, and evaluation reports and the total dollar value of recommendations that funds be put to better use.	56

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	57
• no establishment comment was received within 60 days of providing the report to management	58
• there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.	44-54
Section 5(a)(11): Significant revised management decisions during the current reporting period.	58
Section 5(a)(12): Significant management decisions with which the OIG disagreed.	58
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.	60-61
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.	58
Section 5(a)(18): A description of metrics used for Section 5(a)17 information.	58
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.	58
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.	58
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.	58
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.	58

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 (CIGIE) 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 reporting period, among other activities, the Legislation Committee continued to engage with the Congress on the IG Independence and Empowerment Act, the Administrative False Claims Act, the Federal Information Systems Management Act, and certain provisions within the National Defense Authorization Act for Fiscal Year 2023.

In addition, the Committee coordinated with Congressional staff and experts in the IG community to provide technical assistance on various legislative proposals, including S.4908, the Strengthening Agency Management and Oversight of Software Assets Act, and proposed legislation that would update the Payment Integrity Information Act of 2019 and reintroduce the Chief Financial Officer Vision Act.

The Committee worked with leadership at CIGIE and the Pandemic Response Accountability Committee to consider and review draft legislative language providing for a permanent data analytics capability within CIGIE that benefits the IG Community. It also formed a working group, spearheaded by the FDIC OIG's General Counsel to develop and share feedback with Congressional staff on items to consider when legislating the establishment of new or Special IGs.

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 associated monetary amounts. In some cases, these corrective actions are different from the initial recommendations made in the audit 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 FDIC's Office of Risk Management and Internal Controls (ORMIC) and (2) the OIG's determination of when a recommendation can be closed. ORMIC has categorized the status of these recommendations as follows:

Management Action in Process: (seven recommendations from five 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 and soliciting feedback from additional stakeholders.
EVAL-21-002 **Critical Functions in FDIC Contracts** March 31, 2021	**5**	The FDIC is revising its current policy and procedures in order to implement a management oversight strategy for Critical Functions during the procurement planning process, for each contract involving Critical Functions.
	10	The FDIC is revising its current policy and procedures for determining when and how to assess for contractor over-reliance as part of the management oversight strategy.

Report Number, Title, and Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
Management Action in Process		
EVAL-22-002 **Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders** December 1, 2021	**1**	The FDIC updated procedures in the Formal and Informal Action Procedures (FIAP) Manual. The updates include a process for the Washington Office's review of proposed termination of Bank Secrecy Act Consent Orders and the documentation to provide for the review. The updated FIAP Manual is currently proceeding through the FDIC's internal approval process.
	2	The FDIC updated procedures in the Formal and Informal Action Procedures (FIAP) Manual. The updates include a process for the Washington Office's review of proposed termination of Bank Secrecy Act Consent Orders and the documentation to provide for the review. The updated FIAP Manual is currently proceeding through the FDIC's internal approval process.
AUD-22-003 **Sharing of Threat Information to Guide the Supervision of Financial Institutions** January 18, 2022	**3**	The FDIC has drafted a new Intelligence and Counterintelligence Directive, which incorporates the Charter. Additionally, a new Chief has been selected and other positions are in the interview/selection process.
EVAL-22-003 **The FDIC's Implementation of Supply Chain Risk Management** March 1, 2022	**5**	The Supply Chain Risk Management Team is developing a process, and associated procedures, to implement the Supply Chain Risk Management Directive, which will define a risk-based process for considering supply chain risks in individual procurement actions.

