FDIC Office of Inspector General

Semiannual Report to the Congress

October 1, 2020 – March 31, 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 5,590 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured approximately $9.5 trillion in deposits in 4,978 institutions, of which the FDIC supervised 3,209. The Deposit Insurance Fund balance totaled $119.4 billion as of March 31, 2021. Active receiverships as of March 31, 2021 totaled 229, with assets in liquidation of about $273 million.

Semiannual Report to the Congress

October 1, 2020 – March 31, 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 the Semiannual Report for the period from October 1, 2020 to March 31, 2021.

During the reporting period, we issued our assessment of the *Top Management and Performance Challenges Facing the FDIC* and produced our first video highlighting each Challenge, currently posted on our external website. We identified 10 Challenges, including an important new Challenge on diversity and inclusion. The FDIC faces challenges in the following areas:

- 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.

Our audit and evaluation reports continue to address these important risk areas at the FDIC. During this reporting period, we issued several significant reports on Critical Functions in FDIC Contracts; Mobile Device Management; Personnel Security and Suitability; Information Security; and Critical Building Services. We made a total of 57 recommendations for improvements at the Agency during the reporting period.

Our recommendations from these and other reports are having a meaningful impact and lasting effect on critical FDIC programs and operations. As a result of our recent work, the FDIC has:

- Created an entirely new section on Emergency Preparedness and Readiness;
- Revamped its Personnel Security processes for background investigations;
- Revised the Risk Appetite and Standard Operating Procedures for its Enterprise Risk Management program; and
- Joined with other financial regulators to propose a rule requiring banks to report ransomware attacks and other significant cyber incidents.

In addition, our OIG Special Agents have worked closely with law enforcement partners to investigate criminal matters involving complex financial fraud schemes. During the past 6 months, our cases resulted in 82 indictments, 29 convictions, 36 arrests, and nearly $56 million in monetary recoveries. Importantly, among our successful investigations are a number of Paycheck Protection Program cases of individuals defrauding the Government guaranteed-loan program intended to help those most in need during the pandemic crisis. These investigations are conducted in coordination with the Department of Justice, other members of the Pandemic Response Accountability Committee (PRAC), and the IG community.

Also, in connection with our response to the pandemic, I was pleased to participate in moderating the first panel of the PRAC's Financial Sector Oversight Working Group: "*Pandemic Response: Perspectives from the Banking Industry*." The panel included speakers representing lenders and financial institutions, and the discussion addressed topics related to the operation and administration of the Coronavirus Aid, Relief, and Economic Security (CARES) Act programs and other response efforts.

I am also honored to serve as the Vice Chair of the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) newly created Diversity, Equity, and Inclusion Work Group. The Work Group looks to affirm and advance the IG community's long-standing commitment to these issues. It will also highlight the IG community's outstanding oversight work on matters involving diversity, equity, and inclusion and work to identify ways to continue and strengthen these efforts.

The OIG appreciates the continued support of Members of Congress, as well as that of the FDIC Chairman and Board. We remain committed to serving the American people as a leader in the IG community.

Jay N. Lerner
Inspector General
April 30, 2021

Table of Contents

Acronyms and Abbreviations

ASB	Almena State Bank
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BI	Background Investigation
C&C	Cotton & Company LLP
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIOO	Chief Information Officer Organization
COVID-19	Coronavirus Disease 2019
D&I	Diversity and Inclusiveness
DIF	Deposit Insurance Fund
DOJ	Department of Justice
ECU	Electronic Crimes Unit
ERM	Enterprise Risk Management
FBI	Federal Bureau of Investigation
FBR	Failed Bank Review
FCB	First City Bank
FDIC	Federal Deposit Insurance Corporation
FHFA	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
FSB	First State Bank
IDR	In-Depth Review
IG	Inspector General
IRS-CI	Internal Revenue Service-Criminal Investigations
IT	Information Technology
MDM	Mobile Device Management
OIG	Office of Inspector General
OM	Oversight Manager
OMB	Office of Management and Budget
PBI	Preliminary Background Investigation
PII	Personally Identifiable Information
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
PSSP	Personnel Security and Suitability Program
SAR	Suspicious Activity Report
SBA	Small Business Administration
USAO	United States Attorney's Office
USPIS	U.S. Postal Inspection Service

Introduction and Overall Results

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

Our Office conducts its work in line with a set of Guiding Principles that we have adopted, and the results of our work during the reporting period are presented in this report within the framework of those principles. Our Guiding Principles focus on impactful Audits and Evaluations; significant Investigations; partnerships with external stakeholders (the FDIC, Congress, whistleblowers, and our fellow OIGs); efforts to maximize use of resources; Leadership skills and abilities; and importantly, Teamwork

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

Overall Results (October 1, 2020 – March 31, 2021)	
Audit, Evaluation, and Other Products Issued	**9**
Nonmonetary Recommendations	**56**
Investigations Opened	**72**
Investigations Closed	**48**
Judicial Actions:	
Indictments/Informations	**82**
Convictions	**29**
Arrests	**36**
OIG Investigations Resulted in:	
Fines of	**$253,200**
Restitution of	**$55,616,971 ***
Asset Forfeitures of	**$43,000**
Total	**$55,913,171 ****
Referrals to the Department of Justice (U.S. Attorneys)	**169**
Responses to Requests Under the Freedom of Information/Privacy Act	**5**

*Restitution this period includes $480,000 that was ordered joint and several with individuals yet to be sentenced, and $2,087,244 that was ordered joint and several with individuals sentenced in prior periods.

**Total does not include a negotiated monetary settlement this period in the amount of $2,500,000.

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 information security, personnel security and suitability, governance of the Agency's mobile device management solution, critical functions in FDIC contracts, and security of critical building services. In all, audit and evaluation reports issued during the period resulted in 56 nonmonetary recommendations to management and one recommendation involving $361,533 in funds put to better use.

Importantly, our office also reviews the failures of FDIC-supervised institutions causing material losses to the Deposit Insurance Fund (DIF). 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), we determine whether circumstances surrounding the failures would warrant further review. This period we are reporting the results of three Failed Bank Reviews (FBR) of institutions whose failures did not cause a material loss to the DIF. These FBRs are discussed below, and we determined that none of the failures warranted additional review.

Of note during the reporting period, we also issued our assessment of the *Top Management and Performance Challenges Facing the FDIC*. This document is provided to FDIC management for inclusion in the FDIC's Annual Report. Our assessment is posted on our external website, along with a video summarizing the Challenges.

Also noteworthy during the reporting period is that on December 18, the FDIC, the Federal Reserve Board, and the Office of the Comptroller of the Currency issued a joint press release announcing a proposed new regulation that would require all FDIC-insured financial institutions and their service providers to promptly notify their primary Federal regulator if they experience a destructive cyber incident. This proposed rulemaking is a direct result of an advisory memo issued by the OIG's Office of Information Technology (IT) Audits and Cyber to FDIC management in April 2020, which was issued as part of one of that group's ongoing audits–Receiving and Sharing Threat Information to Guide the FDIC's Supervisory Program.

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

The FDIC's Information Security Program–2020

We issued our audit of the *FDIC's Information Security Program—2020*, in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). We engaged a contractor firm to conduct this audit. The audit determined that the FDIC's overall information security program was operating at a Maturity Level 3 (Consistently Implemented) on a scale of 1-5. Programs operating below a Maturity Level 4 are not considered effective.

The FISMA report describes security control 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. Our findings fell into the following categories:

Risk Management. The FDIC had not fully defined its Enterprise Risk Management governance, roles, and responsibilities. In addition, the FDIC had not yet implemented recommendations to integrate privacy into its Risk Management Framework, nor did the FDIC always address Plans of Action and Milestones in a timely manner.

Risk Acceptance Decisions Not Consistently Reassessed. The FDIC did not consistently review its existing Acceptance of Risk documents after they were initially established, nor did it submit those documents for re-approval. Therefore, it could not effectively assess the level of risk it was incurring relative to established Risk Tolerance levels.

Unauthorized Software on the Network. In May 2020, the FDIC discovered an unauthorized commercial software application installed on 32 desktop workstations, and the application had not been approved by the FDIC's IT governance bodies or subject to established configuration management processes. Notably, the FDIC's Office of the Chief Information Security Officer had previously raised security concerns about this same software. The FDIC subsequently removed the unauthorized software from the workstations.

