FDIC Office of Inspector General

Semiannual Report to the Congress

April 1, 2021 – September 30, 2021

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 5,770 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured $9.49 trillion in domestic deposits in 4,951 institutions, of which the FDIC supervised 3,194. The Deposit Insurance Fund balance totaled $120.5 billion as of June 30, 2021. Active receiverships as of June 30, 2021 totaled 220, with assets in liquidation of about $206 million.

Semiannual Report to the Congress

April 1, 2021 – September 30, 2021

Office of Inspector General

Federal Deposit Insurance Corporation

Inspector General's Statement

On behalf of the Office of Inspector General (OIG) at the Federal Deposit Insurance Corporation (FDIC), I am pleased to present our Semiannual Report for the period from April 1, 2021 through September 30, 2021.

During this reporting period, our audits and evaluations identified weaknesses and areas for improvement, and we provided 12 recommendations to the FDIC to strengthen controls and increase efficiencies. For example, in our audit of the FDIC's Security and Management of Mobile Devices, we found that the FDIC did not have effective controls in three areas, including outdated policies, procedures, and guidance that did not reflect current business practices. In this report, we made recommendations to mitigate the risk of cyber threats and malware that could compromise sensitive FDIC data by allowing an actor to exploit vulnerabilities on the devices. We also issued memoranda on the FDIC's Management of Employee Talent and its External Wireless Network Solution Cloud Service, and made recommendations for improvements in these areas as well.

Every year, we issue our Top Management and Performance Challenges document, which helps to identify the most urgent risks on which policy makers should focus attention. This report is thoroughly researched based on our observations and experiences, academic literature, information from other Government agencies and officials, oversight bodies, and the private sector. The Challenges document also provides a strategic perspective that drives our work for planning purposes. Based on our identification of these high-risk Challenges, we are examining the FDIC's Supply Chain Risk Management; Collection and Sharing of Threat Information; Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders; Examination of Government-Guaranteed Loan Programs; and Implementation of the Information Technology Risk Examination (InTREx) Program; among others.

In addition, our OIG Special Agents and investigative support staff have continued to work closely with law enforcement partners to investigate criminal and administrative matters involving sophisticated, complex multi-million-dollar frauds. These schemes involve bank fraud, embezzlement, money laundering, currency exchange manipulation, and other crimes committed by and against banks, executives, directors, officials, insiders, financial professionals, and others. We are also working to detect and investigate cyber-criminal cases that threaten the banks and banking sector. During the past 6 months, our cases resulted in 58 indictments, 66 convictions, 51 arrests, and more than $359 million in fines, restitution ordered, and other monetary recoveries.

Our Office continues to play a key role in the investigation of individuals and organized groups perpetrating fraud through the Paycheck Protection Program (PPP) under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) and the American Rescue Plan (ARP). To date, we have opened more than 100 cases associated with fraud in the CARES Act and ARP programs. Such cases involve fraudsters who aim to steal funds from the Government programs intended for those most in need during the pandemic. Over the past 6 months, our collaborative work in this area accounted for 26 indictments, 23 convictions, 15 arrests, and nearly $44 million in fines, restitution ordered, and asset forfeitures.

Our ongoing investigative efforts also include coordination and support of the Pandemic Response Accountability Committee's Fraud Task Force and the Department of Justice's COVID-19 Fraud Enforcement Task Force. The FDIC OIG is a key inter-agency partner, and we will continue to work in close collaboration with our law enforcement partners.

I am especially grateful to the dedicated women and men of our Office. Despite the challenges presented by the global pandemic, we continue to produce quality work. We appreciate the support of Members of Congress, and that of the FDIC Chair and Board of Directors. We remain committed to serving the American people as an independent voice and a leader in the Inspector General community.

Jay N. Lerner
Inspector General
October 2021

Table of Contents

Acronyms and Abbreviations

ATO	Authorization to Operate
BSA/AML	Bank Secrecy Act/Anti-Money Laundering
C&C	Cotton & Company LLP
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CFETF	Coronavirus Fraud Enforcement Task Force
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
COVID-19	Coronavirus Disease 2019
D&I	Diversity and Inclusiveness
DE&I	Diversity, Equity, and Inclusion
DIF	Deposit Insurance Fund
DOJ	Department of Justice
ECU	Electronic Crimes Unit
EIDL	Economic Injury Disaster Loan
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FHFA	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
HSI	Homeland Security Investigations
IG	Inspector General
InTREx	Information Technology Risk Examination
IRS-CI	Internal Revenue Service-Criminal Investigation
IT	Information Technology
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
SAR	Suspicious Activity Report
SBA	Small Business Administration
SME	Subject Matter Expert
TIGTA	Treasury Inspector General for Tax Administration
USAO	United States Attorney's Office

Introduction and Overall Results

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

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

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

Overall Results (April 1, 2021–September 30, 2021)	
Audit, Evaluation, and Other Products Issued	**3**
Nonmonetary Recommendations	**12**
Investigations Opened	**55**
Investigations Closed	**41**
Judicial Actions:	
Indictments/Informations	**58**
Convictions	**66**
Arrests	**51**
OIG Investigations Resulted in:	
Fines of	**$187,800**
Restitution of	**$305,635,745** *
Asset Forfeitures of	**$53,779,792**
Total	**$359,603,337** **
Referrals to the Department of Justice (U.S. Attorneys)	**124**
Responses to Requests Under the Freedom of Information/Privacy Act	**10**

*Restitution this period includes $67,598,511 that was ordered joint and several with other individuals sentenced during the period, and $57,671,799 that was ordered joint and several with an individual sentenced in a prior period.

**Total does not include a negotiated monetary settlement of $600,000 or $205,305 in fees that were returned to the Small Business Administration.

Audits, Evaluations, and Other Reviews

The FDIC OIG seeks to conduct superior, high-quality audits, evaluations, and reviews. We do so by:

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

During the reporting period, audit and evaluation work covered activities related to information technology (IT) and human resources management. Audit and evaluation reports issued during the period resulted in 12 recommendations to management. Additionally, as a member of the Council of Inspectors General on Financial Oversight (CIGFO), our Office highlighted work that contributed to financial stability over the past year in the CIGFO Annual Report, issued in July 2021.

Importantly, our Office also reviews the failures of FDIC-supervised institutions causing material losses to the Deposit Insurance Fund (DIF). 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 a failed bank review.

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

Audits and Evaluations

Security and Management of Mobile Devices

During the reporting period, we issued our report on the Security and Management of Mobile Devices. The objective was to determine whether the FDIC had established and implemented effective controls to secure and manage its mobile devices.

The FDIC deploys nearly 4,600 smartphones and more than 150 tablets to its employees and contractor personnel to support its business operations and communications. Although these mobile devices offer opportunities to improve business productivity, they also introduce the risk of cyber threats that could compromise sensitive FDIC data. Such threats may include malicious software known as "malware" that can allow an actor to exploit vulnerabilities on the devices; eavesdrop wireless communications over public networks; and collect and monitor data on mobile applications installed by users, such as the user's location, contacts, and browsing history. The FDIC uses a cloud-based mobile device management (MDM) solution to secure and manage its smartphones and tablets.

The audit found that the FDIC had not established or implemented effective controls in three of nine areas assessed, because the controls and practices did not comply with relevant Federal or FDIC requirements and guidance. Specifically,

- The FDIC's Policies, Procedures, and Guidance pertaining to mobile devices were outdated and did not reflect current business practices and address key elements recommended by the National Institute of Standards and Technology (NIST);
- The FDIC did not conduct Control Assessments of the MDM solution annually; and
- FDIC Logging and Monitoring practices were not guided by written procedures.

Controls and practices in the areas of Awareness Training, Billing Analysis, and Configuration Management were partially effective because they complied with some, but not all, relevant security requirements and guidelines. The FDIC implemented effective controls and practices in the areas of Asset Management, Incident Response, and Data Protection.

The report contained nine recommendations. We recommended that the FDIC fully assess the risks associated with its mobile devices; establish mobile device policies and guidance consistent with NIST guidance; and require Bring Your Own Device users to sign service agreements. We also recommended that the FDIC strengthen awareness training pertaining to the use of mobile devices and define roles, responsibilities, and procedures for reviewing logs generated by the MDM solution. We further recommended that the FDIC routinely report mobile device usage information to FDIC business units and require them to suspend or terminate service for devices that are no longer needed. By implementing this recommendation, we estimated that the FDIC could achieve cost savings. Finally, we recommended that the FDIC develop and implement written roles, responsibilities, and procedures for testing software updates for mobile devices.

The FDIC's Management of Employee Talent

We issued a memorandum to the FDIC regarding its Management of Employee Talent. We conducted an evaluation of the FDIC's allocation and retention of its examination staff 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 concluded our evaluation.

However, in conducting our evaluation, we identified broader concerns regarding the FDIC's overall management of employee talent, and our memorandum advised the FDIC of weaknesses in this area. The term "talent management" encompasses attracting and retaining talent for improving organizational performance, while also considering attrition. Talent management refers to a process to address competency gaps, by implementing and maintaining programs to attract, develop, promote, and retain talent, particularly for mission-critical positions and occupations. Talent management should be a focus for the FDIC, especially given the need to retain employees with skills, experience, and leadership capabilities. Additionally, talent management is important as the FDIC looks to reshape its workforce to transition the Agency and operations following the pandemic.