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-20-001 **Contract Oversight Management** October 28, 2019	The FDIC relies heavily on contractors for support of its mission, especially for information technology, receivership, and administrative support services. Over a 5-year period from 2013 to 2017, the FDIC awarded 5,144 contracts valued at $3.2 billion. Our evaluation objective was to assess the FDIC's contract oversight management, including its oversight and monitoring of contracts using its contracting management information system, the capacity of Oversight Managers (OM) to oversee assigned contracts, OM training and certifications, and security risks posed by contractors and their personnel. We concluded that the FDIC must strengthen its contract oversight management. Specifically, we found that the FDIC was overseeing its contracts on a contract-by-contract basis rather than a portfolio basis and did not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency. We also found that the FDIC's contracting files were missing certain required documents, Personally Identifiable Information was improperly stored, some OMs lacked workload capacity to oversee contracts, and certain OMs were not properly trained or certified. The report contained 12 recommendations to strengthen contract oversight.	12	1	NA

Table 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	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	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	
EVAL-21-002 **Critical Functions in FDIC Contracts** March 31, 2021	The FDIC relies on contractors to provide services in support of its mission. Some of these services cover Critical Functions. We conducted an evaluation to determine whether one of the FDIC's contractors was performing Critical Functions as defined by guidance issued by the Office of Management and Budget (OMB); and if so, whether the FDIC provided sufficient management oversight of the contractor performing such functions. The FDIC did not have policies and procedures for identifying Critical Functions in its contracts, as recommended by OMB Policy Letter 11-01 and best practices. However, we determined that Blue Canopy performed Critical Functions at the FDIC, as defined by OMB Policy Letter 11-01 and best practices. These services are critical to ensuring the security and protection of the FDIC's information technology infrastructure and data. A breach or disruption in these services could impact the security, confidentiality, integrity, and availability of FDIC information. Therefore, the FDIC needed proper oversight of the Critical Functions performed by Blue Canopy to ensure such a breach or disruption of service did not occur. The FDIC, however, did not identify the services performed by Blue Canopy as Critical Functions during its procurement planning phase. Therefore, the FDIC did not implement heightened contract monitoring activities for Critical Functions as stated in OMB's Policy Letter 11-01 and best practices. The report contained 13 recommendations aimed at strengthening the FDIC's internal controls over Critical Functions to align with OMB Policy Letter 11-01 and best practices.	13	12	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-21-004 **Security and Management of Mobile Devices** August 3, 2021	The FDIC deployed 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	2	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 this Memorandum advised the FDIC of our concerns in this area. While the FDIC employs certain talent management activities, the FDIC's retention management strategy did not have clearly defined goals, a process for collecting and analyzing data, and a process for measuring the effectiveness of its retention activities. The report contained three recommendations to improve the FDIC's management of employee talent and for the FDIC to measure the effectiveness of its retention efforts and activities.	3	1	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-22-001 **The FDIC's Information Security Program – 2021** October 27, 2021	The FDIC OIG engaged the firm of Cotton & Company LLP to perform our annual audit under the Federal Information Security Modernization Act of 2014 (FISMA). The audit was planned and conducted based on the Department of Homeland Security's reporting metrics: Fiscal Year 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1 (May 2021) (DHS FISMA Metrics). Inspectors General assign maturity level ratings to key security function areas and the overall security program, using a scale of 1-5. Ratings are determined by a simple majority where the most frequent level (mode) across the component questions will serve as the domain rating. The FDIC's overall information security program was operating at a Maturity Level 4. The FDIC had established certain information security program controls and practices that were consistent with information security policy, standards, and guidelines. However, the audit report describes significant control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. The report contained six recommendations to address these weaknesses.	6	3	NA
EVAL-22-001 **Reliability of Data in the FDIC Virtual Supervisory Information on the Net System** November 22, 2021	The FDIC maintains the Virtual Supervisory Information on the Net (ViSION) system, which supports FDIC supervision and insurance responsibilities. We conducted an evaluation to determine whether key supervisory information in the ViSION system was reliable, which was defined as accurate, complete, and supported by source documentation retained in the FDIC system of record. Among the four key ViSION system data elements tested, we found that two were not reliable. Specifically, we found an error for the Completion Date for 14 banks and an error for the Mail Date for 12 banks. We determined that the unreliable data resulted from weaknesses in the FDIC's procedures and practices for identifying and ensuring the quality of the ViSION system Completion Date and Mail Date data elements. We did not find errors for the Examination Ratings and Start Date data elements. We also found that the FDIC's risk-based assessment of ViSION system data was undocumented and outdated. The report contained six recommendations intended to strengthen the reliability of data in the FDIC ViSION system.	