Privacy Control Weaknesses Not Fully Addressed. The FDIC had not completed actions to address previously-identified privacy control weaknesses, such as integration of privacy considerations into its Risk Management Framework; implementation of its planned Document Labeling initiative; establishment of controls to effectively secure Personally Identifiable Information (PII) stored in network shared drives; and disposal of PII within established timeframes.

Oversight and Monitoring of Outsourced Systems Not Adequate. In June 2020, the FDIC rescinded its Outsourced Solution Assessment Methodology used to assess security and privacy risks associated with outsourced information systems because it did not align with National Institute of Standards and Technology guidance. As a result, the FDIC had not properly categorized some of its systems covered by the assessment methodology or subjected these systems to a proper risk assessment, authorization to operate, and ongoing monitoring.

Cloud-based Systems Not Subject to Annual Control Assessments. As of April 2020, the FDIC had 14 cloud based systems that provided critical IT services. The FDIC did not subject these cloud-based systems to required annual control assessments.

We made eight recommendations for the FDIC to reassess its risk acceptance decisions in accordance with policy; implement control improvements to prevent the unauthorized installation of software on the network; and complete actions to address open Plans of Action and Milestones related to baseline configurations. We also recommended that the FDIC assess and improve controls for managing administrative accounts; implement a process to ensure all outsourced information systems are subject to the Risk Management Framework; and ensure all cloud-based systems are subject to annual security and privacy control assessments. Finally, we recommended that the FDIC update its IT contingency planning policy and incorporate additional scenarios into its IT contingency plan testing. FDIC Management concurred with the eight recommendations in the report.

The FDIC's Personnel Security and Suitability Program

We issued an evaluation report on the FDIC's Personnel Security and Suitability Program (PSSP) during the reporting period. The effectiveness of the FDIC's PSSP is critically important to ensure that FDIC employees and contractor personnel are properly screened and investigated prior to being granted access to systems and entrusted with sensitive, confidential, or, in some cases, classified information.

Before individuals can be hired by the FDIC, they must meet minimum standards for employment with the FDIC. Contractor personnel must meet minimum standards of integrity and fitness. Determining whether an individual meets the FDIC's minimum employment or integrity and fitness standards is accomplished by way of a preliminary background investigation (PBI). Federal regulations also require that a background investigation (BI) be conducted on each Federal employee and contractor.

We found that the FDIC's PSSP was not fully effective in ensuring that: (1) PBIs were completed in a timely manner; (2) BIs were ordered and adjudicated commensurate with position risk designations; and (3) re-investigations were ordered within required timeframes. Specifically, after analyzing PSSP-related data for all employees and contractor personnel with access to the FDIC's IT systems as of December 2, 2019, we determined that:

- The FDIC did not remove multiple contractors with unfavorable background investigation adjudications in a timely manner;
- The FDIC did not follow its Insider Threat protocols and conducted limited risk assessments for the contractors with unfavorable adjudications;
- The FDIC did not initiate and order numerous required periodic reinvestigations in a timely manner;
- Data on contractor position risks were unreliable;
- Employee background investigations were sometimes not commensurate with position risk;
- Some of the FDIC files were missing certain PBI data; and
- The FDIC was not meeting its goals for completing PBIs within a specified timeframe.

Importantly, the results of our evaluation led us to conclude that the risks within the FDIC's PSSP were not fully reflected in the FDIC's Risk Inventory as a component of its Enterprise Risk Management program. This risk analysis was particularly important as the FDIC was beginning contingency planning for surge staffing in the event that the current pandemic negatively impacts the banking sector. We noted that the FDIC's Operating Committee, as the Risk Management Council, needed to ensure that the Division of Administration was satisfactorily addressing the risks associated with the PSSP.

We made 21 recommendations aimed at strengthening the PSSP's controls and ensuring that the FDIC is in full compliance with Federal requirements. The FDIC concurred with all 21 recommendations.

Governance of the FDIC's Mobile Device Management Solution

Our audit report on Governance of the FDIC's Mobile Device Management (MDM) Solution highlighted weaknesses related to the FDIC's actions to implement a new mobile device management solution. The FDIC relies heavily on smartphones and tablets to support its business operations and communications. The FDIC uses a cloud-based MDM solution to secure and manage these mobile devices.

In August 2019, the FDIC decided to replace its MDM solution with a new MDM solution (proposed MDM solution) which offered greater functionality. On October 4, 2019, the FDIC awarded a contract valued at $965,000 for the proposed MDM solution. However, in November 2019, the FDIC decided to terminate the contract because the FDIC could not validate whether the proposed MDM solution would satisfy the FDIC's security requirements. In addition to the FDIC's internal and contractor resources expended on the project, the FDIC compensated the vendor $343,533 for the proposed MDM solution. Notwithstanding the payment to the vendor, the FDIC never used the solution for which it had signed a contract to purchase.

The objective of our audit was to assess the adequacy of the FDIC's governance over the proposed MDM solution. The audit focused on the FDIC's actions to evaluate, procure, authorize, and subsequently terminate its contract for the proposed MDM solution. We found that the FDIC's Chief Information Officer Organization (CIOO) did not:

- Identify elevated and growing risks associated with the proposed MDM solution in reports describing the health and status of the project provided to CIOO Executives and other FDIC stakeholders;
- 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 in its procedures for managing the use of Limited Authorizations to Operate.

In addition, 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.

Our report contained five recommendations intended to strengthen the FDIC's processes and governance for evaluating, authorizing, and procuring new technologies. In addition, we identified $361,533 of funds put to better use (termination payment of $343,533 and $18,000 paid to a contractor after security concerns were identified). FDIC management concurred with all of the recommendations.

Critical Functions in FDIC Contracts

One of our reports during the period focused on Critical Functions in FDIC Contracts. Like other Federal agencies, the FDIC relies on contractors to support a wide range of activities. 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.

If agencies do not effectively oversee their contracts and establish strong control environments, contractors could inappropriately influence government decision-making and an agency could lose control of its mission and operations. In response to this risk, in September 2011, OMB provided guidance. This guidance focuses on managing the performance of Inherently Governmental Functions and Critical Functions in order "to ensure that government action is taken as a result of informed, independent judgments made by government officials." OMB defines a Critical Function as one "that is necessary to the agency being able to effectively perform and maintain control of its mission and operations. Typically, critical functions are recurring and long-term in duration."

The contractor that was the main focus of our review performed services in support of the FDIC's information security and privacy program. We considered these services to fit the OMB definition of Critical Functions. For 2019, this contractor's services comprised 38.3 percent ($16.2 million) of the FDIC's annual operating expenses for information security and privacy ($42.3 million).

We determined that the FDIC did not have policies and procedures for identifying Critical Functions in its contracts, as recommended by OMB and embodied in industry standards. Therefore, while we determined that the contractor performed Critical Functions at the FDIC, the FDIC did not identify these services as Critical Functions during its procurement planning phase.

As a result, the FDIC also did not implement heightened contract monitoring activities for Critical Functions as outlined in OMB guidance and best practices identified and used by other government agencies. Such heightened contract monitoring activities would include: (1) performing a procurement risk assessment, (2) establishing a management oversight strategy, (3) conducting periodic reviews, and (4) providing formal reports to the FDIC Board of Directors on an individual and aggregate basis.

Without these best practices in place, the FDIC could not be assured that it would provide sufficient management oversight of this contractor or other contractors performing Critical Functions. In particular, the FDIC may not ensure that it has an adequate number of employees with the appropriate training, experience, and expertise to oversee the procurements of Critical Functions.

We made 13 recommendations in this report. The recommendations included incorporating provisions of OMB guidance into the FDIC's policies and procedures, identifying Critical Functions during the procurement process, and implementing heightened contract monitoring for Critical Functions. FDIC management concurred with 1 of the 13 recommendations and partially concurred with the remaining 12 recommendations.

Security of Critical Building Services at FDIC-owned Facilities

Another report we issued during the reporting period focused on the Security of Critical Building Services at FDIC-owned Facilities. The FDIC relies heavily on critical building services to perform mission-essential functions and ensure the health and safety of its employees, contractors, and visitors. These services include electrical power; water; and heating, ventilation, and air conditioning; and they may face threats to their uninterrupted operations from numerous sources, such as cyberattacks, insiders, environmental disasters, and other dangers.

