FDIC Office of Inspector General

Semiannual Report to the Congress

April 1, 2020 – September 30, 2020

Integrity • Independence • Accuracy • Fairness • Objectivity • Accountability • Transparency • Professionalism • Judgment

Under the Inspector General Act of 1978, as amended, the Federal Deposit Insurance Corporation Office of Inspector General (FDIC OIG) 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 5,580 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured more than $8.8 trillion in deposits in 5,066 institutions, of which the FDIC supervised 3,264, not including U.S. insured branches of foreign banks. The Deposit Insurance Fund balance totaled $114.7 billion as of June 30, 2020. Active receiverships as of September 30, 2020 totaled 238, with assets in liquidation of about $370 million.

Office of Inspector General

Semiannual Report to the Congress

April 1, 2020 – September 30, 2020

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 April 1, to September 30, 2020. I am proud of the hard work and dedication of the women and men of the OIG, particularly during a time when our Nation is facing the unique challenges of the current pandemic and an altered workplace. We remain steadfast in carrying out the mission of the OIG, and our results attest to the OIG's unwavering commitment to public service.

Our Evaluation and Audit reports issued during this reporting period will have a meaningful impact and lasting effects on critical FDIC programs and operations. Our work covered the FDIC's Readiness for Crises; its Implementation of Enterprise Risk Management; its Regional Automated Document Distribution and Imaging System; the causes of the failure of Enloe State Bank and the FDIC's supervision of this bank; and Preventing and Addressing Sexual Harassment. We made a total of 44 recommendations for improvements at the Agency and in its operations.

In addition, our OIG Special Agents have worked closely with law enforcement partners to investigate criminal matters involving complex financial fraud schemes. In one case, for example, a former banker and mortgage broker were convicted on multiple counts, including conspiracy, bank fraud, false statements on credit applications, wire fraud, and mail fraud. They were sentenced to 84 months and 132 months in prison, respectively, and ordered to pay restitution of $6.8 million, joint and several. In another case, three separate defendants pleaded guilty to working with bank executives to defraud First NBC Bank of more than $123 million.

Importantly, over the past 6 months, our Office has been actively engaged as a member of the Pandemic Response Accountability Committee, established by the Coronavirus Aid, Relief, and Economic Security Act (CARES Act). This Committee is charged with coordinating efforts of Federal Inspectors General (IG) to oversee $2.6 trillion in Federal emergency relief. We have worked with our colleagues in the IG community to conduct objective and independent oversight, and to detect fraud, waste, and abuse.

In connection with our response to the pandemic, in September, we participated in a press conference at the Department of Justice announcing that over 50 individuals who allegedly committed fraud to obtain money from the Paycheck Protection Program (PPP) had been criminally charged. These cases involved attempts to steal over $175 million from the PPP, and because of our investigative work with our partners, the Government has recovered or frozen more than $30 million and the work continues.

In closing, I want to acknowledge the OIG teams and individuals who received Awards for Excellence from the Council of the Inspectors General on Integrity and Efficiency (CIGIE) for outstanding audit and investigative work at the IG community's recent award ceremony. Also deserving of recognition is our Assistant Inspector General for Investigations, Matthew Alessandrino, who was honored as a recipient of American University's Roger W. Jones Award for his career achievements.

We appreciate 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 and joining with others to navigate through these challenging and unprecedented times.

Jay N. Lerner
Inspector General
October 30, 2020

Table of Contents

Acronyms and Abbreviations

CARES Act	Coronavirus Aid, Relief, and Economic Security Act
C&C	Cotton & Company LLP
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
COVID-19	Coronavirus Disease 2019
D&I	Diversity and Inclusiveness
DIF	Deposit Insurance Fund
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOJ	Department of Justice
ECU	Electronic Crimes Unit
ERM	Enterprise Risk Management
ESB	Enloe State Bank
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FHFA	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
FRB	Federal Reserve Board
FSOC	Financial Stability Oversight Council
GAO	Government Accountability Office
HUD	Department of Housing and Urban Development
IG	Inspector General
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
OC	Operating Committee
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
RADD	Regional Automated Document Distribution and Imaging System
RMC	Risk Management Council
SAR	Suspicious Activity Report
SBA	Small Business Administration
USAO	United States Attorney's Office