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. Therefore, we recommended that the FDIC:

- Develop and implement defined, objective, quantifiable, and measurable goals related to retention management at the FDIC.
- Develop and implement a process to collect and analyze the relevant data regarding employee retention across the FDIC and provide the data and analyses to Divisions and Offices.
- Develop metrics and indicators to assess the effectiveness of the FDIC's employee retention activities and to determine if the FDIC's retention activities are achieving their desired results and outcomes.

The FDIC concurred with the three recommendations.

Concerns Related to the FDIC's Pending Authorization to Operate Its External Wireless Network Solution Cloud Service

While conducting our ongoing audit of Security Controls Over FDIC Wireless Networks, we identified concerns that required the Chief Information Officer's (CIO) prompt attention. These concerns related to the FDIC's pending Authorization to Operate (ATO) its external wireless network solution cloud service (Wireless solution). The Wireless solution allows system administrators to set up, monitor, and configure wireless networks through a cloud-based service. We issued a memorandum to advise the FDIC of our concerns in this area.

Although the Chief Information Officer Organization (CIOO) followed the Outsourced Solution Assessment Methodology processes prior to placing the Wireless solution in operation, the CIOO had not been able to fully assess the risks and authorize the Wireless solution to operate in the FDIC's IT environment consistent with NIST guidance. We therefore advised that the CIOO should consider whether additional actions should be taken, such as putting in place an acceptance of risk (AR) for the Wireless solution pending the completion of the FedRAMP authorization process and ATO. In addition, we noted that it is important that the FDIC's Cyber Risk Management Section be aware of all uses of the Wireless solution in the FDIC environment to ensure risks are fully evaluated as part of the AR and ATO processes, as applicable.

In responding to our memorandum, the FDIC indicated it had taken several actions to fully assess the risks and authorize all systems authorized under legacy approvals, including issuing a memorandum, signed by the Authorizing Official, recording the decision to allow the continued operation of the systems, including the wireless solution. The assessment for the wireless solution is planned to occur following the solution's FedRAMP authorization, to ensure that use cases are known and stakeholders are fully informed.

Annual Report of the Council of Inspectors General on Financial Oversight

CIGFO published its annual report for 2021 during this reporting period. This report highlights CIGFO activities and presents write-ups from the member agency IGs related to their work to help strengthen the financial system through their oversight of Federal programs.

Coverage in the CIGFO report of the FDIC OIG's significant work during the past year includes discussion of the Top Management and Performance Challenges facing the FDIC, Crisis Readiness, Enterprise Risk Management, Personnel Security and Suitability, and our In-Depth Review of Enloe State Bank. 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. Additional information about what the CIGFO member IGs are reporting and how they are helping to ensure financial stability can be found on CIGFO's site at https://oig.treasury.gov/Council-of-Inspectors-General-on-Financial-Oversight.

Ongoing Work

Our Office continues to conduct work in areas that we identified in 2020 as the Top Management and Performance Challenges Facing the FDIC:

- Ensuring Readiness in a Pandemic Environment;
- Mitigating Cybersecurity Risks in the Banking Sector;
- Improving IT Security Within the FDIC;
- Securing FDIC Personnel, Facilities, and Information;
- Promoting and Aligning Strong Governance at the FDIC;
- Augmenting the FDIC's Sharing of Threat Information;
- Supporting Diversity in Banking;
- Managing Human Resources and Planning for the Future Workforce;
- Overseeing Contracts and Managing Supply Chain Risk; and
- Enhancing Rulemaking at the FDIC.

At the end of the reporting period, we had 14 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:

- *The FDIC's Termination of Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Consent Orders*. The objective is to determine whether the FDIC considered factors similar to other Federal bank regulators in terminating BSA/AML Consent Orders, terminated BSA/AML Consent Orders in accordance with FDIC-established guidance, monitored FDIC Regional Office termination decision-making to ensure consistency across the Regions, and documented its actions.
- *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.
- *Receiving and Sharing Threat Information to Guide the FDIC's Supervisory Program*. The objective is 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.

- *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.
- *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.
- *Supply Chain Risk Management*. The objective is to determine whether the FDIC developed and implemented its Supply Chain Risk Management Program in alignment with the Agency's goals and best practices.

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

Finally, of note during the reporting period, we are conducting our annual assessment of the *Top Management and Performance Challenges Facing the FDIC*. Our assessment helps to identify the most urgent risks on which policy makers should focus attention. We research and identify areas of challenge based on our observations and experiences; academic literature; and information from other Government agencies and officials, oversight bodies, and the private sector. As in the past, the upcoming Challenges document will provide a strategic perspective that drives our work for the coming year.

This document will be issued in February 2022 and is provided to FDIC management for inclusion in the FDIC's Annual Report. We will post our assessment on our external website, along with a video summarizing the Challenges.

Pandemic Response Accountability Committee Updates

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

PRAC Data Analytics Expo: The PRAC hosted a Data Analytics Expo where members of the IG community presented on their analytics and underlying technology capabilities. The expo resulted in the sharing of community best practices and assisted the PRAC with providing tools and services that augment, rather than replicate, IG analytic capabilities.

New PRAC Identity Fraud Working Group: The PRAC announced creation of the new Identity Fraud Reduction and Redress Working Group. IGs across government will share data and findings to fight fraudsters and protect individuals' pandemic relief money.

Testimony: *Assessing the Federal Government's COVID-19 Relief and Response Efforts and Impact*. In July, the Chair of the PRAC testified before the U.S. House of Representatives Committee on Transportation and Infrastructure about the Federal response to the COVID-19 pandemic, oversight efforts, areas for improvement, and the impact of pandemic relief on the transportation sectors and their workers.

Roundtable Listening Forum with the National Academy of Public Administration: The PRAC and the National Academy of Public Administration held a roundtable event to examine the impact of pandemic response programs and spending on underserved communities and the extent to which the pandemic response was equitable. It was a conversation about lessons learned and recommendations to improve administration of the American Rescue Plan and future disaster relief efforts.

Relief Fund Data: The PRAC released an updated dataset of Coronavirus Relief Fund spending by states, eligible local governments, Tribal governments, the District of Columbia, and U.S. Territories. The PRAC also released Provider Relief Fund data on its website and will continue to share updates on the money that went to hospitals, medical offices, and doctors in response to the COVID-19 crisis.

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

The FDIC OIG investigates significant matters of wrongdoing and misconduct relating to FDIC employees, contractors, and institutions. We do so by:

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

Our investigations are largely based upon referrals from the FDIC; our law enforcement partners, including other OIGs; the Department of Justice (DOJ), including U.S. Attorneys' Offices (USAO) and the Federal Bureau of Investigation (FBI); and referrals from our OIG Hotline. Our Office plays a key role in investigating sophisticated schemes of bank fraud, money laundering, embezzlement, and currency exchange rate manipulation. Our cases often involve bank executives, officers, and directors; other financial insiders such as attorneys, accountants, and commercial investors; private citizens conducting businesses; and in some instances, FDIC employees.

DOJ COVID-19 Fraud Enforcement Task Force

In May 2021, the Attorney General announced the establishment a COVID-19 Fraud Enforcement Task Force (CFETF). The FDIC OIG supports this effort as a key interagency partner for the Department of Justice (DOJ). Our Office is contributing to the CFETF efforts in: (1) identifying cross-governmental resources, investigative techniques, and information for uncovering fraud schemes and the actors who perpetrate them; (2) harnessing what we have learned about COVID-19-related and other types of fraud from past efforts; and (3) deterring, detecting, and disrupting future frauds. This effort augments and incorporates existing coordination mechanisms between the OIG and DOJ and we will continue to work in close coordination with related efforts underway throughout the Federal government.

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

Since many of the programs in the CARES Act and related legislation are administered through banks and other insured institutions, our Office of Investigations has been actively involved in investigating pandemic-related financial crimes affecting the banks. In addition, our Office regularly coordinates with the supervisory and resolutions components within the FDIC to watch for developing patterns of crimes and other trends in light of the pandemic. Our Special Agents have been working proactively with other OIGs; 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. Notably, during the reporting period, the FDIC OIG's efforts related to the Federal government's COVID-19 pandemic response resulted in 26 indictments/criminal complaints, 15 arrests, and 23 convictions, often involving fraud in the Paycheck Protection Program (PPP). Fines, restitution ordered, and asset forfeitures resulting from these cases totaled nearly $44 million.

The cases discussed below are illustrative of some of the OIG's investigative success during the reporting period. They are the result of efforts by FDIC Special Agents and support staff in Headquarters, Regional Offices, and the OIG's ECU. As noted, these cases reflect the cooperative efforts of OIG investigators, FDIC Divisions and Offices, other OIGs, USAOs, and others in the law enforcement community throughout the country. These working partnerships contribute to ensuring the continued safety and soundness of the Nation's banks and help ensure integrity in the FDIC's programs and activities. Actions in cases involving COVID 19-relief fraud are also included in our discussion of cases from the reporting period.

International Wholesale Currency Dealer Pleads Guilty to Unlawfully Operating in the United States

On July 29, GPOMCT Grupo Empresarial S.A. De C.V., an international, Mexico-based wholesale currency dealer and currency exchange business, pleaded guilty to unlawfully operating in the United States.

As admitted in the plea agreement, GPOMCT imported shipments of currency from Mexico into the United States for the purposes of selling Mexican pesos to a currency exchange located in San Ysidro, California, identified only as "MSB 1" in the plea agreement. Between September 2019 and September 2020, GPOMCT imported approximately 195 shipments of currency—each worth between $90,000 and $100,000 in U.S. dollars—and delivered them to MSB 1 in San Ysidro. GPOMCT used the services of an armored car company to collect currency from MSB 1 as payment and deliver it to a third-party intermediary in Miami, Florida.