The FDIC maintains a Facilities Management Contract with EMCOR Government Services, Inc. (EMCOR), under which the contractor operates, maintains, repairs, and replaces mechanical equipment that supports building services at the FDIC's Virginia Square facility.

We assessed whether the FDIC had effective controls and practices to protect electrical power; heating, ventilation, and air conditioning; and water services at its Virginia Square facility. Our audit focused on security controls over three information systems used by the FDIC, EMCOR, and its subcontractors to monitor, manage, and help ensure the uninterrupted delivery of these critical building services. We also assessed compliance with key security provisions in the Facilities Management Contract.

The FDIC implemented various controls and practices to protect critical building services and ensure their continued delivery. We found, however, that the FDIC did not subject the three information systems to the Risk Management Framework established by the National Institute of Standards and Technology, as required by OMB policy. As a result, we identified ineffective security controls, and a lack of security oversight and monitoring, for all three systems we reviewed. Ineffective security controls increased the risk of unauthorized access to these three systems, which could have led to a disruption of the systems, corruption of the systems' data, or other malicious activity.

The FDIC also did not maintain signed Confidentiality Agreements for EMCOR or its subcontractor personnel working at the Virginia Square facility, as required by the Facilities Management Contract and FDIC policy. Confidentiality Agreements are important to the security posture of the FDIC, because these personnel had access to the FDIC's information technology network and sensitive areas in the Virginia Square facility. In addition, the FDIC did not ensure that all EMCOR and subcontractor personnel had completed Information Security and Privacy Awareness Training or Insider Threat and Counterintelligence Awareness Training, as required by FDIC policy.

We made 10 recommendations to address these weaknesses, and FDIC management concurred with all 10.

Reports of Failed Banks

One of the most important statutory responsibilities of our Office under the Federal Deposit Insurance (FDI) Act is to conduct material loss reviews of failed FDIC-supervised institutions when those failures cause a significant loss to the Deposit Insurance Fund, that is, a loss exceeding $50 million. When the DIF incurs a loss under $50 million, the FDI Act requires the Inspector General of the appropriate federal banking agency to determine the grounds upon which the state or federal banking agency appointed the FDIC as receiver and whether any unusual circumstances exist that might warrant an In-Depth Review (IDR) of the loss. We completed three such Failed Bank Reviews during the reporting period, as discussed below:

Failed Bank Review of First State Bank, Barboursville, West Virginia
On April 3, 2020, the West Virginia Division of Financial Institutions closed the First State Bank (FSB) and appointed the FDIC as receiver. FSB was a locally owned, state-chartered nonmember bank located in Barboursville, West Virginia, that the FDIC first insured on May 14, 1934. FSB was wholly owned by First Bancshares, Inc., a single bank holding company. The bank President and Chief Executive Officer's family controlled 82 percent of Bancshares' common stock and Bancshares' Employee Stock Ownership Plan owned the remaining 18 percent of common stock.

According to the FDIC's Division of Finance, the estimated loss to the DIF was $47 million or 30 percent of the bank's $156 million in total assets. The West Virginia Division of Financial Institutions took possession and closed FSB because it had experienced longstanding capital and asset quality issues, was substantially impaired (as of March 11, 2020), and had become insolvent.

We determined that FSB was the victim of an employee fraud scheme discovered in 2012 that impacted its financial condition. However, as identified in multiple FDIC examinations conducted from 2012 through 2019, the Board's oversight of the bank was also deficient and the bank's risk management practices were poor. FSB's Board and management failed to execute actions and address recommendations to improve FSB's safety and soundness, its capital levels and liquidity continued to decline, and the bank ultimately failed.

We concluded that no unusual circumstances existed that warranted an IDR.

Failed Bank Review of First City Bank of Florida, Fort Walton Beach, Florida
On October 16, 2020, the Florida Office of Financial Regulation closed the First City Bank of Florida (FCB) and appointed the FDIC as receiver. FCB was a state-chartered nonmember bank located in Fort Walton Beach, Florida. FCB was wholly owned by Florida First City Banks, Inc., a single bank holding company. According to the FDIC's Division of Finance, the estimated loss to the DIF as of November 30, 2020 was approximately $10 million or 7 percent of the bank's $136 million in total assets. According to Office of Financial Regulation documentation, the Office took possession and closed the Bank because FCB had experienced longstanding issues related to capital, asset quality, and earnings, and had become "imminently insolvent" as of June 30, 2020.

We determined that FCB suffered from longstanding capital and loan quality problems, resulting from poor credit underwriting and administration practices, and significant exposure to commercial real estate markets. The bank was unable to recover from the financial crisis that began in 2007 despite the subsequent improvement in economic and real estate market conditions. As identified in FDIC examinations, the Board and Management failed to execute actions and address recommendations to improve FCB's safety and soundness. In addition, FCB's capital levels and earnings continued to decline, and the bank ultimately failed.

Given that the FDIC identified the risk and took action to address it in 2019, the unusual circumstances did not warrant an IDR of the loss.

Failed Bank Review of Almena State Bank, Almena Kansas

On October 23, 2020, the Kansas Office of the State Bank Commissioner closed Almena State Bank (ASB) and appointed the FDIC as receiver. ASB was a state-chartered, nonmember bank that the FDIC insured in 1936. The bank operated two offices in Almena and Norton, Kansas. The bank was wholly owned by Almena Investments, LLC, a one-bank holding company. The former Chairman of the Board of Directors and his wife jointly controlled 59 percent of the outstanding shares of the bank.

According to the FDIC's Division of Finance, the estimated loss to the DIF was $18 million or 27 percent of the bank's $69 million in total assets. The Kansas Office of the State Bank Commissioner took possession and closed ASB because it was considered to be critically undercapitalized, lacked a plan to restore capital, and operated in an unsafe and unsound manner.

We determined that ASB experienced longstanding capital and asset quality issues resulting from the aggressive growth strategy initiated in 2014 to expand its loan portfolio by originating large-dollar guaranteed loans issued by the U.S. Small Business Administration and Farm Service Agency of the U.S. Department of Agriculture. It launched this growth strategy without sufficient experience, and coupled with hazardous lending practices and inadequate Board oversight, this strategy resulted in the bank's deterioration. ASB's Board and management failed to comply with a 2019 FDIC and State Bank Commissioner-issued Consent Order, including the development and implementation of capital and liquidity restoration plans. The bank became undercapitalized in May 2019 and critically undercapitalized in July 2020. The Board was unable to remediate the bank's deficient capital condition resulting in its failure.

We concluded that no unusual circumstances existed that warranted an IDR of the loss.

Ongoing audit and evaluation reviews at the end of the reporting period were addressing such issues as the FDIC's Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders, Mobile Device Security and Management, Data Reliability in the Virtual Supervisory Information on the Net System, Receiving and Sharing Threat Information, Security Controls over the FDIC's Wireless Networks, and Security Controls over the Windows Active Directory, among others. These ongoing reviews are listed on our website and, when completed, their results will be presented in an upcoming semiannual report.

****

Top Management and Performance Challenges Facing the FDIC

During the reporting period, we issued our report identifying the Top Management and Performance Challenges facing the FDIC. We did so pursuant to the Reports Consolidation Act of 2000 and the Office of Management and Budget Circular A-136 (revised August 27, 2020). The purpose of our report is to summarize the most serious challenges facing the Agency, and to briefly assess the FDIC's progress to address them. This document also helps guide the focus of our independent oversight work at the FDIC.

The Top Challenges document is based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities. This year, we identified the following 10 Top Challenges facing the FDIC:

- **Ensuring Readiness in a Pandemic Environment:** The FDIC should continue to stand ready to fulfill its mission to maintain financial stability in the banking system, and to identify and mitigate risks through examinations. The FDIC should also prepare for bank failures in the event that losses overwhelm banks. Further, the FDIC should review banks' adherence to Government-guaranteed loan program requirements (such as the Paycheck Protection Program or PPP) and identify risks that may affect the safety and soundness of a financial institution.
- **Mitigating Cybersecurity Risks in the Banking Sector:** In recent months, cyberattacks against banks have increased with growing frequency and severity, and may intensify during the pandemic. The FDIC should ensure that it has IT examination processes and staff with the requisite skills to identify and mitigate cybersecurity risks at banks, including those associated with third-party service providers.
- **Improving IT Security Within the FDIC:** Federal agencies face a growing risk of cybersecurity incidents. The rapid transition to remote work in response to pandemic protocols amplifies the Government's reliance on IT systems and accelerates implementation of technologies. The FDIC must have robust controls to secure its systems and ensure the protection of its information and data.
- **Securing FDIC Personnel, Facilities, and Information:** The FDIC is responsible for protecting a workforce of approximately 5,800 employees and 1,600 contract personnel who work at 94 FDIC facilities throughout the country. The FDIC should continue to strengthen its programs to ensure that its facilities are secure, that staff meet suitability requirements, and that the FDIC work environment is safe and free from discrimination and harassment. The FDIC should also maintain the security of its IT systems and hard-copy records containing sensitive information about banks and PII of employees, contractors, bank management, and bank deposit holders.