Introduction and Overall Results

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

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

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

Overall Results (April 1, 2020 – September 30, 2020)	
Audit, Evaluation, and Other Products Issued	**7**
Nonmonetary Recommendations	**44**
Investigations Opened	**94**
Investigations Closed	**26**
Judicial Actions:	
Indictments/Informations	77
Convictions	35
Arrests	42
OIG Investigations Resulted in:	
Fines of	$ 298,100
Restitution of	$ 15,345,554*
Asset Forfeitures of	$ 146,035
Total	**$ 15,789,689**
Referrals to the Department of Justice (U.S. Attorney)	**209**
Proposed Regulations and Legislation Reviewed	**2**
Responses to Requests Under the Freedom of Information/Privacy Act	**8**

* Restitution this period includes a $6,804,260 that was ordered joint and several with other individuals sentenced during this period, and $1,059,226 that was ordered joint and several with an individual yet to be sentenced.

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 the FDIC's readiness for crises, enterprise risk management (ERM), efforts to prevent and address sexual harassment, and security controls in the FDIC's official electronic system for supervisory business records. 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. We are reporting the results of our In-Depth Review of one such failure not meeting the threshold but warranting further review in this report, that of Enloe State Bank, Cooper, Texas. In all, audit and evaluation reports issued during the period resulted in 44 recommendations to management.

We also issued the results of our failed bank reviews of two other institutions: Louisa Community Bank, Louisa, Kentucky, and Ericson State Bank, Ericson, Nebraska. These failed bank reviews are discussed below, and we determined that neither failure warrants additional review. We also learned of an additional failure causing a loss to the DIF of $46.8 million, an amount less than the material loss threshold: The First State Bank, Barboursville, West Virginia, and a failed bank review of that institution was in process at the end of the reporting period.

Also of note during the reporting period, the FDIC OIG joined other Members of the Council of Inspectors General on Financial Oversight in issuing an annual report that captured the financial oversight work of Council Members during the past year.

Results of these audits, evaluations, and other reviews are summarized in the following sections.

Audits and Evaluations

The FDIC's Readiness for Crises

We evaluated 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.

The FDIC's mission is to maintain stability and public confidence in the Nation's banking system by insuring deposits, examining and supervising financial institutions for safety and soundness and consumer protection, making large and complex financial institutions resolvable, and managing receiverships. To achieve its mission, the FDIC must be prepared for a broad range of crises that could impact the banking system.

The OIG 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 found that the FDIC should fully establish these seven elements of a readiness framework to address crises that could impact insured depository institutions. In summary, we found that the FDIC:

- Did not have a documented Agency policy and did not have documented procedures to provide for a consistent crisis readiness planning process;
- Should develop an Agency-wide all-hazards readiness plan as well as Agency-wide hazard-specific readiness plans, as needed;
- Did not train personnel to understand the content of crisis readiness plans;
- Should document the important results of all readiness plan exercises;
- Did not have a documented process to monitor implementation of lessons learned;
- Should establish a central repository of plans to facilitate periodic maintenance; and
- Should regularly assess and report on Agency-wide progress on crisis readiness plans and activities to the FDIC Chairman and senior management.

We made 11 recommendations to improve the FDIC's crisis readiness planning. Management concurred with seven recommendations and partially concurred with four recommendations.

The FDIC's Implementation of 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 FDIC Operating Committee (OC) as the "focal point" for the coordination of risk management at the FDIC. The FDIC further designated the OC as the FDIC's Risk Management Council (RMC) and the oversight body for ERM.