By offering a variety of services as a wholesale currency dealer, GPOMCT admitted that it operated as an unlicensed money transmitting business in the United States and agreed to criminally forfeit $1.1 million as property involved in its unlawful operations. By failing to register as a money transmitting business, GPOMCT did not file currency and transactional reports with the Department of the Treasury, as required by the Bank Secrecy Act, nor did it subject itself to inspection by the Department of the Treasury for compliance with these financial laws and regulations.

Source: USAO, Southern District of California, and Department of Homeland Security-Investigations (HSI).
Responsible Agencies: FDIC OIG and HSI. Prosecuted by the USAO, Southern District of California.

New Jersey Man Sentenced to More Than 5 Years in Federal Prison for $3.5 Million Bank Fraud Scheme

On April 29, Mehul Khatiwala, of Voorhees, New Jersey, was sentenced to 63 months in Federal prison, followed by 4 years of supervised release, for conspiracy to commit bank fraud and for three counts of bank fraud, in connection with schemes to fraudulently obtain a total of approximately $15 million in loans from Cecil Bank. Khatiwala was also ordered to pay a $50,000 fine and forfeit and pay restitution of $3,593,801.

According to his plea agreement, from February 2011 through January 2014, Khatiwala and two co-conspirators executed a scheme to defraud Cecil Bank, the Small Business Administration (SBA), and other financial institutions by misrepresenting material facts in order to obtain financing for the purchase of two hotels and a multifamily residential property. Khatiwala defaulted on the loans, causing losses to Cecil Bank and the SBA of more than $3.5 million.

Responsible Agencies: FDIC OIG, Federal Housing Finance Agency (FHFA) OIG, SBA OIG, and the Special Inspector General for the Troubled Asset Relief Program. Prosecuted by the USAO, District of Maryland.

Fifth Employee in Cash Flow Partners' Bank Fraud Conspiracy Admits Role in Multimillion-Dollar Loan Scheme

On June 30, Cesar Mendez, of New York City, New York, pleaded guilty to an information charging him with one count of conspiracy to commit bank fraud.

According to documents filed in this case and statements made in court, between March 2016 and September 2019, Cash Flow Partners LLC, a business consulting firm with offices in New York and New Jersey, released internet advertisements and held seminars offering to assist customers in obtaining bank loans, including loans insured by the FDIC. When customers submitted documentation supporting their bank loan applications to Cash Flow Partners, Mendez and others created false documentation to make customers' loan applications appear more financially viable than they actually were. Victim banks sustained losses of over $4 million.

Four of Mendez's conspirators, Edward Espinal, Gladys Collins, Jennie Frias, and Raymundo Torres, previously pleaded guilty to charges relating to their role in the Cash Flow bank fraud conspiracy and are awaiting sentencing.

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

Maryland Man Sentenced to 7½ -Year Prison Term for Fraud, Money Laundering, and Identity Theft Scheme

On August 13, Kelvin Otunyo, of Hyattsville, Maryland, was sentenced to 90 months in prison, followed by 4 years of supervised release, for his role in at least six schemes to deposit and launder stolen and unauthorized checks valued at more $350,000. He was also ordered to pay a restitution judgment in the amount of $124,157 and a forfeiture money judgment in the amount of $303,207.

Otunyo pleaded guilty on April 1, 2021 to two counts of bank fraud, one count of aggravated identity theft, and two counts of conspiracy to commit money laundering. According to court papers, between August 2017 and at least August 2018, Otunyo and co-conspirators engaged in a series of schemes in which they obtained stolen or unauthorized checks from victims, established fraudulent shell corporations and bank accounts, and deposited or attempted to deposit the checks before laundering the resulting proceeds. The frauds were committed using false IDs and fraudulent aliases. Otunyo also procured the real name and Social Security Number of an identity theft victim for use in one of the schemes. In total, the six schemes involved nine stolen or unauthorized checks from eight victims totaling $355,745.

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

Farm Equipment Chief Executive Officer Sentenced to Prison, Ordered to Pay $6.3 Million in Restitution

On September 16, Rickey Carter, of Nashville, Georgia, who pleaded guilty to orchestrating a complicated fraud involving millions of dollars of loans by multiple creditors, was sentenced to 63 months in prison, followed by 5 years of supervised release, and was ordered to pay more than $6.3 million in monetary restitution to the banks and creditors he defrauded.

Carter was the President and Chief Executive Officer of Nashville Tractor (NTI), a business that sold and leased agricultural and construction equipment, attachments, and parts. In 2016, he obtained an SBA loan in the principal amount of $5 million. At the same time, NTI obtained a new line of credit and signed a credit agreement in the amount of $625,000. In 2010, Carter had entered into an ongoing Wholesale Financing and Security Agreement with CNH Industrial Capital America, LLC (CNH) to finance NTI's purchases of inventory for retail sale or lease. He also entered into a Retail Financing Agreement with CNH under which CNH would purchase NTI's interest in retail installment contracts for the purchase of agricultural and construction equipment with retail customers. The CNH agreement was a primary source of farm and construction equipment inventory for NTI.

During 2015, NTI began having financial and cash flow issues, which made it difficult to make payments due on the loans and to make payroll. During that time, Carter began a practice of selling equipment that NTI held in trust but not paying the cash over to CNH and other creditors, as required.

As part of the fraudulent scheme, Carter falsified NTI's financial records in order to inflate the company's net worth. Carter also created fraudulent retail installment contracts for the sale or lease of numerous items of equipment with CNH using the names of real people whose information was available to Carter. Carter continued through the SBA loan period to provide false and fraudulent information. In total, Carter admitted to being accountable for an intended fraud loss totaling more than $3.5 million but not more than $9.5 million.

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

Two South Florida Lawyers and Former Chief Operating Officer Sentenced for Roles in Massive 1 Global Capital Investment Scheme

On August 27, Andrew Dale Ledbetter, of Fort Lauderdale, Florida; Stephen Allen Schwartz, of Delray Beach, Florida; and Jan Douglas Atlas, of Fort Lauderdale, Florida; were sentenced for their roles in a fraud scheme that affected more than 3,600 investors in 42 states.

According to court documents, 1 Global was a commercial lending business based in Hallandale Beach, Florida, that made the equivalent of "pay day" loans to small businesses at high interest rates, termed merchant cash advance loans. Schwartz was a director and consultant at 1 Global, and also held out as a Chief Operating Officer in the company's marketing materials. Ledbetter was an attorney licensed in the State of Florida who had an of counsel position at a law firm and acted in a fundraising capacity at 1 Global beginning in or around 2015. Atlas was a partner at the same law firm and acted as outside counsel for 1 Global.

Substantial questions arose during the operation of the business as to whether 1 Global was offering or selling a security and whether the investment offering was required to be registered with the U.S. Securities and Exchange Commission. Ledbetter and Atlas knew that if 1 Global's investment offering was determined to be a security, it would undermine the ability of 1 Global to raise funds from retail investors and to continue to operate without substantial additional expenses and reporting requirements. Such a classification would undermine the profits and fees that Ledbetter and other principals at 1 Global would be able to obtain from 1 Global's operations.

At the request of 1 Global's principals, Atlas authored two opinion letters in 2016 containing false information that Atlas allegedly knew would be used by 1 Global to operate the business unlawfully. Ledbetter used and relied on Atlas's opinion letters to continue to raise money illegally, in numerous pitches and communications to investment advisors and investors.

According to court documents, Ledbetter was personally involved in raising more than $100 million in investor funds that went to 1 Global, through his own pitches as well as through investment advisors he attracted to 1 Global. Over the years, Ledbetter received approximately $3 million from 1 Global, the majority of which was for commissions. Atlas received approximately $627,000 from Ledbetter's commissions. Neither attorney disclosed these commissions to the law firm. Ledbetter routinely held himself out to investors and investment advisers as outside counsel to 1 Global, and also personally vouched for 1 Global in pitches and marketing materials, without disclosing his extravagant commissions.

In addition, in order to attract investments, Schwartz, Ledbetter, and others made false and misleading representations to investors and potential investors as to the profitability of 1 Global's business in marketing materials and periodic account statements.

Source: USAO, Southern District of Florida.
Responsible Agencies: FDIC OIG, FBI, and the Internal Revenue Service – Criminal Investigation (IRS-CI). Prosecuted by the USAO, Southern District of Florida, and DOJ's Criminal Division, Fraud Section.

Jury Convicts Five Former Officers and Employees of Banc-Serv Partners in $5 Million Scheme to Defraud the Small Business Administration

On August 5, a federal jury convicted five former officers and employees of Banc-Serv Partners LLP in a 13-year conspiracy to defraud the SBA in connection with its programs to guarantee loans made to small businesses.

According to the evidence presented at trial, the defendants — Kerri Agee, of Noblesville, Indiana, former President, Chief Executive Officer and founder of Banc-Serv; Kelly Isley, of Westfield, Indiana, Banc-Serv's former Chief Operating Officer; Nicole Smith, of Indianapolis, Indiana, a former Banc-Serv employee; Chad Griffin, of Carmel, Indiana, Banc-Serv's former Chief Marketing Officer; and Matthew Smith, of Westfield, Indiana, Banc-Serv's co-founder and a former director of a lending institution that originated loans with Banc-Serv — fraudulently obtained SBA-guaranteed loans on behalf of their clients, knowing that the loans did not meet SBA's guidelines and requirements for the guarantees.