- **Ensuring and Aligning Strong Governance at the FDIC:** Effective governance is critical to ensure that the FDIC assesses risks and consistently implements its policies. The FDIC should ensure the establishment and proper function of its governance processes, including an Enterprise Risk Management program. Quality data is also a critical component of FDIC governance to allow the Board, Executives, and Managers to assess the effectiveness of FDIC programs.
- **Augmenting the FDIC's Sharing of Threat Information:** Sharing threat information is critical to ensuring that banks and examiners have the necessary information to protect financial institutions, the banking sector, and the economy. Timely and actionable threat information allows bank management to mitigate risks and thwart dangers, and prompts the FDIC to adjust supervisory strategies in a timely fashion. Without effective threat information sharing, policy makers, bank examiners, and bank management may be unaware of threats that could affect the integrity, safety, and soundness of financial institutions.
- **Supporting Diversity in Banking:** Minority communities and businesses have suffered significantly during the pandemic. The FDIC plays an important role to support Minority Depository Institutions that serve and promote minority and low- and moderate-income communities. This work can be enhanced with the FDIC's continued commitment to diversity and inclusion in the Federal regulatory process, which is critical for the FDIC to foster greater financial inclusion for all Americans.
- **Managing Human Resources and Planning for the Future Workforce:** Forty-two percent of FDIC employees (nearly 2,400 individuals) are eligible to retire within 5 years. The FDIC faces retirement rates of almost 60 percent among FDIC Executives and Managers over that same time period. The FDIC should continue to manage the agency's exposure to gaps in leadership and mission-critical skills, especially given the significant investments in, and time required for, bank examiner commissioning.
- **Overseeing Contracts and Managing Supply Chain Risk:** The FDIC's contracting budget for 2021 is approximately $549 million, including an increase from 2020 of more than $166 million (43 percent) for contractor-provided services. The FDIC should execute a contracting program that ensures effective oversight of its acquisition of goods and services. In addition, the FDIC should ensure that it adequately manages and mitigates supply chain risks associated with such contracts.
- **Enhancing Rulemaking at the FDIC:** The FDIC should have a transparent rulemaking process that balances the need for regulation and the burden on financial institutions' compliance. A foundational component of rulemaking is reliable information to measure a regulation's costs and benefits.

We believe that the researched and deliberative analysis in our Top Management and Performance Challenges document will be beneficial and constructive for policy makers, including the FDIC and Congressional oversight bodies. We further hope that it is informative for the American people regarding the programs and operations at the FDIC and the Challenges it faces.

Pandemic Response Accountability Committee Identifies Management Challenges

The Coronavirus Aid, Relief, and Economic Security (CARES) Act and other related legislation provide more than $3 trillion in Federal spending to address the public health and economic crises resulting from the Coronavirus Disease 2019 (COVID-19) pandemic. The more than $3 trillion in pandemic response funds includes those funds authorized under the Coronavirus Response and Relief Supplemental Appropriations Act as well as the Coronavirus Preparedness and Response Supplemental Appropriations Act, 2020; the Families First Coronavirus Response Act; the CARES Act; and the Paycheck Protection Program and Health Care Enhancement Act.

As part of the Coronavirus Stimulus Bill, the IG community has come together to form the Pandemic Response Accountability Committee (PRAC). The FDIC OIG is serving as a member on the PRAC, which conducts and coordinates oversight of covered funds and the Coronavirus response, and supports other Inspectors General in order to: detect and prevent fraud, waste, abuse, and mismanagement; and identify major risks that cut across programs and agency boundaries.

In June 2020, the PRAC released its first Management Challenges report, titled *Top Challenges Facing Federal Agencies: COVID-19 Emergency Relief and Response Efforts*. The PRAC summarized the challenges by broad issue categories to identify common themes and key areas of concern. While many challenges varied from agency to agency, the analysis identified common concerns across agencies despite their different sizes and missions. The challenges identified were:

- Financial Management of Relief Funding,
- Grants and Guaranteed Loan Management,
- IT Security and Management, and
- Protecting Health and Safety.

Given the changing nature of the pandemic and the Federal government's response, the PRAC re-visited the original top management challenges to ensure that the PRAC is providing timely information to Congress and the Administration about the response efforts. In February 2021, the PRAC reached back out to OIGs from more than 40 agencies that received emergency funds or were involved in the pandemic response and reviewed Management Challenges reports issued by OIGs since March 2020. As a result, the PRAC added four new management challenges:

- Preventing and Detecting Fraud against Government Programs,
- Informing and Protecting the Public from Pandemic-Related Fraud,
- Data Transparency and Completeness, and
- Federal Workforce Safety.

Our Office looks forward to continuing to work with the IG community to oversee the funds provided in the legislation and to keep the public informed, as we address the challenges and work on this important oversight effort.

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; and the Department of Justice (DOJ), including U.S. Attorneys' Offices (USAO) and the Federal Bureau of Investigation (FBI). 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.

Pandemic Response: Perspectives from the Banking Industry Virtual Listening Forum

On February 4, the PRAC's Financial Sector Oversight working group released a video of its first in a series of panels with experts from the financial services sector. FDIC IG Jay N. Lerner, and the IG for the Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection, Mark Bialek moderated the first panel titled: "Pandemic Response: Perspectives from the Banking Industry." The panel included speakers from lenders and financial institutions that administer programs established or expanded through pandemic relief legislation. Panelists represented a variety of views ranging from community banks, minority depository institutions, and large financial institutions.

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 electronic-related prohibited activity that may harm or threaten to harm FDIC programs or operations. 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 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 funds distributed through the CARES Act. Notably, during the reporting period, the FDIC OIG's efforts related to the Federal government's COVID-19 pandemic response resulted in 48 indictments/criminal complaints, 21 arrests, and 16 convictions, often involving fraud in the Paycheck Protection Program (PPP).

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 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. Three actions in cases involving COVID-relief fraud are also included in our discussion of cases from the reporting period.

Former Aurora Business Owner Sentenced for $30 Million Fraud Schemes

On October 16, Russell Grundy, of Hilton Head South Carolina, formerly of Aurora, was sentenced to 8 years in federal prison without parole, and was ordered to pay $14,847,451 in restitution to his victims, for his role in a series of fraud schemes totaling more than $30 million.

In January 2020, Grundy pleaded guilty to two counts of wire fraud, one count of making a false statement on a loan application, and one count of money laundering.

Grundy's multiple schemes to defraud financial institutions, a Native American Tribe, and his former clients potentially totaled more than $30 million and resulted in nearly $15 million in actual losses.

Source: USAO for the Western District of Missouri.
Responsible Agencies: FDIC OIG, FBI, Internal Revenue Service-Criminal Investigations (IRS-CI), and the Small Business Administration (SBA) OIG.
Prosecuted by the USAO, Western District of Missouri.

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

On October 27, Gladys Collins, of Wayne, New Jersey, pleaded guilty to an information charging her 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, Collins 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.

Three of Collins' conspirators have previously pleaded guilty to charges relating to their role in the Cash Flow Partners bank fraud conspiracy and are awaiting sentencing.

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

Boulder Man Sentenced to 5 Years in Federal Prison for Nearly $32 Million Bank Fraud Scheme

On November 9, Michael Scott Leslie, of Boulder, Colorado, was sentenced to 5 years in federal prison for bank fraud and aggravated identity theft.

Leslie owned, operated, or otherwise had an interest in several business entities, some of which were operated out of Colorado. Through these business entities, Leslie sold residential mortgage loans to investors, including an FDIC-insured bank in Texas.