We found that the FDIC needed to establish a clear governance structure, and clearly define authorities, roles, and responsibilities related to ERM. Importantly, the FDIC did not clearly articulate in its policies and procedures how the OC, as the FDIC's designated RMC, performed its responsibilities. In particular, we noted that the FDIC should define the Operating Committee's role with respect to its oversight of the establishment of the FDIC's Risk Profile; oversight of the assessment of risks; oversight of the development of risk responses; and the final determinations of the approaches and actions to address the risks included in the FDIC's Risk Profile.

We also found that the FDIC had not clearly defined the roles, responsibilities, and processes of other committees and groups involved in ERM. The FDIC did not:

- Ensure that the Board endorsed the Risk Appetite statement prior to its issuance;
- Ensure effective communications to the Board relating to ERM;
- Ensure that the Board understood its role with respect to ERM at the FDIC;
- Develop procedures to specify how risk committee activities were to be accomplished and how they interfaced with other ERM processes;
- Require documentation of meetings of the various risk committees; and
- Update and memorialize ERM processes for the Risk Management and Internal Controls Branch.

Without a clear governance structure over ERM, the FDIC cannot ensure that ERM will fully mature and be integrated into the Agency and its culture. Integrating ERM leads to improved decision-making and enhanced performance.

We made eight recommendations to strengthen the FDIC's implementation of ERM. Management concurred with five recommendations and non-concurred with the remaining three recommendations.

Preventing and Addressing Sexual Harassment

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 also 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. An effective sexual harassment prevention program can help to protect employees and the agency from such harm and costs.

Our evaluation objective was 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.

FDIC leadership demonstrated commitment to preventing sexual harassment through global notices to FDIC staff and the agency's Diversity and Inclusion Strategic Plan. However, the FDIC had not established a strategy to acknowledge employees, supervisors, and managers, for creating and maintaining a culture in which harassment is not tolerated.

We also found that the FDIC should improve its policies, procedures, and training to ensure that:

- Employees and supervisors know how to identify and report sexual harassment, and ensure that reporting does not result in fear of retaliation;
- Supervisors know how to promptly and effectively address sexual harassment misconduct; and
- Discipline is proportionate to the level of misconduct.

FDIC policies did not clearly define sexual harassment, include all avenues of reporting allegations of sexual harassment, or clearly describe the roles and responsibilities for preventing sexual harassment and monitoring allegations of such misconduct. Although the FDIC had developed and implemented adequate procedures to address unlawful sexual harassment complaints, we found that it had not developed procedures for addressing sexual harassment misconduct allegations. These procedures include: (1) tracking; (2) investigating; (3) reporting; and (4) resolving misconduct allegations. Further, the FDIC had not developed and implemented adequate procedures for applying disciplinary action in response to substantiated harassment allegations, including sexual harassment allegations. In addition, the FDIC should improve its training for employees and supervisors on how to identify conduct that constitutes "sexual harassment," report allegations of sexual harassment, and address allegations.

Finally, we found that the FDIC did not have agency-specific program accountability or oversight practices, including performance goals, metrics, or surveys to determine its effectiveness in preventing and addressing sexual harassment allegations.

Our report contained 15 recommendations to improve the FDIC's activities to prevent and address sexual harassment. These recommendations addressed four broad areas: improving policies and procedures relating to FDIC actions in response to sexual harassment misconduct allegations; promoting a culture in which sexual harassment is not tolerated; ensuring consistent and proportionate discipline; and enhancing training for employees and supervisors. The FDIC concurred with 12 of the 15 recommendations and provided alternative actions to address the remaining 3 recommendations.

Security Controls Over the Federal Deposit Insurance Corporation's Regional Automated Document Distribution and Imaging System

The FDIC relies heavily on information systems to carry out its mission. As of February 11, 2020, the FDIC maintained 274 information systems, nearly half of which contained sensitive information and Personally Identifiable Information (PII). One of these systems is the FDIC's Regional Automated Document Distribution and Imaging System (RADD).