The evidence at trial proved that from approximately 2004 until October 2017, the defendants helped originate SBA loans on behalf of various financial institutions and other lenders and, on multiple occasions, fraudulently obtained guarantees for loans that the SBA had deemed ineligible. They did so by, among other things, knowingly misrepresenting what the loans would be used for and unlawfully diverting previously denied loan applications into expedited approval channels at the SBA. When the fraudulently guaranteed loans defaulted, the defendants caused the submission of the reimbursement requests to the SBA to purchase the defaulted loans from investors and lending institutions, thereby shifting some of the losses on the ineligible loans to the SBA. The fraudulent loans presented at trial totaled approximately $5 million in guaranteed disbursements, which were not eligible for SBA guarantees.

Agee was convicted of one count of conspiracy to commit wire fraud affecting a financial institution and four counts of wire fraud affecting a financial institution. Isley was convicted of one count of conspiracy to commit wire fraud affecting a financial institution and two counts of wire fraud affecting a financial institution. Nicole Smith was convicted of one count of conspiracy to commit wire fraud affecting a financial institution and two counts of wire fraud affecting a financial institution. Griffin was convicted of one count of conspiracy to commit wire fraud affecting a financial institution. Matthew Smith was convicted of one count of conspiracy to commit wire fraud.

Source: SBA OIG.
Responsible Agencies: FDIC OIG, SBA OIG, Department of Housing and Urban Development OIG, and FBI. Prosecuted by the DOJ Fraud Section in the Southern District of Indiana.

Cedar Rapids Man Sentenced to Federal Prison for Fraud Charges

On April 19, Christopher Michael Goerdt, of Cedar Rapids, Iowa, was sentenced to 69 months in prison for bank fraud, aggravated identity theft, wire fraud, and misapplication by a bank officer. In addition, Goerdt was ordered to serve 5 years of supervised release following his prison term, pay $1,500 to the Crime Victims' Fund, and pay $1,124,343.60 in restitution to the victims of his crimes.

Goerdt participated in fraudulent activities at multiple financial institutions as early as 2006. He obtained and used a credit card in the name of a bank for his own personal use. In addition, Goerdt falsified loan documents, diverted loan proceeds, altered appraisals, made false statements to investigators, and obtained loans without the knowledge of customers. The loss attributed to Goerdt as a result of his schemes was nearly $900,000. Goerdt also knew he was being investigated by law enforcement and continued his scheme by seeking employment that would allow him to commit additional fraud at Farm Bureau Financial Services.

Source: FDIC Division of Risk Management Supervision.
Responsible Agencies: FDIC OIG, FBI, and Iowa Division of Criminal Investigation. Prosecuted by the USAO, Southern District of Iowa.

Michigan Man Sentenced for COVID-19 Relief Fraud

On September 14, Michael Bischoff, of Macomb County, Michigan, was sentenced to 32 months in Federal prison for fraudulently seeking nearly $1 million in PPP loans, after pleading guilty in November of 2020 to bank fraud. In addition to the prison sentence, Bischoff was ordered to serve 3 years of supervised release and pay $534,590 in restitution and a $5,000 fine.

According to court documents, Bischoff, who owned multiple pizza restaurants in Macomb County, admitted to defrauding several financial institutions by submitting at least nine falsified PPP loan applications that included false representations about payroll, business expenses, and the number of employees working at his restaurants. To help secure the PPP loans, Bischoff also submitted multiple fabricated tax documents and fraudulently used another person's personal identifying information. In total, Bischoff fraudulently sought approximately $931,000 in COVID-19 relief funds and received approximately $593,590.

Responsible Agencies: FDIC OIG, SBA OIG, and the U.S. Secret Service. Prosecuted by the USAO, Eastern District of Michigan, and DOJ's Criminal Division, Fraud Section.

Texas Man Sentenced for $24 Million COVID-19 Relief Fraud Scheme

On July 28, Dinesh Sah, of Coppell, Texas, was sentenced to more than 11 years in prison for wire fraud and money laundering offenses in connection with his fraudulent scheme to obtain approximately $24.8 million in forgivable PPP loans. Sah was also ordered to pay $17,284,649.79 in restitution.

According to court documents, Sah submitted 15 fraudulent applications, filed under the names of various purported businesses that he owned or controlled, to eight different lenders seeking approximately $24.8 million in PPP loans. He claimed that these businesses had numerous employees and hundreds of thousands of dollars in payroll expenses when, in fact, no business had employees or paid wages consistent with the amounts claimed in the PPP applications.

Sah further submitted fraudulent documentation in support of his applications, including fabricated federal tax filings and bank statements for the purported businesses, and falsely listed other persons as the authorized representatives of certain of these businesses without the authority to use their identifying information on the applications.

As a result of his scheme, Sah received over $17 million in PPP loan funds and diverted the proceeds for his personal benefit. Sah also sent millions of dollars in PPP proceeds in international money transfers. As part of his guilty plea, Sah agreed to forfeit, among other property, eight homes, six luxury vehicles, and more than $9 million in fraudulent proceeds that the government had seized to date.

Source: DOJ.
Responsible Agencies: FDIC OIG, IRS-CI, and Treasury Inspector General for Tax Administration (TIGTA). Prosecuted by the USAO, Northern District of Texas.

Texas Wedding Planner Sentenced in COVID-19 Fraud Scheme

On September 16, Fahad Shah, of Murphy, Texas, was sentenced to 31 months in prison and 3 years of supervised release for perpetrating a scheme to fraudulently obtain more than $3.3 million in PPP loans.

According to court documents, Shah sought approximately $3.3 million in PPP funds, claiming his family's business, WBF Weddings by Farah Inc., employed more than 100 individuals and paid millions of dollars in compensation to those employees. In actuality, the business had no employees aside from Shah and his wife. Based on his false representations and forged documents, an SBA-approved lender provided over $1.5 million in PPP funds to Shah. Shah then used those funds for his personal gain.

Source: DOJ.
Responsible Agencies: FDIC OIG, SBA OIG, FHFA OIG, IRS-CI, and TIGTA. Prosecuted by the USAO, Eastern District of Texas, and DOJ's Criminal Division, Fraud Section.

Washington Tech Executive Sentenced for COVID-19 Relief Fraud Scheme

On August 24, Mukund Mohan, of Clyde Hill, Washington, was sentenced to 2 years in prison for perpetrating a scheme to fraudulently obtain COVID-19 disaster relief loans guaranteed by the SBA through the Economic Injury Disaster Loan (EIDL) Program and PPP under the CARES Act.

According to court documents, Mohan sought more than $5.5 million through eight fraudulent disaster loan applications. In support of the fraudulent loan applications, Mohan submitted fake and altered documents, including fake Federal tax filings and altered incorporation documents. For example, he misrepresented to a lender that, in 2019, his company Mahenjo Inc. had dozens of employees and paid millions of dollars in employee wages and payroll taxes. In support of Mahenjo's loan application, he submitted false incorporation documents and tax forms suggesting that the company had been in business prior to 2020. In truth, Mohan purchased Mahenjo in May 2020 and at the time he purchased the company, it had no employees and no business activity. The incorporation documents that he submitted to the lender were altered and the Federal tax filings he submitted were fake. Five of Mohan's eight fraudulent loan applications were approved, and he fraudulently obtained nearly $1.8 million in COVID-19 relief funds.

In addition to the prison sentence, Mohan was ordered to pay a fine of $100,000 and $1,786,357 in restitution.

Source: DOJ.
Responsible Agencies: FDIC OIG, FHFA OIG, TIGTA, and IRS-CI. Prosecuted by DOJ's Criminal Division, Fraud Section, and the USAO, Western District of Washington.

Three South Florida Men Plead Guilty to Conspiring to Launder Fraudulently Obtained COVID-19 Relief Money and Proceeds from Business Email Compromise Scheme

On September 2, Broward County, Florida, residents Jimpcy One, Gousman Lemy, and Frantz Guillaume, Jr. a/k/a Sandro Saintfloeur, pleaded guilty in Federal district court to conspiring with each other to launder proceeds obtained from business email compromise schemes and fraudulently obtained COVID-19 relief loans. Each defendant admitted to laundering close to $2 million dollars to disguise the nature and source of the illicit funds.

According to court documents, in July 2017, Lemy and Guillaume laundered a little over $425,000 obtained from a business email compromise of a Texas-based university. Then, in 2019, One joined Lemy and Guillaume in laundering over $900,000 obtained from a business email compromise of another U.S.-based victim company. In each business email compromise scheme, co-conspirators sent false and fraudulent emails from a hacked account that tricked the victims into wiring money into accounts controlled by the defendants and their co-conspirators. They then sought to conceal the origin of this fraudulently obtained money by transferring it among the bank accounts of various shell companies that they controlled.

When the coronavirus pandemic hit the United States in 2020, the co-conspirators allegedly initiated a new fraud scheme using existing shell companies from the email compromise scheme, as well as newly created and reactivated shell companies. The co-conspirators allegedly submitted false and fraudulent loan applications under two U.S. government relief programs authorized by the CARES Act to help small businesses and their employees survive the COVID-19 economic crisis: the PPP and EIDL. In June and July 2020, through false submissions in the names of their shell companies, the co-conspirators fraudulently applied for and received close to $2 million in PPP and EIDL funds, which was laundered amongst them.

Source: FBI Miami Office and the USAO, Southern District of Florida. Responsible Agencies: FDIC OIG, FBI, and SBA OIG with assistance from the United States Secret Service and TIGTA Cybercrimes Division. Prosecuted by the USAO, Southern District of Florida.