Between October 2015 and the end of 2017, Leslie devised and executed a scheme to defraud the victim bank by selling it 144 fraudulent residential mortgage loans valued at $31,908,806.88. These loans were purportedly originated by one of Leslie's companies, Montage Mortgage, and "closed" by Snowberry, which earned fees for the closing. The loans were then presented and sold to the victim bank until Montage identified a final investor. For these 144 fraudulent loans, that final investor was Mortgage Capital Management. Leslie never disclosed to the victim bank that he operated this entity and Snowberry, or the fact that sales to Mortgage Capital Management, even if they had been real, were not arms-length transactions.

The borrowers listed on these 144 fraudulent loans were real individuals, but they had no idea that their identities had been used as part of the sale of the fraudulent loans. To execute this scheme, Leslie forged signatures on closing documents and fabricated and altered credit reports as well as title documents, often by using the names of legitimate companies. The fraudulent real estate transactions were never filed with the respective counties in which the properties were located, there were no closings, and no liens were ever recorded. Through numerous bank accounts for the various business entities and his personal accounts, the defendant used money in a Ponzi-like fashion from prior fraudulent loans sold to the victim bank to fund future fraudulent loans. This complex flow of money continued until the defendant's fraud was detected. When the fraud was discovered, the victim bank still had 12 fraudulent loans, valued at $3,887,505.93, on its books that it could not, given that the loans did not exist, sell to any other legitimate third-party investor.

Source: DOJ.
Responsible Agencies: FDIC OIG, Housing and Urban Development OIG, and FBI. Prosecuted by the USAO, District of Colorado.

Former Bank Executive Sentenced to Prison for $15 Million Construction Loan Fraud

On November 10, Troy A. Gregory, of Lawrence, Kansas, was sentenced to 60 months in prison for his role in carrying out a bank fraud scheme to obtain a $15 million construction loan from 26 Kansas banks. He was ordered to pay $4,731,208.16 in restitution.

Following a 2-week trial in August 2019, Gregory was found guilty of four counts of bank fraud and two counts of false statements. According to the evidence presented at trial and at the sentencing hearing, Gregory was a bank executive and loan officer who had made millions of dollars in loans to a group of borrowers who were struggling to make payments on the loans. Beginning in late 2007, Gregory initiated the process of making a $15.2 million construction loan to build an apartment complex to that same group of borrowers so they could pay back the other outstanding loans. Gregory's bank shared this loan with 25 other Kansas banks. To convince the other banks to participate, Gregory made and caused others to make false statements about the strength of the borrowers, the debt status of the apartment property, and the existence of approximately $1.7 million in certificates of deposit for collateral on the loan, all to get the loan approved.

Instead of using the loan funds promised for building the apartments, Gregory immediately diverted over $1 million of the loan to pay for part of the certificates of deposit pledged as collateral, pay off debt on the apartment property, and make payments on unrelated loans.

The victim banks collectively lost approximately $5 million on this fraudulent loan.

Source: IRS-CI.
Responsible Agencies: FDIC OIG, IRS-CI, FBI, Federal Housing Finance Agency (FHFA) OIG, and the Federal Reserve Board OIG. Prosecuted by the Securities and Financial Fraud Unit-Fraud Section, DOJ.

Former Louisville Investment Advisor Sentenced to 8 Years in Federal Prison

On December 17, Christopher Hibbard, of Louisville, Kentucky, was sentenced to 97 months in prison and 3 years of supervised release after pleading guilty on June 30, 2020 to one count of investment fraud and nine counts of wire fraud.

From about February 9, 2007 to December 20, 2008, Hibbard made dozens of wire transfers from the brokerage account of a Louisville resident in the total amount of $1,226,995. Hibbard admitted that he had misappropriated and used a substantial portion of the client's monies for his own personal use. After nearly exhausting the funds in the account, Hibbard presented the client with fraudulent brokerage statements that were used to lull the client into believing the account contained as much as $4 million.

In addition, between January 10, 2011, and December 20, 2017, Hibbard initiated over 300 unauthorized automated clearing house transfers by wire in interstate commerce from client accounts under his management to an American Express account that he controlled. Hibbard caused the transfers to be made without the knowledge, permission, or other authorization of the account holder(s), thereby misappropriating and embezzling more than $3 million in client monies and using the funds for personal expenditures. In order to effectuate his scheme to defraud, Hibbard engaged in unauthorized trading and liquidation of clients' investments, made unauthorized withdrawals from client annuity accounts, and committed acts of forgery.

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

Former Bank President Sentenced for Arson and Fraud Scheme

On February 23, Anita Gail Moody, of Cooper, Texas, was sentenced to 96 months in federal prison, after pleading guilty in June 2020 to conspiracy to commit bank fraud and arson. In addition, Moody agreed to pay $11,136,241.82 in restitution.

On May 11, 2019, according to information presented at court, Moody was the President of Enloe State Bank in Cooper, Texas, when the bank had a fire that was determined to be arson. The fire was contained to the bank's boardroom, but the entire bank suffered smoke damage. Several files had been stacked on the boardroom table, all of which were burned in the fire. Coincidentally, the bank was scheduled for a review by the Texas Department of Banking the following Monday.

Further investigation into the fire and the bank revealed that Moody had been creating false nominee loans in the names of several people, including some actual bank customers. Moody eventually admitted to setting the fire in the boardroom to cover up the criminal activity concerning the false loans. She also admitted to using the fraudulently obtained money to fund her boyfriend's business, other businesses of friends, and her own lifestyle. The fraudulent activity, which began in 2012, resulted in a loss to the bank of approximately $11 million.

Source: Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and FDIC Division of Risk Management Supervision.
Responsible Agencies: FDIC OIG and ATF. Prosecuted by the USAO, Eastern District of Texas.

Raleigh County Pharmacist Sentenced to More than 11 Years in Prison for Fraud Scheme

On March 18, Natalie Cochran, of Daniels, West Virginia, was sentenced to 135 months in prison, 3 years of supervised release, and was ordered to pay over $2.5 million in restitution to her victims for her role in a fraud scheme that cost victims over $2 million in losses. Cochran earlier pleaded guilty to wire fraud and money laundering.

Cochran, the owner of Technology Management Solutions and Tactical Solutions Group, knowingly defrauded and took money and property from individuals, a financial institution, and several other companies from approximately June 2017 through at least August 22, 2019. She persuaded them to invest in the two companies she owned and in phony government contracts by making false representations regarding her and her companies' experience and purported success as government contractors. Cochran convinced at least 11 people to invest approximately $2.5 million in alleged government contracts. The investors paid through personal checks, cashier's checks and wire transfers. She also convinced an investor to send $511,920 through a wire transfer from North Carolina. Cochran never invested the money she received from victims. Instead, she put it into her personal and business bank accounts for personal purposes unrelated to the investments.

As part of this scheme, Cochran used some investors' funds to pay other investors a partial return on their investment.

Source: USAO, Southern District of West Virginia.
Responsible Agencies: FDIC OIG, United States Secret Service, and the West Virginia State Police. Prosecuted by the USAO, Southern District of West Virginia.

Washington Man Pleads Guilty to $244 Million Ghost-Cattle Scam

On March 31, Cody Allen Easterday, of Mesa, Washington, pleaded guilty to defrauding Tyson Foods Inc. and another company (Company 1) out of more than $244 million.

According to court documents, Easterday used his company, Easterday Ranches Inc., to enter into a series of agreements with Tyson and Company 1 under which Easterday Ranches agreed to purchase and feed cattle on behalf of Tyson and Company 1. Per the agreements, Tyson and Company 1 would advance Easterday Ranches the costs of buying and raising the cattle. Once the cattle were slaughtered and sold at market price, Easterday Ranches would repay the costs advanced (plus interest and certain other costs), retaining as profit the amount by which the sale price exceeded the sum repaid to Tyson and Company 1.

Beginning in approximately 2016 and continuing through November 2020, Easterday submitted and caused others to submit false and fraudulent invoices and other information to Tyson and Company 1. These false and fraudulent invoices sought and obtained reimbursement from the victim companies for the purported costs of purchasing and growing hundreds of thousands of cattle that neither Easterday nor Easterday Ranches ever purchased, and that did not actually exist. As a result of the scheme, Tyson and Company 1 paid Easterday Ranches over $244 million for the purported costs of purchasing and feeding these ghost cattle.