6	4	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-22-002 **Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders** December 1, 2021	The Bank Secrecy Act (BSA), and subsequent laws and regulations, established anti-money laundering (AML) recordkeeping and reporting requirements for financial institutions. When a financial institution is not in compliance with BSA/AML requirements, the FDIC may issue a Consent Order. We conducted an evaluation to determine whether the FDIC (i) considered factors similar to other Federal bank regulators in terminating BSA/AML Consent Orders; (ii) terminated BSA/AML Consent Orders in accordance with FDIC-established guidance; (iii) monitored FDIC Regional Office termination decision-making to ensure consistency across the Regions; and (iv) documented its actions. We found that the factors considered by the FDIC to terminate Consent Orders differed from the factors used by other Federal bank regulators. In addition, we found that FDIC guidance did not address how to apply the terms "substantial compliance" and "partially met." We also found that termination decisions were not centrally monitored, which would serve as an important internal control. Further, the FDIC did not consistently prepare and maintain documentation to support the monitoring of, and termination decision-making for, BSA/AML Consent Orders. The report contained 10 recommendations intended to enhance the FDIC's BSA/AML Consent Order termination-related guidance and procedures.	10	10	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
REV-22-001 **Whistleblower Rights and Protections for FDIC Contractors** January 4, 2022	Whistleblowers play an important role in safeguarding the Federal Government against waste, fraud, and abuse. In 2016, Congress enacted legislation to permanently expand whistleblower protections to the employees of Government contractors and subcontractors. We conducted a review to determine whether the FDIC aligned its procedures and processes with laws, regulations, and policies designed to ensure notice to contractors and subcontractors about their whistleblower rights and protections. We found that the FDIC procedures and processes were not aligned with laws, regulations, and policies designed to ensure notice to contractor and subcontractor employees about their whistleblower rights and protections. Further, the FDIC's Legal Division, under its separately delegated contracting authority, had not adopted any whistleblower provisions or included any whistleblower clauses in its contracts. In addition, we determined that the FDIC had not established any requirements for FDIC officials to determine whether contractors have carried out their obligations under the FDIC's Whistleblower Rights Notification Clause. The FDIC also did not obtain Confidentiality Agreements from all of its contractors and contract personnel, as required. We also found that Legal Division guidance may be unclear and confusing to contractor or subcontractor whistleblowers as to whom they should report criminal behavior or allegations of fraud, waste, abuse, or mismanagement. The report contained 10 recommendations intended to ensure that contractors and subcontractors are informed of their whistleblower rights and protections.	10	5	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-22-003 **Sharing of Threat Information to Guide the Supervision of Financial Institutions** January 18, 2022	To fulfill its mission, the FDIC acquires, analyzes, and disseminates threat information relating to cyber and other threats to the financial sector and FDIC operations. Effective sharing of threat information enriches situational awareness, supports informed decision-making, and guides supervisory strategies and policies. Our objective was to determine whether the FDIC established effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. We found that the FDIC did not establish effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. The FDIC acquired and analyzed certain information pertaining to threats against financial institutions and disseminated some information to certain supervisory personnel. However, we identified gaps in each component of the Threat Sharing Framework-Acquisition, Analysis, Dissemination, and Feedback. The report contained 25 recommendations.	25	20	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-22-003 **The FDIC's Implementation of Supply Chain Risk Management** March 1, 2022	In 2021, the FDIC awarded 483 contracts totaling over $2 billion for the acquisition of products and services. These products and services are provided by many types of vendors, contractors, and subcontractors. The supply chain for each vendor, contractor, or subcontractor may present unique risks to the FDIC. Therefore, the FDIC must implement a robust Supply Chain Risk Management (SCRM) Program to identify and mitigate supply chain risks that threaten its ability to fulfill its mission. 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 established in the SCRM Implementation Project Charter, including identifying and documenting known risks to its supply chain and establishing metrics and indicators for their continuous monitoring and evaluation. Further, the FDIC was not conducting supply chain risk assessments during its procurement process. In addition, FDIC had not integrated Agency-wide supply chain risks into its Enterprise Risk Management processes. We also determined that Contracting Officers did not maintain contract documents in the Contract Electronic File system, as required. The report contained nine recommendations to improve the FDIC's SCRM Program and retention of contract documents. **Note:** *Recommendation 9 in this report was previously closed in July 2022 based on the FDIC's implementation of controls in a new FDIC Acquisition Management System. However, due to the FDIC subsequently reverting back to the predecessor system, this recommendation can no longer be implemented as intended and thus remains unresolved.*	9	6	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
REV-22-002 **Controls Over Payments to Outside Counsel** March 16, 2022	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. We conducted a review to determine whether the Legal Division's review and oversight of payments to OC could be improved. We found that the FDIC Legal Division should improve its review and oversight of payments to OC in four areas: (1) increasing the analysis of FDIC data; (2) providing clear guidance in specific areas; (3) sharing the results of post-payment reviews with those involved in the invoice review process; and (4) providing a periodic training program to reinforce expectations and requirements. The report contained eight recommendations designed to improve the FDIC Legal Division's review and approval of payments to OC, ensure consistency and conformance with the FDIC's procedural requirements, and promote the FDIC's efforts to reduce and recover disallowed costs.	8	7	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**	
Information Technology and Cybersecurity				
AUD-22-004 September 27, 2022	*The FDIC's Information Security Program - 2022*			
Totals for the Period		**$0**	**$0**	**$0**