West L.A. Man Pleads Guilty to Fraudulently Obtaining Approximately $9 Million in COVID-19 Relief Loans, Some of Which Was Gambled Away

On September 14, Andrew Marnell, of West Los Angeles, California, pleaded guilty to Federal charges stemming from a scheme that used a series of corporations he controlled to fraudulently obtain approximately $9 million in loans from COVID 19-relief programs, some of which he used on gambling excursions to Las Vegas and transferred to his stock trading accounts. He pleaded guilty to one count of bank fraud and one count of money laundering.

Marnell admitted that he fraudulently obtained PPP loans guaranteed by the SBA under the CARES Act. Marnell obtained seven PPP loans from financial institutions for corporations he controlled that brought him just under $9 million. He submitted fraudulent loan applications that made numerous false and misleading statements about the companies' business operations and payroll expenses. Marnell, often using aliases, submitted fake and altered documents, including bogus Federal tax filings and employee payroll records.

Marnell admitted that he fraudulently obtained $170,000 in EIDL loans. Once the loans were funded, Marnell transferred millions of dollars from the fraudulently obtained loan proceeds to his brokerage accounts to make risky stock market bets, according to court documents, which noted that Marnell spent hundreds of thousands of dollars in fraudulently obtained loan proceeds at various gambling establishments.

As part of the plea agreement, Marnell agreed to forfeit items related to the pilfered PPP loan funds, including more than $1.54 million seized from several brokerage accounts, $319,298 in cash recovered from his residence, numerous electronic devices, a Rolex Oyster watch, a Range Rover, and a Ducati motorcycle.

In addition to any prison sentence he receives, Marnell has agreed to pay restitution to the victim lenders to compensate the losses from this case, an amount believed to be $7,341,376.

Source: DOJ.
Responsible Agencies: FDIC OIG, FHFA OIG, FBI, IRS-CI, TIGTA, and SBA OIG. Prosecuted by DOJ's Fraud Section and the USAO, Central District of California.

Strong Partnerships with Law Enforcement Colleagues

The OIG has partnered with various USAOs throughout the country in bringing to justice individuals who have defrauded the FDIC or financial institutions within the jurisdiction of the FDIC, or criminally impeded the FDIC's examination and resolution processes. The alliances with the USAOs have yielded positive results during this reporting period. Our strong partnership has evolved from years of hard work in pursuing offenders through parallel criminal and civil remedies resulting in major successes, with harsh sanctions for the offenders. Our collective efforts have served as a deterrent to others contemplating criminal activity and helped maintain the public's confidence in the Nation's financial system.

During the reporting period, we partnered with USAOs in the following areas:

Alabama	Maryland	Oklahoma
Arkansas	Massachusetts	Oregon
California	Michigan	Pennsylvania
Colorado	Minnesota	Rhode Island
District of Columbia	Mississippi	South Carolina
Florida	Missouri	South Dakota
Georgia	Montana	Tennessee
Hawaii	Nebraska	Texas
Idaho	Nevada	Utah
Illinois	New Hampshire	Virginia
Indiana	New Jersey	Washington
Iowa	New York	West Virginia
Kansas	North Carolina	Wisconsin
Kentucky	North Dakota	
Louisiana	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; South Jersey SAR Task Force; Pennsylvania Electronic Crimes Task Force; NJ COVID-19 Fraud Task Force; Newark HSI Financial Fraud Working Group; Northern District of New York PPP Fraud Working Group.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force; Northern District of Georgia Mortgage Fraud Task Force; Eastern District of North Carolina Bank Fraud Task Force; Northern District of Alabama Financial Fraud Working Group; Northern District of Georgia SAR Review Team; Middle District of Georgia SAR Review Team; South Carolina Financial Fraud Task Force; Eastern District of North Carolina Financial Crimes Task Force; Western District of North Carolina Financial Crimes Task Force; Middle District of North Carolina Financial Crimes Task Force; COVID Working Groups for: Southern District of Florida, Middle District of Florida, Northern District of Florida; SAR Review Groups for: Miami, Palm Beach, Treasure Coast Financial Crimes Review Team, Key West/Monroe County.
Kansas City Region	Kansas City SAR Review Team; St. Louis SAR Review Team; Minnesota Inspector General Council; Minnesota Financial Crimes Task Force; Nebraska SAR Review Team; Southern District of Iowa SAR Review Team.
Chicago Region	Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Central District of Illinois Financial Fraud Working Group; Northern District of Illinois SAR Review Team; Northern District of Illinois Bankruptcy Fraud Working Group; Cook County Region Organized Crime Organization; Financial Investigative Team, Milwaukee, Wisconsin; Eastern District of Wisconsin SAR Review Team; Western District of Wisconsin SAR Review Team; Western District of Wisconsin Bankruptcy Fraud Working Group; Indiana Bank Fraud Working Group; Northern District of Indiana SAR Review Team; FBI Louisville Financial Crime Task Force; U.S. Secret Service Louisville Electronic Crimes Task Force; Western District of Kentucky SAR Review Team; Eastern District of Kentucky SAR Review Team; Southern District of Ohio SAR Review Team.
San Francisco Region	Fresno Mortgage Fraud Working Group for the Eastern District of California; Sacramento Mortgage Fraud Working Group for the Eastern District of California; Sacramento SAR Working Group; Orange County Financial Crimes Task Force-Central District of California; Orange County SAR Review Team; Northern District of California Money Laundering SAR Review Task Force; San Diego Financial Investigations and Border Crimes Task Force; Northern Nevada Financial Crimes Task Force; Financial Services Roundtable coordinated by the USAO of the Northern District of California; Los Angeles Complex Financial Crimes Task Force – Central District of California; Los Angeles Real Estate Fraud Task Force – Central District of California; Homeland Security San Diego Costa Pacifica Money Laundering Task Force; DOJ National Unemployment Insurance Fraud Task Force; California Unemployment Insurance Benefits Task Force; Nevada Fight Fraud Task Force; Las Vegas SAR Review Team; COVID Benefit Fraud Working Group, USAO District of Oregon; Financial Crimes Task Force, USAO District of Hawaii; DOJ Transnational Elder Fraud Strike Task Force.
Dallas Region	SAR Review Team for Northern District of Mississippi; SAR Review Team for Southern District of Mississippi; Oklahoma City Financial Crimes SAR Review Working Group; Austin SAR Review Working Group; Houston High Intensity Drug Trafficking Area SAR Team.
Mid-Atlantic Region	Virginia Crime Analysts Network; Northern Virginia Financial Initiative SAR Review Team; Pandemic Response Accountability Committee (PRAC) Fraud Task Force; PRAC Law Enforcement Coordination Subcommittee; PRAC Data Analytics Subcommittee; Council of the Inspectors General on Integrity and Efficiency (CIGIE) COVID-19 Working Group; DOJ Stimulus Funds Fraud Working Group; District of Maryland SAR Review Task Force; Western District of Virginia SAR Review Task Force, Roanoke, Virginia; Western District of Virginia SAR Review Task Force, Abingdon, Virginia; Eastern District of Virginia SAR Review Task Force; Central Eastern District of Virginia SAR Review Task Force; Northern Virginia Eastern District of Virginia SAR Review Task Force; DOJ Foreign Corrupt Practices Act SAR Initiative; District of Columbia SAR Review Task Force; Southern District of West Virginia SAR Review Task Force; Northern District of West Virginia SAR Review Task Force.
Electronic Crimes Unit	Washington Metro Electronic Crimes Task Force; High Technology Crime Investigation Association; 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; Secret Service Cyber Task Force, Newark, New Jersey; Council of Federal Forensic Laboratory Directors; FBI Los Angeles' Orange County Cyber Task Force; 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. Specifically, in keeping with our Guiding Principles, we have focused on strengthening relations with partners and stakeholders, efficiently and effectively administering resources, and promoting leadership and teamwork. A brief listing of some of our key efforts in these areas follows.

Strengthening relations with partners and stakeholders.

- Communicated with the Chairman, FDIC Director, 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.
- Sent a joint message from the IG and FDIC Chairman regarding the importance of cooperating with the OIG and announced the updated and revised FDIC Directive on Cooperation with the Office of Inspector General. Under the Directive, FDIC employees and contractor personnel have an obligation to promptly report to the OIG all instances of actual or suspected fraud, waste, abuse, misconduct, or mismanagement in connection with FDIC programs and operations. The Directive also states that FDIC employees and contractor personnel have a duty to fully cooperate with the work of the OIG and provide prompt and complete responses to requests.
- Coordinated with the FDIC Director, in his capacity as Chairman of the FDIC Audit Committee, to provide status briefings and present the results of completed audits, evaluations, and related matters for his and other Committee members' consideration. Presented the results of OIG audits, evaluations, and other reviews at monthly Audit Committee meetings.
- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
- Posted video summaries of OIG-issued audit and evaluation reports on our external website to provide stakeholders an additional opportunity to learn about the work of the OIG and the findings and recommendations our auditors and evaluators have made to improve FDIC programs and operations.