Easterday used the fraud proceeds for his personal use and benefit, and for the benefit of Easterday Ranches. In connection with his commodity futures trading, Easterday also defrauded the CME Group Inc., which operates the world's largest financial derivatives exchange. On two separate occasions, Easterday submitted falsified paperwork to the exchange that resulted in the exchange exempting Easterday Ranches from otherwise-applicable position limits in live cattle futures contracts.

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

Engineer Pleads Guilty to More Than $10 Million of COVID-Relief Fraud

On February 9, Shashank Rai, of Beaumont, Texas, pleaded guilty to one count of making false statements to a bank for his role in filing fraudulent bank loan applications seeking more than $10 million in forgivable loans guaranteed by the SBA under the CARES Act.

As part of his guilty plea, Rai admitted that he sought millions of dollars in forgivable loans guaranteed by the SBA from two different banks by claiming to have 250 employees earning wages when, in fact, no employees worked for his purported business. Rai made two fraudulent claims to two different lenders for loans guaranteed by the SBA for COVID-19 relief through the PPP.

According to court documents, the Texas Workforce Commission provided information to investigators of having no records of employee wages having been paid in 2020 by Rai or his purported business, Rai Family LLC. In addition, the Texas Comptroller's Office of Public Accounts reported to investigators that Rai Family LLC reported no revenues for the fourth quarter of 2019 or the first quarter of 2020.

According to court documents, materials recovered from the trash outside of Rai's residence included handwritten notes that appeared to reflect an investment strategy for the $3 million, which is the amount of money that Rai allegedly sought from the second lender.

Source: DOJ.
Responsible Agencies: FHFA OIG, SBA OIG, and USPIS. Prosecuted by the Fraud Section of the Criminal Division of DOJ and the USAO, Eastern District of Texas.

Man Purchased Lamborghini After Receiving $3.9 Million in PPP Loans

On February 10, David T. Hines, of Miami, Florida, pleaded guilty to one count of wire fraud for his role in obtaining $3.9 million in PPP funds, and using those funds, in part, to purchase a Lamborghini sports car.

As part of his guilty plea, Hines admitted that he fraudulently sought millions of dollars in PPP loans through applications to an insured financial institution on behalf of different companies. Hines caused to be submitted fraudulent loan applications that made numerous false and misleading statements about the companies' respective payroll expenses. The financial institution approved and funded approximately $3.9 million in PPP loans.

Hines further admitted that within days of receiving the PPP funds, he used the funds to purchase a 2020 Lamborghini Huracan sports car for approximately $318,000. Plea documents indicate that in the days and weeks following the disbursement of PPP funds, Hines did not make payroll payments that he claimed on his loan applications, but did, however, use the PPP proceeds for personal expenses.

Source: Fraud Section of the Criminal Division of DOJ.
Responsible Agencies: FDIC OIG, USPIS, SBA OIG, Federal Reserve Board OIG, and IRS-CI. Prosecuted by the Fraud Section of the Criminal Division of DOJ.

Pewaukee Man Pleads Guilty to Directing COVID-Relief Fraud Scheme

On February 23, Thomas Smith, of Pewaukee, Wisconsin, pleaded guilty to one count of bank fraud for his role in fraudulently obtaining over $1 million in PPP loans.

As part of his guilty plea, Smith admitted that he fraudulently sought over $1.2 million in PPP loans through applications to an insured financial institution on behalf of eight different companies. According to his plea agreement, Smith caused fraudulent loan applications to be submitted that made numerous false and misleading statements about the companies' respective payroll expenses. Based on these representations, the financial institution approved and funded over $1 million in loans. According to plea documents, Smith then directed his co-conspirators to send him portions of the PPP funds within days of receiving them and used the proceeds for personal expenses.

Responsible Agencies: FDIC OIG, FBI, IRS-CI, and SBA OIG. Prosecuted by the USAO, Eastern District of Wisconsin and the Fraud Section of the Criminal Division of DOJ.

Coppell Man Pleads Guilty to $24 Million COVID-Relief Fraud Scheme

On March 24, Dinesh Sah, of Coppell, Texas, pleaded guilty to one count of wire fraud and one count of money laundering for his role in orchestrating a fraudulent scheme to obtain approximately $24.8 million in forgivable PPP loans and laundering the proceeds.

To execute his scheme, Sah admitted that he 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 admitted that he 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.

Sah admitted that, based on his false statements and fabricated documents, he received over $17 million in PPP loan funds and diverted the proceeds for his personal benefit. As part of his guilty plea, Sah will forfeit, among other property, eight homes, numerous luxury vehicles, and more than $7.2 million in fraudulent proceeds that the government had seized to date.

Source: DOJ, Fraud Section.
Responsible Agencies: FDIC OIG, IRS-CI, and Treasury Inspector General for Tax Administration. Prosecuted by the USAO, Northern District of Texas, and the Fraud Section of the Criminal Division of DOJ.

Strong Partnerships with Law Enforcement Colleagues

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

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

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

We also worked closely with DOJ; the FBI; other OIGs; other Federal, state, and local law enforcement agencies; and FDIC Divisions and Offices as we conducted our work during the reporting period.

Keeping Current with Criminal Activities Nationwide

The FDIC OIG participates in the following bank fraud, mortgage fraud, cyber fraud, and other working groups and task forces throughout the country. We benefit from the perspectives, experience, and expertise of all parties involved in combating criminal activity and fraudulent schemes nationwide.

New York Region	New York Identity Theft Task Force; Newark Suspicious Activity Report (SAR) Review Task Force; El Dorado Task Force - New York/New Jersey High Intensity Drug Trafficking Area; South Jersey Bankers Association; New York External Fraud Group; Philadelphia Financial Exploitation Prevention Task Force; Eastern District of Pennsylvania Money Laundering Working Group; New Jersey Security Association; Bergen County New Jersey Financial Crimes Association; Long Island Fraud and Forgery Association; Connecticut USAO Bank Secrecy Act Working Group; Connecticut U.S. Secret Service Financial Crimes Task Force; South Jersey SAR Task Force; Pennsylvania Electronic Crimes Task Force; NJ COVID-19 Fraud Task Force; Newark HSI Financial Fraud Working Group; Northern District of New York PPP Fraud Working Group.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force; Northern District of Georgia Mortgage Fraud Task Force; Eastern District of North Carolina Bank Fraud Task Force; Northern District of Alabama Financial Fraud Working Group; Northern District of Georgia SAR Review Team; Middle District of Georgia SAR Review Team; South Carolina Financial Fraud Task Force; 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; Southern 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; Madison, Wisconsin, SAR Review Team; Indiana Bank Fraud Working Group; Northern District of Indiana SAR Review Team; Southern 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.
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.
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	New York FBI Cyber Task Force; 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; 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 Financial Officer, Chief Operating Officer, and other senior FDIC officials through the IG's and senior OIG leadership's regularly scheduled meetings with them and through other forums.
- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
- 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.
- 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 releases, as appropriate.
- 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.
- Maintained congressional working relationships by communicating with various Committee staff on issues of interest to them; providing them our *Semiannual Report to the Congress*; notifying interested congressional parties regarding the OIG's completed audit and evaluation work; monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the FDIC's Office of Legislative Affairs on any Congressional correspondence pertaining to the OIG.

- Briefed committee staff on the House Financial Services Committee on several reports and work of the OIG: our Office's Top Management and Performance Challenges report; and findings related to the FDIC's Implementation of Enterprise Risk Management, Preventing and Addressing Sexual Harassment, and the FDIC's IT security (FISMA 2020). We also provided an overview of financial fraud cases related to the pandemic and the CARES Act, in particular, the Paycheck Protection Program.
- Briefed the House Financial Services Committee during a Roundtable on Cybersecurity. IG Lerner discussed our Office's priority focus on addressing cyber risks in the banking sector; ongoing work; our designated IT Audits and Cyber office, dedicated to information security; and our revamped, updated Electronic Crimes Unit, responsible for investigating sophisticated cybercrimes.
- 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, Council of Counsels to the IGs, and Federal Audit Executive Council; responding to multiple requests for information on IG community issues of common concern; and commenting on various legislative matters through CIGIE's Legislation Committee.
- 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.
- 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, 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.

Administering resources prudently, safely, securely, and efficiently.