Other products issued:

- *Background Investigations for Privileged Account Holders (AEC Memorandum-22-002) June 22, 2022.*

Table IV: Audit and Evaluation Reports Issued with Questioned Costs

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

As of the end of the semiannual period, management had not made a management decision on two of the recommendations in the report related to the finding. Specifically, we recommended that the FDIC:

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

At the time we issued our report, the FDIC stated that it concurred with Recommendation 13. Further, while the FDIC did not concur with Recommendation 14, its non-concurrence was based on a misunderstanding that the OIG recommendation was calling for the construction of Sensitive Compartmented Information Facilities (SCIF) for FDIC Regional Offices. Our recommendation, however, focused on a means and infrastructure to share classified information at an appropriate level and did not call for the construction of SCIFs.

Nevertheless, the FDIC has indicated it now plans to reverse its longstanding position and eliminate the security clearances for Regional personnel (except for the Regional Directors in New York and Dallas), for the limited purposes of a "severe business continuity event" and its few personnel involved in the Interagency Country Exposure Review Committee (ICERC)), rather than implementing the recommendations to improve the processes for sharing classified National Security Information with its Regional Offices.

As a result of this reversed position, we consider Recommendations 13 and 14 to be unresolved and will work with the FDIC to seek resolution during the audit follow-up process. If resolution is not reached by February 2023, the OIG will elevate the recommendations to the Audit Follow-up Official for a final Management Decision.

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	55
Number of Persons Referred to the Department of Justice for Criminal Prosecution	169
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	0
Number of Indictments and Criminal Informations	56

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

Table 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

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

FDIC OIG Review Activity for the Period April 1, 2022 through September 30, 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. Peer reviews of our audit and evaluation functions are posted on our website at: www.fdicoig.gov.

Definition of Audit Peer Review Ratings

Pass: The system of quality control for the audit organization has been suitably designed and complied with to provide the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

Pass with Deficiencies: The system of quality control for the audit organization has been suitably designed and complied with to provide the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects with the exception of a certain deficiency or deficiencies that are described in the report.

Fail: The review team has identified significant deficiencies and concludes that the system of quality control for the audit organization is not suitably designed to provide the reviewed OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects or the audit organization has not complied with its system of quality control to provide the reviewed OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

Audit Peer Reviews

On a 3-year cycle, peer reviews are conducted of an OIG audit organization's system of quality control in accordance with the CIGIE *Guide for Conducting Peer Reviews of Audit Organizations of Federal Offices of Inspector General*, based on requirements in the Government Auditing Standards (Yellow Book). Federal audit organizations can receive a rating of pass, pass with deficiencies, or fail.