- Recognized Whistleblower Appreciation Day, which commemorates the first enactment of whistleblower protections in Federal statute in 1778. The FDIC IG and FDIC Chairman sent out a joint statement regarding the rights, protections, and responsibilities of Whistleblowers. The message reminded FDIC employees to report fraud, waste, abuse, misconduct, or mismanagement at the FDIC to a supervisor, the OIG, or the U.S. Office of Special Counsel. The message also provided important resources about whistleblower protections and rights and information for reaching the OIG's Whistleblower Protection Coordinator.
- 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 Chairman and FDIC Director 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 other inquiries 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.
- 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, and Inclusion 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, Assistant IGs for Management, and Council of Counsels to the IGs; responding to multiple requests for information on IG community issues of common concern; and commenting on various legislative matters through CIGIE's Legislation Committee.
- Supported efforts of the PRAC through active participation in its meetings, forums, and work groups and by playing a key role in collaboration with law enforcement partners in investigations of fraud in pandemic-relief programs. Also adopted 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 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. Provided FDIC OIG input for CIGFO Annual Report.
- Communicated with the Government Accountability Office on ongoing efforts related to our oversight roles and issues of mutual interest.
- Coordinated with the Office of Management and Budget to address budget matters of interest.
- 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 interest. Joined law enforcement partners in numerous financial, mortgage, suspicious activity report review, cyber fraud, COVID, and PRAC-related working groups nationwide.
- Promoted transparency to keep the American public informed through four main means: the FDIC OIG website to include, for example, summaries of completed work, listings of ongoing work, and information on unimplemented recommendations; Twitter communications to immediately disseminate news of report and press release issuances and other news of note; external video summaries of report findings; and participation in the IG community's oversight.gov website, which enables users to access, sort, and search thousands of previously issued IG reports and other oversight areas of interest.
- Increased transparency of our work on oversight.gov by including press releases related to investigative cases and related actions, in addition to posting our audits and evaluations, and updated on an ongoing basis the status of FDIC OIG recommendations remaining unimplemented.
- Completed a Peer Review of the Audit Organization of the Securities and Exchange Commission's OIG, in accordance with Government Auditing Standards and the CIGIE Guide for Conducting Peer Reviews of Audit Organizations of Federal Offices of Inspector General.

Administering resources prudently, safely, securely, and efficiently.

- Formulated the OIG's budget for FY 2023 and proposed $48.4 million to conduct oversight of the FDIC. This amount is approximately 4 percent above the FY 2022 request. It will allow the OIG to maintain the FY 2022 baseline and staffing structure, including projected increases in salary and benefits costs; make additional investments in the OIG's information technology, data analytics, and cybersecurity infrastructure; and continue the OIG's capacity to conduct statutorily-mandated reviews of failed banks.
- Combined two component OIG offices conducting independent audits and evaluations of the FDIC into a unified Office of Audits, Evaluations, and Cyber under the leadership of a single Assistant Inspector General to consolidate and strengthen OIG oversight of FDIC programs and operations.
- Continued implementation of our Office of Information Technology's strategic plan and IT Road Map for 2021-2023, designed to deliver robust and modern IT solutions to advance capabilities in supporting the OIG mission; support IT innovation and foster growth of technical skills and talent among OIG users; streamline and digitize information management workflows and processes; minimize development and operational costs; enhance the public relations of the OIG through the Internet-facing website; facilitate sharing of information and best practices; improve the OIG's overall security posture and disaster recovery capabilities; and enhance support for telework and the digital workplace. Shared 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, equipment, and electronic devices.
- Launched the OIG's new electronic Investigations Management System (IMS), which will modernize OI's investigations management capabilities; streamline and digitize workflows and business processes; enhance internal controls; improve stakeholder reporting capabilities; and facilitate Special Agents' work in Headquarters and Regional Office locations. Another enhancement of the new system is a new OIG Hotline portal. Complainants and whistleblowers will fill out a new intake form that will capture information and intake of complaints directly into IMS for assessment by the Hotline team.
- Continued build-out of the OIG's Electronic Crimes Unit, with launch of the lab anticipated for 2022.
- Continued pursuing component office Implementation Plans designed to achieve the OIG's Strategic Goals, Guiding Principles, and Vision for 2021.
- Established a 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.

- Held a Town Hall Meeting facilitated by the IG and Deputy IGs to provide Office heads an opportunity to update all OIG staff on Office initiatives and priorities, to connect with staff through open dialogue, and to assure staff the their health and safety is of paramount importance during the mandatory telework period as the OIG prepares for the eventual Return to the Office.
- Enhanced the OIG's intranet site to increase collaboration, especially in a virtual environment, and to provide component offices more control over and access to information, guidance, and procedures, to better conduct their work.
- Maintained the "Helpful Resources During Pandemic" collaboration site for all of OIG, as a means to provide continuous updates on the pandemic and offer helpful information resources to OIG staff as the Office continued to operate under mandatory telework conditions.
- 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, IT system updates, and training.
- 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 and evaluations; and support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.
- Continued to review and update a number of OIG internal policies related to audit, evaluation, investigation, operations, and administrative processes of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the Office. Continued to move all policies to a central SharePoint site for easier access and updating capabilities.
- Carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. Positions filled during the reporting period included Special Agents in Charge, a human resources specialist, audit and evaluation staff, and criminal investigators.
- 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.
- Integrated and leveraged use of MS Teams throughout our Office to promote virtual collaboration and communication, particularly during this current time of the pandemic, when mandatory telework for our Office is in place.

Exercising leadership skills and promoting teamwork.

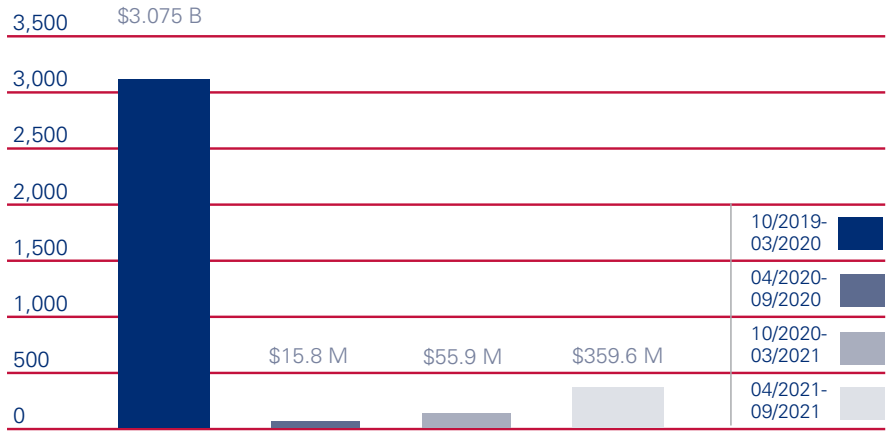
- Enhanced the OIG's intranet site to promote teamwork by having the page launch as the opening home page for OIG staff and expanded content to include cross-cutting information of interest to staff.
- Continued biweekly OIG senior leadership meetings to affirm the OIG's unified commitment to the FDIC OIG mission and to strengthen working relationships and coordination among all FDIC OIG offices.
- Supported efforts of the Workforce Council as that group explored issues relating to performance management program and related rewards and recognition matters.
- Kept OIG staff 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 and communications and other announcements.
- Enrolled OIG staff in several different FDIC and CIGIE Leadership Development Programs to enhance their leadership capabilities.
- Held training sponsored by the Arbinger Group 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 discussion sessions for attendees.
- Participated in CIGIE's Professional Development/LIFT's Perspectives from Leadership event. This IG community-wide forum featured leadership insights from the FDIC IG; Deputy IG; AIG for Audits, Evaluations, and Cyber; and was moderated by the FDIC OIG's Engagement and Learning Officer (ELO).
- Carried out monthly coordination meetings for audit, evaluation, and investigation leadership to better communicate, coordinate, and maximize the effectiveness of ongoing work.
- Celebrated individual and group accomplishments through an annual All Hands Award Ceremony and through an ongoing awards and recognition program for staff across all component offices to acknowledge their contributions to the Office.
- Continued to support members of the OIG pursuing professional training and certifications to enhance the OIG staff members' expertise and knowledge.

- Shared information from our 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; planned for training from the NeuroLeadership Institute; 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 Diversity and Inclusiveness (D&I) Working Group and other initiatives. These included sharing information obtained through participation at Cornell University's Diversity and Inclusion Certificate Program; bi-monthly D&I Working Group updates in our Office newsletters; developing a D&I collaboration site and beginning to formulate a strategic plan; and special acknowledgments of Juneteenth, LGBTQ+ Pride, Whistleblower Appreciation, Asian American Pacific Heritage, Jewish Heritage, and Hispanic Heritage.
- Continued active involvement in CIGIE's Diversity, Equity, and Inclusion (DE&I) Work Group, of which the FDIC IG is Vice Chair. The FDIC IG co-led CIGIE's first community-wide Town Hall event focusing on the IG community's ongoing DE&I efforts to enhance the "lifecycle" experience of OIG employees -- recruiting, hiring, staffing, professional development, training, awareness, awards, and promotions -- as well as ways to strengthen the oversight work of OIGs by incorporating DE&I principles into their audits, evaluations, and investigations. The FDIC IG also took part in a panel discussion hosted by the IDEA Council of the U.S. Postal Service OIG – Inclusion, Diversity, Equity, and Awareness to share ideas and innovations from other OIGs, including challenges, successes, and the impact of such efforts.
- Took a leadership role in the CIGFO joint working group on Crisis Readiness. The OIG's Assistant IG for Audits, Evaluations, and Cyber served as co-lead of the effort to compile forward-looking guidance for the Financial Stability Oversight Council and its members to consider in preparing for crises.
- Led efforts of the PRAC's Law Enforcement Coordination Subcommittee. Our Special Agent in Charge of the Mid-Atlantic Region is Chair of this group.