RADD serves as the official recordkeeping and electronic filing system for the FDIC's supervisory business records. RADD contains over 5 million electronic supervisory business records. The large amount of sensitive information in RADD underscores the need for effective security controls to mitigate security incidents.

Our audit objective was to assess the effectiveness of selected security controls for protecting the confidentiality, integrity, and availability of information in RADD. We assessed security controls in eight areas covered in National Institute of Standards and Technology (NIST) guidance: Plans of Action and Milestones, Configuration Management, Access Management, Removable Media, Encryption, Audit Logging, Security Authorization and Continuous Monitoring, and Contingency Planning.

We found that the FDIC's controls and practices were effective in five of the eight security control areas assessed. However, controls and practices in the remaining three security control areas were not fully effective – because either they did not comply with FDIC policy requirements or they were not implemented in a manner consistent with relevant NIST guidance. Specifically, the FDIC did not use a secure encryption solution to protect RADD data; did not implement a control to prevent unauthorized access to certain sensitive documents in RADD; and did not adequately document roles, responsibilities, and procedures for reviewing and maintaining RADD audit logs.

The report contained two recommendations to address the access control and audit logging weaknesses identified during the audit. The FDIC had already completed corrective actions to address them at the time we issued our final report.

Reports of Failed Banks

In-Depth Review of the Failure of Enloe State Bank, Cooper, Texas

On May 31, 2019, the Texas Department of Banking (TDB) closed Enloe State Bank (ESB), and the FDIC was appointed as receiver for the Bank. As of July 31, 2020, the estimated loss to the Deposit Insurance Fund resulting from ESB's failure was approximately $21 million. Our review analyzed the causes of the Bank's failure and evaluated the FDIC's supervision of the Bank.

Causes of Failure: 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. ESB's President was a dominant official with significant control over Bank operations and limited oversight by the Bank's Board of Directors. The Bank President used her role as primary lender, with inadequately controlled systems access, to originate millions of dollars in fraudulent loans. She hid these loans from the Board and regulators with assistance from others. The losses on the fraudulent loans severely diminished the Bank's earnings and depleted capital to the point from which the Bank could not recover.

The FDIC's Supervision of ESB: The FDIC and the TDB provided ESB with supervisory recommendations and actions that addressed issues related to the eventual causes of the Bank's failure. However, these recommendations and actions did not persuade the Bank's Board and management to effectively resolve the identified weaknesses. We found that the FDIC did not:

- Identify the existence and impact of a dominant official in a timely manner;
- Consistently identify and follow up on weaknesses in the Bank's audit program;
- Conduct additional testing to address unusual loan-related activity, which may have helped identify the fraudulent activity sooner than 2019; and
- Perform additional procedures to determine the likelihood of fraud once the examination in 2018 identified a dominant official, unsatisfactory Board oversight, and inadequate internal controls and audits.

In the case of ESB, examiners did not identify that fraud might be occurring at the institution until 2019, which was too late to save the Bank.

We made eight recommendations for the FDIC to improve examiner guidance and training in such areas as identifying dominant officials; understanding the independence and qualifications of internal auditors; recognizing the importance of adequate external financial audit coverage; monitoring and following up on State-issued Matters Requiring Board Attention; ensuring that system user access controls are adequately tested; conducting additional procedures related to loan activity and the likelihood of fraud; and considering issues holistically to facilitate fraud detection.

The FDIC concurred with three recommendations in our report and stated that it "partially agreed" with five recommendations.

Failed Bank Review of Louisa Community Bank, Louisa, Kentucky

On October 25, 2019, the Kentucky Department of Financial Institutions (KDFI) closed Louisa Community Bank, and the FDIC was appointed receiver. The Bank was a locally owned, state-chartered nonmember bank located in Louisa, Kentucky. The institution was established and became insured on August 7, 2006. The Bank had no holding company. According to the FDIC's Division of Finance, the estimated loss to the DIF was $4.5 million or 17 percent of the Bank's $27.4 million in total assets. According to KDFI documentation, the Bank had "permitted capital to become impaired to a level which d[id] not permit the Bank to operate in a safe and sound manner" and, therefore, the KDFI took possession of and closed the Bank.