- Formulated the OIG's budget for FY 2022 and proposed $46.5 million to conduct oversight of the FDIC. The budget maintains our existing baseline and staffing structure and proposes an increase in positions for a potential increase in criminal investigations and enhancement of the OIG's data analytics capabilities.
- Continued efforts by the OIG's Office of Information Technology to coordinate a strategic approach to facilitate the integration of technology in OIG processes. This office is working with the FDIC to integrate the OIG's new IT demand roadmap and strategic plan. The OI case management system, ECU Lab buildout, and OIG Dashboard project are its current priorities.
- Continued pursuing component office implementation plans designed to achieve the OIG's Strategic Goals, Guiding Principles, and Vision for 2021.
- Held mini-town hall meetings facilitated by the IG and Deputy IGs for each component office of the OIG to connect with staff through open dialogue and update staff regarding ongoing initiatives and future plans.
- Established a new Mid-Atlantic Region as part of the organization of our Office of Investigations for geographical coverage of cases in the District of Columbia, Maryland, Virginia, and West Virginia, and appointed a Special Agent in Charge for that region.
- Continued our work in developing a new case management system for our Office of Investigations.
- Pursued enhancements to the OIG's processes for records management and retention.
- Redesigned 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 the OIG, as a means to provide continuous updates on the pandemic and offer helpful information resources to OIG staff.
- Launched *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.
- Upgraded TeamMate with improved features, security, and stability for the OIG's audit and evaluation-related work.
- 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. Took steps 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 that of Special Agent in Charge of the Mid-Atlantic Region, 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.
- Continued to closely monitor OIG spending, with attention to expenses involved in procuring equipment, software, and services to improve the OIG's IT environment, and to track recurring expenses incurred by each component Office in the OIG.
- 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.

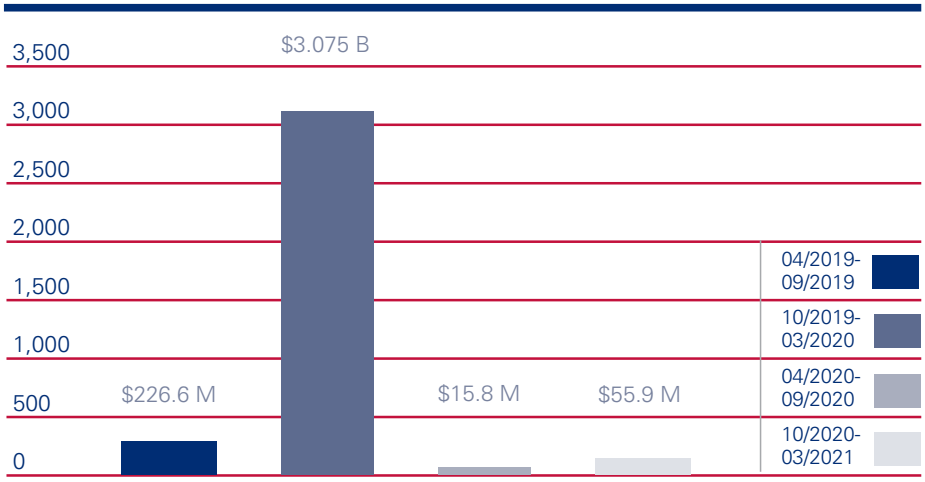
- Produced the OIG's *Vision 2021* video, with the theme "Strive and Thrive," to reinforce office-wide priority goals – Strategic implementation, Proactive Innovation, Professional Development, and Building Community in the OIG – and explained each component office's role in the teamwork needed to achieve those goals.
- 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 and began implementing that group's recommendations related to OIG rewards and recognition and work/life balance.
- 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 OIG newsletters and other announcements.
- Enrolled OIG staff in several different FDIC 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.
- Carried out monthly coordination meetings for audit, evaluation, and investigation leadership to better communicate, coordinate, and maximize the effectiveness of ongoing work.
- Acknowledged individual and group accomplishments through an ongoing awards and recognition program and recognized staff across all component offices for 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.
- 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 welcoming members of the OIG staff to attend D&I meetings, bi-monthly D&I Working Group updates in our Office newsletters, training on Diversity and Inclusion, and special acknowledgments of Black History Month and Women's History Month.
- Recognized OIG Veterans for their service to our Nation through an initiative sponsored by our Workforce Council.

- Shared information from our Engagement and Learning Officer throughout the OIG to promote employee engagement, career development, and a positive workplace culture.
- Participated on the Council of the Inspectors General on Integrity and Efficiency's Diversity, Equity, and Inclusion Work Group, for which the IG serves as Vice Chair.
- Hosted the Small Business Administration Inspector General for our Black History Month event, which included a panel discussion on Historically Black Colleges and Universities led by members of the OIG who attended these academic institutions.
- Took a leadership role in the CIGFO joint working group on Crisis Readiness. The OIG's Assistant IG for Program Audits and Evaluations is co-leading the project 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	
April 2019 – September 2019	24
October 2019 – March 2020	37
April 2020 – September 2020	44
October 2020 – March 2021	56

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.	36
Section 5(a)(1): Significant problems, abuses, and deficiencies.	4-14
Section 5(a)(2): Recommendations with respect to significant problems, abuses, and deficiencies.	4-14
Section 5(a)(3): Significant recommendations described in previous semiannual reports on which corrective action has not been completed.	37
Section 5(a)(4): Matters referred to prosecutive authorities.	47
Section 5(a)(5): Summary of each report made to the head of the establishment regarding information or assistance refused or not provided.	46
Section 5(a)(6): Listing of audit, inspection, and evaluation reports by subject matter with monetary benefits.	43
Section 5(a)(7): Summary of particularly significant reports.	4-14
Section 5(a)(8): Statistical table showing the total number of audit, inspection, and evaluation reports and the total dollar value of questioned costs.	44
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.	45
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	46
• no establishment comment was received within 60 days of providing the report to management	46
• there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.	38-42

Reporting Requirements (continued)	Page
Section 5(a)(11): Significant revised management decisions during the current reporting period.	46
Section 5(a)(12): Significant management decisions with which the OIG disagreed.	46
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.	49-50
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.	47
Section 5(a)(18): A description of metrics used for Section 5(a)17 information.	47
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.	47
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.	47
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.	47
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.	47

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 (CIGIE) Legislation Committee. Much of the FDIC OIG's activity reviewing legislation and regulation occurs in connection with that Committee.

In January 2021, CIGIE provided a letter outlining Legislative Priorities for the 117th Congress. CIGIE welcomes the opportunity to engage on legislation related to these following priorities:

- Enhancing the Institutional Independence of OIGs,
- Prohibiting the Use of Appropriated Funds to Deny IG Access,
- Testimonial Subpoena Authority,
- Improving CIGIE Transparency and Accountability Through a Single Appropriation,
- Providing Continuous Oversight During a Lapse in Appropriations,
- Reforming the Program Fraud Civil Remedies Act, and
- Reforming OIG Semiannual Reports.

CIGIE also identified recommended reforms that, although not among the highest priorities noted above, are worthy of consideration for improving government oversight:

- Protecting Cybersecurity Vulnerability Information,
- Statutory Exclusion for Felony Fraud Convicts to Protect Federal Funds, and
- Enhancing CIGIE's Role in Recommending IG Candidates.

The FDIC OIG supports CIGIE's identification of these legislative priorities and reforms intended to strengthen oversight of Federal programs or resolve certain challenges that IGs face under current law.

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 Control 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 two 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		
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.
	4*	In April 2019, the FDIC began executing a Privacy Continuous Monitoring program that aligns with OMB Circular A-130 and ensures privacy controls are regularly assessed for effectiveness. The FDIC plans to implement the Privacy Continuous Monitoring program for all information systems containing personally identifiable information over a 3-year period, with priority for new and changing authorizations over the next year.
EVAL-20-004 **The FDIC's Readiness for Crises** April 7, 2020	**3***	The FDIC will develop a crisis readiness procedures document that expands on the crisis readiness policy. The procedures will discuss the FDIC's methods of response, communicate roles and responsibilities, define general expectations for readiness plan content and testing, and raise FDIC employee awareness of crisis planning and response processes.

*Implementation scheduled for a future date.