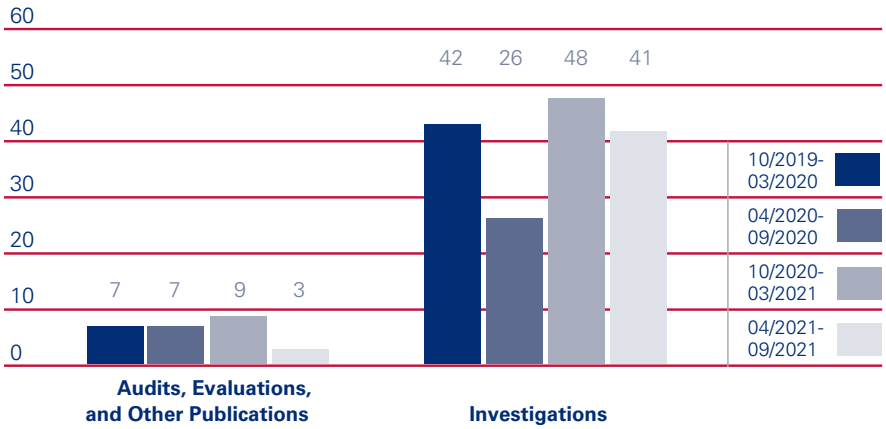
Cumulative Results (2-year period)

Nonmonetary Recommendations	
October 2019 – March 2020	37
April 2020 – September 2020	44
October 2020 – March 2021	56
April 2021 – September 2021	12

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



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.	35
Section 5(a)(1): Significant problems, abuses, and deficiencies.	4-7
Section 5(a)(2): Recommendations with respect to significant problems, abuses, and deficiencies.	4-6
Section 5(a)(3): Significant recommendations described in previous semiannual reports on which corrective action has not been completed.	36
Section 5(a)(4): Matters referred to prosecutive authorities.	49
Section 5(a)(5): Summary of each report made to the head of the establishment regarding information or assistance refused or not provided.	48
Section 5(a)(6): Listing of audit, inspection, and evaluation reports by subject matter with monetary benefits.	45
Section 5(a)(7): Summary of particularly significant reports.	4-7
Section 5(a)(8): Statistical table showing the total number of audit, inspection, and evaluation reports and the total dollar value of questioned costs.	46
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.	47
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	48
• no establishment comment was received within 60 days of providing the report to management	48
• there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.	37-44

Reporting Requirements (continued)	Page
Section 5(a)(11): Significant revised management decisions during the current reporting period.	48
Section 5(a)(12): Significant management decisions with which the OIG disagreed.	48
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.	51-52
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.	49
Section 5(a)(18): A description of metrics used for Section 5(a)17 information.	49
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.	49
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.	49
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.	49
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.	49

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. In March 2019, Inspector General Lerner became Vice Chair of the Council of the Inspectors General on Integrity and Efficiency's Legislation Committee. Much of the FDIC OIG's activity reviewing legislation and regulation occurs in connection with that Committee.

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

Most recently, the Legislation Committee has continued to pursue legislative priorities that the FDIC OIG supports, including increasing the institutional independence of IGs through reforms to the Vacancies Act, enhancing the ability of IGs to access information through testimonial subpoena authority, and providing continuous IG oversight during lapses in appropriations. The FDIC OIG is also leading a Legislation Committee project to propose revisions to statutorily-mandated OIG audits so that any mandates are tailored to the highest risks.

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

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

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

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

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

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 will consult stakeholders to evaluate the usefulness of the newly captured acquisition data and consider any possible reporting enhancements resulting from the acquisition system and business process modernization effort and make a recommendation to the Deputy to the Chairman and Chief Operating Officer for revised portfolio-level reporting.
AUD-20-003 **The FDIC's Privacy Program** December 18, 2019	**3**	The FDIC began a process in 2019 to ensure privacy plans are developed and approved for all systems containing personally identifiable information. The FDIC will fully implement this process over a 3-year period, with priority for new and changing authorizations over the next year.
EVAL-21-002 **Critical Functions in FDIC Contracts** March 31, 2021	**10**	The FDIC will consider and further study potential methodologies for assessing contractor overreliance, including how other agencies make such determinations. Based on its study, the FDIC will provide guidance to divisions and offices for assessing the potential for contractor overreliance and maintaining Federal control of essential functions or those necessary during a business continuity event.

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods

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

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-20-001 **The FDIC's Information Security Program - 2019** October 23, 2019	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct this audit. The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. C&C found that the FDIC established a number of information security program controls and practices that complied or were consistent with FISMA requirements and Federal information security policy, standards, and guidelines. However, C&C identified weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. C&C concluded that the FDIC's overall information security program was operating at a Maturity Level 3 (Consistently Implemented). The report contained three recommendations intended to ensure that (i) employees and contractor personnel properly safeguard sensitive electronic and hardcopy information and (ii) network users complete required security and privacy awareness training.	3	1	NA
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 Total	Recommendations Outstanding	Potential Cost Savings
AUD-20-003 **The FDIC's Privacy Program** December 18, 2019	The significant amount of personally identifiable information held by the FDIC underscores the importance of implementing an effective Privacy Program that ensures proper handling of this information and compliance with privacy laws, policies, and guidelines. The Office of Management and Budget's (OMB) Circular A-130, Managing Information as a Strategic Resource (OMB Circular A-130), organizes relevant privacy-related requirements and responsibilities for Federal agencies into nine areas. The audit objective was to assess the effectiveness of the FDIC's Privacy Program and practices. We assessed effectiveness by determining whether the FDIC's Privacy Program controls and practices complied with selected requirements defined in eight of the nine areas covered by OMB Circular A-130. We found that the Privacy Program controls and practices we assessed were effective in four of eight areas examined. However, privacy controls and practices in the remaining four areas were either partially effective or not effective. The report contained 14 recommendations intended to strengthen the effectiveness of the FDIC's Privacy Program and records management practices.	14	3	NA
EVAL-20-003 **Cost Benefit Analysis Process for Rulemaking** February 4, 2020	The FDIC OIG conducted an evaluation of the FDIC's Cost Benefit Analysis Process for Rulemaking. Through the Banking Act of 1933, Congress provided the FDIC with the authority to promulgate rules to fulfill the goals and objectives of the Agency. A cost benefit analysis informs the agency and the public whether the benefits of a rule are likely to justify the costs, or determines which of various possible alternatives is most cost effective. Our evaluation objective was to determine if the FDIC's cost benefit analysis process for rules was consistent with best practices. We found that the FDIC's cost benefit analysis process was not consistent with widely recognized best practices identified by the OIG. Specifically, we found that the FDIC had not established and documented a process to determine when and how to perform cost benefit analyses. We also found that the FDIC did not leverage the expertise of its Regulatory Analysis Section economists during initial rule development; did not require the Chief Economist to review and concur on the cost benefit analyses performed, which is an important quality control; was not always transparent in its disclosure of cost benefit analyses to the public; and did not perform cost benefit analyses after final rule issuance. The report contained five recommendations to improve the FDIC's cost benefit analysis process.	5	5	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
EVAL-20-004 **The FDIC's Readiness for Crises** April 7, 2020	The FDIC OIG conducted an evaluation of the FDIC's Readiness for Crises. We initiated this evaluation in 2018, and it covered the FDIC's readiness planning and preparedness activities up to early 2019. Our work was not conducted in response to the pandemic situation, nor was the report specific to any particular type of crisis. Effective crisis readiness plans and activities can help the FDIC support the safety and soundness of insured depository institutions, as well as the stability and integrity of the Nation's banking system. Our evaluation objective was to assess the FDIC's readiness to address crises that could impact insured depository institutions. We identified best practices that could be used by the FDIC. Our review of these best practices identified seven important elements of a crisis readiness framework that are relevant to the FDIC – (i) Policy and Procedures; (ii) Plans; (iii) Training; (iv) Exercises; (v) Lessons Learned; (vi) Maintenance; and (vii) Assessment and Reporting. We reported that the FDIC should fully establish these seven elements of a readiness framework to address crises that could impact insured depository institutions. The report contained 11 recommendations to improve the FDIC's crisis readiness planning.	11	1	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-20-007 **In-Depth Review of Enloe State Bank, Cooper, Texas** September 30, 2020	Enloe State Bank (the Bank) was a state-chartered, nonmember bank that operated its sole office in rural Cooper, Texas. On May 31, 2019, the Texas Department of Banking closed the Bank and appointed the FDIC as receiver. When a bank fails and the FDIC's Deposit Insurance Fund (DIF) incurs a loss under $50 million as a result of the bank failure, Section 38(k)(5) of the Federal Deposit Insurance (FDI) Act requires that the Inspector General of the appropriate Federal banking agency conduct a Failed Bank Review (FBR). The purpose of the FBR is 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 (IDR) of the loss. Section 38(k)(5) also requires Inspectors General to report information about the results of FBRs in their semiannual reports to Congress. When the Inspector General determines that an IDR is warranted, Section 38(k)(5) requires that the Inspector General report on the review to the FDIC and Congress. We found that an IDR was warranted given the extent of the irregular loans identified that contributed to an extraordinarily high estimated loss rate. The objectives of this evaluation were to (1) determine the causes of Enloe State Bank's failure and the resulting loss to the DIF and (2) evaluate the FDIC's supervision of the Bank, including the FDIC's implementation of the Prompt Corrective Action provisions of Section 38 of the FDI Act. Enloe State Bank failed because the President and the senior-level Vice President perpetrated fraud by originating and concealing a large number of fraudulent loans over many years. The Bank's President was a dominant official with significant control over bank operations and limited oversight by the Board of Directors (Board). As the Bank's capital levels deteriorated, the FDIC took action consistent with Prompt Corrective Action provisions. That is, the FDIC notified the Bank that it was "critically undercapitalized" and required it to take actions necessary to increase capital to become "adequately capitalized" as defined by Section 38 of the FDI Act. Ultimately, the Bank's Board was not able to satisfy that requirement. The report contained eight recommendations to improve examiner guidance and training.	8	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	
AUD-21-001 **The FDIC's Information Security Program – 2020** October 27, 2020	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct this audit. The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. Applying the FISMA metrics, the FDIC's overall information security program was operating at a Maturity Level 3 (Consistently Implemented). The FDIC established a number of information security program controls and practices that were consistent with FISMA requirements and Federal information security policy, standards, and guidelines. However, the FISMA report identified weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. The report contained eight recommendations intended to improve the effectiveness of the FDIC's information security program and practices.	8	4	NA
AUD-21-002 **Governance of the FDIC's Mobile Device Management Solution** December 21, 2020	The FDIC relies heavily on smartphones and tablets to support its business operations and communications. The FDIC uses a cloud-based mobile device management (MDM) solution to secure and manage these mobile devices. We conducted an audit to assess the adequacy of the FDIC's governance over a proposed MDM solution. We found that the FDIC's Chief Information Officer Organization did not identify elevated and growing risks associated with the project; resolve security concerns identified by the Office of the Chief Information Security Officer prior to procuring the proposed MDM solution; or establish roles and responsibilities for managing the use of Limited Authorizations to Operate. Further, the FDIC's Acquisition Services Branch did not engage the Legal Division to review the procurement of the proposed MDM solution, consistent with FDIC guidance. The report contained five recommendations intended to strengthen the FDIC's processes and governance for evaluating, authorizing, and procuring new technologies.	5	1	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
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	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-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 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-21-004 August 3, 2021	*Security and Management of Mobile Devices*			
AEC Memorandum 21-001 August 17, 2021	*Concerns Related to the FDIC's Pending Authorization to Operate Its External Wireless Solution Cloud Service*			
Resource Management				
AEC Memorandum 21-002 September 1, 2021	*The FDIC's Management of Employee Talent*			
Totals for the Period		**$0**	**$0**	**$0**