The Department of State OIG conducted a peer review of the FDIC OIG's audit function and issued its report on the peer review on September 16, 2022. The FDIC OIG received a rating of **Pass**. In the Department of State OIG's opinion, the system of quality control for the audit organization of the FDIC OIG in effect for the year ended March 31, 2022, had been suitably designed and complied with to provide the FDIC OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards and applicable legal and regulatory requirements in all material respects.

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

Inspection and Evaluation Peer Reviews

The Tennessee Valley Authority OIG conducted a peer review of the FDIC OIG's evaluation function and issued its report on the peer review on June 28, 2022. This required external peer review was conducted in accordance with CIGIE Inspection and Evaluation Committee guidance as contained in the *CIGIE Guide for Conducting External Peer Reviews of Inspection and Evaluation Organizations of Federal Offices of Inspector General*, December 2020.

The External Peer Review Team assessed the extent to which the FDIC OIG complied with standards from CIGIE's Quality Standards for Inspection and Evaluation (Blue Book), January 2012. Specifically, the Review Team assessed quality control, planning, data collection and analysis, evidence, records maintenance, reporting, and follow up. The assessment included a review of the FDIC OIG's internal policies and procedures implementing the seven covered Blue Book standards. It also included a review of selected inspection and evaluation reports issued between April 1, 2021, and March 31, 2022, to determine whether the reports complied with the covered Blue Book standards and the FDIC OIG's internal policies and procedures.

The Review Team determined that the FDIC OIG's policies and procedures generally were consistent with the seven Blue Book standards addressed in the external peer review. Additionally, all three reports reviewed generally complied with the covered Blue Book standards and the FDIC OIG's associated internal policies and procedures.

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.

Congratulations

Congratulations to CIGIE Award Winners

The following FDIC OIG teams were recognized at the CIGIE Awards Ceremony in October:

Award for Excellence - Audit — The Sharing of Threat Information to Guide the Supervision of Financial Institutions

This review examined the Threat Information Sharing processes at the FDIC to acquire, analyze, disseminate, and use relevant and actionable threat information. The report made 25 recommendations for improvements and efficiencies at the Agency, and as a result, the FDIC is creating an entirely new function, the Intelligence & Threat Sharing Unit. In addition, we identified that there was no requirement for banks to promptly report destructive cyber incidents that could threaten the safety and soundness of insured financial institutions; subsequently, the financial regulators promulgated a rule requiring banks to report such computer security incidents.

Team Members:

- Joe Nelson
- Judy Hoyle
- Billy Cheng
- Abby Woods
- Danietta Asugo
- Melissa Mulhollen
- Tom Ritz
- Regina Sandler
- Cynthia Hogue

Award for Excellence - Investigation — Stephen Calk Investigation

Stephen Calk, the former Chairman and Chief Executive Officer of Federal Savings Bank, was investigated for corruptly using his position as the head of a bank to issue millions of dollars in loans to a lobbyist and political consultant, in exchange for personal benefit. These benefits included the defendant's placement on the Economic Advisory Council during the campaign and assistance in obtaining a senior position with the prior Presidential Administration. The defendant was convicted at trial by a jury and subsequently sentenced to a year and a day of imprisonment and ordered to pay a $1.25 million fine.

Team Members: James Greczek, Special Agent, FDIC OIG, New York, along with our law enforcement partners from the FBI and U.S. Attorney's Office in the Southern District of New York.

Other FDIC OIG personnel recognized at the CIGIE Awards Ceremony based on nominations from other OIGs:

Senior Special Agent Vikas Arora – Nominated by the Small Business Administration OIG for his work on a team investigating a criminal enterprise that defrauded pandemic relief programs under the CARES Act. The investigation resulted in savings of more than $18 million, forfeitures totaling $7.6 million, and $31.5 million in restitution.

Special Agent in Charge Anand Ramlall and Senior Special Agent Clarice Bramley — Nominated by the Federal Housing Finance Agency OIG for their efforts on an investigation leading to the successful prosecution of a multi-million dollar mortgage lending and servicing fraud scheme.

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

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

FDIC-009-2022