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods

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

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-20-003 **The FDIC's Privacy Program** December 18, 2019	The significant amount of personally identifiable information (PII) 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	6	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	2	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-20-003 **Cost Benefit Analysis Process for Rulemaking** February 4, 2020	The FDIC OIG conducted an evaluation of the FDIC's Cost Benefit Analysis Process for Rulemaking. Through the Banking Act of 1933, Congress provided the FDIC with the authority to promulgate rules to fulfill the goals and objectives of the Agency. A cost benefit analysis informs the agency and the public whether the benefits of a rule are likely to justify the costs, or determines which of various possible alternatives is most cost effective. Our evaluation objective was to determine if the FDIC's cost benefit analysis process for rules was consistent with best practices. We found that the FDIC's cost benefit analysis process was not consistent with widely recognized best practices identified by the OIG. Specifically, we found that the FDIC had not established and documented a process to determine when and how to perform cost benefit analyses. We also found that the FDIC did not leverage the expertise of its Regulatory Analysis Section economists during initial rule development; did not require the Chief Economist to review and concur on the cost benefit analyses performed, which is an important quality control; was not always transparent in its disclosure of cost benefit analyses to the public; and did not perform cost benefit analyses after final rule issuance. The report contained five recommendations to improve the FDIC's cost benefit analysis process.	5	5	NA
EVAL-20-004 **The FDIC's Readiness for Crises** April 7, 2020	The FDIC OIG conducted an evaluation of the FDIC's Readiness for Crises. We initiated this evaluation in 2018, and it covered the FDIC's readiness planning and preparedness activities up to early 2019. Our work was not conducted in response to the current pandemic situation, nor is 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 made 11 recommendations to improve the FDIC's crisis readiness planning.	11	11	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-20-005 **The FDIC's Implementation of Enterprise Risk Management** July 8, 2020	Enterprise Risk Management (ERM) is an agency-wide approach to addressing the full spectrum of internal and external risks facing an agency. The FDIC Board of Directors (Board) designated the Operating Committee as the "focal point" for the coordination of risk management at the FDIC. The FDIC further designated the Operating Committee as the FDIC's Risk Management Council and the oversight body for ERM. We conducted an evaluation to assess the FDIC's implementation of ERM against relevant criteria and best practices. We assessed the FDIC against those best practices that, in our professional judgment, aligned with the structure of the Agency and the FDIC's decision to use the Operating Committee as its Risk Management Council. We found that the FDIC needed to establish a clear governance structure, and clearly define authorities, roles, and responsibilities related to ERM. We also found that the FDIC had not clearly defined the roles, responsibilities, and processes of other committees and groups involved in ERM. Our report contained eight recommendations to strengthen the FDIC's implementation of ERM.	8	2	NA
EVAL-20-006 **Preventing and Addressing Sexual Harassment** July 10, 2020	Sexual harassment in an organization can have profound effects and serious consequences for the harassed individual, fellow colleagues, and the agency as a whole. In some situations, a harassed individual may risk losing her/his job or the chance for a promotion, and it may lead the employee to suffer emotional and physical consequences. It may lead to a hostile work environment, which can reduce productivity and morale at an organization, harm the agency's reputation and credibility, and expose the enterprise to litigation expenses and monetary judgments. Therefore, an effective sexual harassment prevention program can help to protect employees and the agency from such harm and costs. We conducted an evaluation to determine whether the FDIC had established an adequate sexual harassment prevention program, including policies, procedures, and training to facilitate the reporting of sexual harassment allegations and address reported allegations in a prompt and effective manner. We found that the FDIC had not established an adequate sexual harassment prevention program and should improve its policies, procedures, and training to facilitate the reporting of sexual harassment allegations and address reported allegations in a prompt and effective manner. Our report contained 15 recommendations to improve the FDIC's activities to prevent and address sexual harassment.	15	13	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 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. Our report contained eight recommendations to improve examiner guidance and training.	8	8	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-21-001 October 27, 2020	*The FDIC's Information Security Program–2020*			
AUD-21-003 March 29, 2021	*Security of Critical Building Services at FDIC-owned Facilities*			
Resource Management				
AUD-21-002 December 21, 2020	*Governance of the FDIC's Mobile Device Management Solution*			$361,533
EVAL-21-001 January 19, 2021	*The FDIC's Personnel Security and Suitability Program*			
EVAL-21-002 March 31, 2021	*Critical Functions in FDIC Contracts*			
Totals for the Period		**$0**	**$0**	**$361,533**

Other products issued – Failed Bank Reviews:

- *The First State Bank, Barboursville, West Virginia* (FBR-21-001)
  November 24, 2020
- *First City Bank of Florida, Fort Walton Beach, Florida* (FBR-21-002)
  March 15, 2021
- *Almena State Bank, Almena, Kansas* (FBR-21-003)
  March 26, 2021

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.	1	$361,533
Subtotals of A & B	**1**	**$361,533**
C. For which a management decision was made during the reporting period.	1	$361,533
(i) dollar value of recommendations that were agreed to by management.	1	$361,533
- based on proposed management action.	1	$ 361,533
- based on proposed legislative action.	0	$0
(ii) dollar value of recommendations that were not agreed to by management.	0	$0
D. For which no management decision has been made by the end of the reporting period.	0	$0
Reports for which no management decision was made within 6 months of issuance.	0	$0

Table VI: Status of OIG Recommendations Without Management Decisions
During this reporting period, there were two recommendations more than 6 months old without management decisions. In our report, *The FDIC's Implementation of Enterprise Risk Management* (EVAL-20-005), dated July 8, 2020, we found that:

- The Board was not involved in endorsing the risk appetite statement as suggested by the Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management Framework 2017;
- The FDIC did not provide the same level of information regarding enterprise risk management (ERM) to each Board member; and
- Board members had different perspectives on the role of the Board in implementing ERM.

Therefore, we recommended that the FDIC: (1) define the roles and responsibilities of the Board with respect to ERM, including its role in endorsing the risk appetite statement; and (2) develop and implement ERM communication protocols to the Board.

Upon issuance of our report, we considered these two recommendations to be unresolved and agreed to work with the FDIC to seek resolution during the evaluation follow-up process.

On January 21, 2021, the FDIC submitted a Corrective Action Closure request asking for the recommendations to be closed. However, we determined that the FDIC had not taken corrective actions sufficient to resolve the intent of our recommendations. Therefore, the two recommendations remained unresolved at the close of the reporting period for this Semiannual Report (March 31, 2021).

After the close of the reporting period (in April 2021), the FDIC proposed additional corrective actions to address the recommendations, and we consider the proposed actions to be management decisions sufficient to resolve the recommendations. The recommendations, however, remain unimplemented until we receive a written description of the actual corrective actions from the FDIC, and at such time, we will review the materials and determine if such actions are sufficient to close 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	48
Number of Persons Referred to the Department of Justice for Criminal Prosecution	168
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	0
Number of Indictments and Criminal Informations	82

Note: Description of the metrics used for the above information: Reports issued reflects case closing memorandums issued to FDIC management. With respect to the 168 referrals to DOJ, the total represents 138 individuals, 28 business entities, and 2 cases where the subject is unknown at present. Total does not include one referral to DOJ on a civil matter. Our total indictments and criminal informations includes indictments, informations, and superseding indictments, as applicable.

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

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

Table XIII: Instances of Whistleblower Retaliation

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

Table XIV: Instances of Agency Interference with OIG Independence

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

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

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

Appendix 2

Information on Failure Review Activity

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

FDIC OIG Review Activity for the Period October 1, 2020 through March 31, 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.

As discussed earlier in this report, the OIG issued the results of three Failed Bank Reviews during the reporting period:

- *The First State Bank, Barboursville, West Virginia* (FBR-21-001)
  November 24, 2020
- *First City Bank of Florida, Fort Walton Beach, Florida* (FBR-21-002)
  March 15, 2021
- *Almena State Bank, Almena, Kansas* (FBR-21-003)
  March 26, 2021

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

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

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

The following staff members retired from the FDIC OIG during the reporting period. We appreciate their many contributions to the Office over the years and wish them well in future endeavors. Congratulations to all.

Janice Baltimore
Office of Program Audits and Evaluations

Wade Boone
Office of Program Audits and Evaluations

Rhonda Bunte
Office of Program Audits and Evaluations

DeGloria Hallman
Office of Program Audits and Evaluations

Laurie Younger
Office of Investigations

Kelvin Zwiefelhofer
Office of Investigations

DESIGN: FDIC/DOA/CSB/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.

www.pandemicoversight.gov

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 and an on-line form 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