Table IV: Audit and Evaluation Reports Issued with Questioned Costs

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

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

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

Table VI: Status of OIG Recommendations Without Management Decisions
During this reporting period, there were five recommendations more than 6 months old without management decisions. In our report, C*ritical Functions in FDIC Contracts* (EVAL-21-002), dated March 31, 2021, we found that 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. During our evaluation, we determined that Blue Canopy performed Critical Functions at the FDIC. Specifically, Blue Canopy performed tasks that are critical to ensuring the security and protection of the FDIC's information technology infrastructure and data.

The FDIC, however, did not identify the services performed 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 Policy Letter 11-01 and best practices. We made recommendations aimed at strengthening the FDIC's internal controls over Critical Functions to align with OMB Policy Letter 11-01 and best practices. The FDIC stated that it partially concurred with the recommendations; however, the FDIC response did not provide specific actions taken or planned.

Specifically, the FDIC has expressed reluctance to incorporate the term "Critical Function" into its process, as that term is used and defined in OMB Policy Letter 11-01. The definition of essential functions as used by the FDIC is restricted to those functions that impact continuity of operations planning. Critical Functions, on the other hand, are broader and cover all functions that are necessary to the agency being able to effectively perform and maintain control of its mission and operations. The FDIC plans to consider and further study the issues and does not intend to implement corrective actions until March 31 and June 30, 2022. We continue to work with the FDIC to resolve the recommendations.

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	41
Number of Persons Referred to the Department of Justice for Criminal Prosecution	124
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	0
Number of Indictments and Criminal Informations	58

Note: Description of the metrics used for the above information: Reports issued reflects case closing memorandums issued to FDIC management. With respect to the 124 referrals to DOJ, the total represents 88 individuals, 34 business entities, and 2 cases where the subject is unknown at present. Our total indictments and criminal informations includes indictments, informations, and superseding indictments, as applicable.

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

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

Table XIII: Instances of Whistleblower Retaliation

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

Table XIV: Instances of Agency Interference with OIG Independence

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

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

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

Appendix 2

Information on Failure Review Activity

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

FDIC OIG Review Activity for the Period April 1, 2021 through September 30, 2021 (for failures that occur on or after January 1, 2014 causing losses to the Deposit Insurance Fund of less than $50 million)

When the Deposit Insurance Fund incurs a loss under $50 million, Section 38(k) of the Federal Deposit Insurance Act requires the Inspector General of the appropriate federal banking agency to determine the grounds upon which the state or Federal banking agency appointed the FDIC as receiver and whether any unusual circumstances exist that might warrant an in-depth review of the loss.

We did not issue any Failed Bank Reviews during the reporting period, and as of the end of the reporting period, there were no Failed Bank Reviews in process.

Appendix 3

Peer Review Activity

Federal Inspectors General are required to engage in peer review processes related to their audit and investigative operations. The IG community has also implemented a peer review program for the inspection and evaluation functions of an OIG as well. The FDIC OIG is reporting the following information related to the most current peer reviews that our organization has undergone.

Definition of Audit Peer Review Ratings

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

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

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

Audit Peer Reviews

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

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

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

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

Inspection and Evaluation Peer Reviews

A CIGIE External Peer Review Team conducted a peer review of our Office of Program Audits and Evaluations (PAE) (recently re-named Audits, Evaluations, and Cyber) and completed its review in April 2019. Members of the peer review team included participants from the Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection OIG, the U.S. Department of Education OIG, and the U.S. Nuclear Regulatory Commission OIG.

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

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

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 and Farewell

Council of the Inspectors General on Integrity and Efficiency (CIGIE) Awards

We congratulate the OIG's CIGIE Award Winners who were recognized at CIGIE's Annual Awards Ceremony on October 12, 2021. These awards are in recognition of the outstanding work and dedication of our teams and individuals, as well as their commitment to help preserve the integrity of the banking system and recommend efficiencies and improvements at the FDIC.

Award for Excellence—Evaluation: Preventing and Addressing Sexual Harassment

Team Members: Lisa Conner, Philip Hodge, Rhonda Bunte, Leon Wellons, Cindy Hogue, Stacey Luck, Shelley Shepherd, Sandra Moses.

Award for Excellence—Audit: Security of Critical Building Services at FDIC-owned Facilities

Team Members: Joe Nelson, Luke Itnyre, Jin Zhu, Alexander Kreckel, Jill Benham, Cam Thurber, Sharon Tushin.

Award for Excellence—Investigation: Price Fixing by Foreign Exchange Traders for Central and Eastern European, Middle Eastern and African Currencies

Team Members from FDIC OIG: Gregory Coats, Melisa Baca, Shelley Shepherd, along with partners from the Department of Justice.

Award for Excellence—Special Act: Council of Counsels to Inspectors General COVID-19 Working Group

Team Members: Stacey Luck and several attorneys from the IG community.

Award for Excellence—Evaluations: Inspection & Evaluation Blue Book Working Group

Team Members: Dawn Gilbert and several colleagues from the IG community.

Retirement Congratulations

The following staff member retired from the FDIC OIG during the reporting period. We appreciate his many contributions to the Office over the years and wish him well in future endeavors.

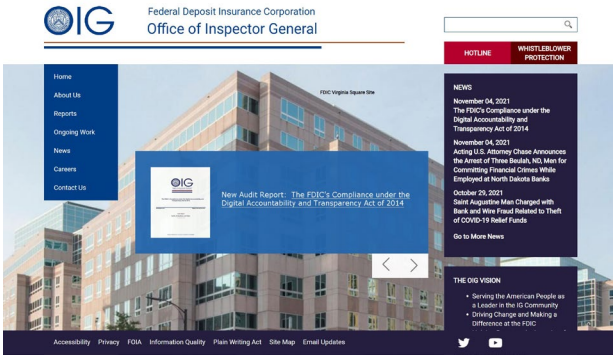
Robert Fry
Evaluations Manager

Farewell to Mark Mulholland

During the reporting period, Mark Mulholland, former Assistant Inspector General for IT Audits and Cyber left the OIG to assume a position in the FDIC's Chief Information Officer Organization. Mark's career included more than 31 years of outstanding work in the IG community, beginning at the General Services Administration OIG in 1989, and including service with the Resolution Trust Corporation and FDIC OIGs. We wish Mark continued success in his new role with the FDIC.

DESIGN: FDIC/OCOM/GRAPHIC DESIGN AND PRINTING UNIT

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



Follow us on Twitter: @FDIC_OIG.

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

OVERSIGHT.GOV
ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE

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

PANDEMIC RESPONSE ACCOUNTABILITY COMMITTEE

www.pandemicoversight.gov

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

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

Make a Difference

OIG HOTLINE

The Office of Inspector General (OIG) Hotline is a convenient mechanism employees, contractors, and others can use to report instances of suspected fraud, waste, abuse, and mismanagement within the FDIC and its contractor operations. Instructions for contacting the Hotline can be found at **www.fdicoig.gov**.

Whistleblowers can contact the OIG's Whistleblower Protection Coordinator through the Hotline by indicating: **Attention: Whistleblower Protection Coordinator.**

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-009-2021