Based on the review of key FDIC documents, the Bank's failure resulted from an "ineffective and dysfunctional" Board of Directors (Board) and executive management that led to poor risk management practices, operational deficiencies, weak internal controls, and inaccurate accounting and reporting that adversely impacted every facet of the Bank.

The Board and executive management also failed to maintain adequate and qualified staffing in key management positions, and were unable to address the many financial, managerial, operational, and regulatory issues that examiners started to identify in 2014. The Bank became unprofitable in 2015, followed by material operational losses and elevated credit losses that eroded capital levels and stressed liquidity.

We determined that proceeding with an In-Depth Review of the loss was not warranted, because we did not identify unusual circumstances in connection with the Bank's failure.

Failed Bank Review of Ericson State Bank, Ericson, Nebraska

On February 14, 2020, the Nebraska Department of Banking and Finance (NDBF) closed Ericson State Bank, and the FDIC was appointed receiver. The Bank was a state-chartered nonmember Bank located in Ericson, Nebraska. Wheeler County Bancshares, Inc., a one-bank holding company, owned 1,999 shares or 99.95 percent of the institution's outstanding common stock. According to the FDIC's Division of Finance, the estimated loss to the DIF was $14.1 million or 14 percent of the Bank's $100.9 million in total assets. According to NDBF documentation, the NDBF took possession and closed the Bank because the Bank was insolvent, operated in an unsafe and unauthorized manner, and lacked prospects for a capital injection.

We determined that unusual circumstances existed related to the escalation of the Bank President's actions in extending funds to related entities owned by his son without proper documentation and support and knowingly advancing funds beyond the Nebraska Legal Lending Limit. According to the FDIC, this related-entity lending did not pose substantial risk to the Bank until after the FDIC's 2016 examination. During the next FDIC examination, in 2019, the FDIC identified the risk, and examiners concluded that Board and Management performance were "critically deficient" and downgraded the Bank's composite rating from a "2" to a "4."

Given that the FDIC identified the risk and took action to address it in 2019, the unusual circumstances did not warrant an OIG In-Depth Review 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, the FDIC's Personnel Suitability and Security Program, allocation and retention of safety and soundness examination staff, and security of the FDIC's mobile devices, among others. These ongoing reviews are listed on our website and, when completed, their results will be presented in an upcoming semiannual report.

CIGFO 2020 Annual Report and Other Activities

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) established the Council of Inspectors General on Financial Oversight (CIGFO) to oversee the Financial Stability Oversight Council (FSOC) and suggest measures to improve financial oversight. FSOC has a statutory mandate that created collective accountability for identifying risks and responding to emerging threats to U.S. financial stability.

The CIGFO members meet quarterly to discuss the ongoing work of each Inspector General who is a member of the Council, with a focus on concerns that may apply to the broader financial sector, and to exchange ideas about ways to improve financial oversight. In July 2020, CIGFO published its annual report, which includes individual discussions of the work of the member IGs during the previous year. That report is available on the Treasury website indicated below.

Of note, during the course of the year, CIGFO continued to monitor coordination efforts among and between FSOC members. To assist in that regard, CIGFO members were briefed on and/or discussed the following:

- National Cyber Investigative Joint Task Force – structure and core services of its Virtual Currency Team and an overview of what virtual currency is and its key attributes.
- Federal Deposit Insurance Corporation Office of Inspector General – overview of fraud schemes associated with cybercrimes and strategies to prevent them.
- Intelligence Community Inspector General – results of an audit of the appropriate federal entities' implementation of the Cybersecurity Information Sharing Act of 2015.
- FSOC's interpretative guidance on nonbank financial designations.
- Events related to whistleblower rights and protections.
- Components of the economic stimulus included in the Coronavirus Aid, Relief, and Economic Security Act and the oversight role of the IG community.

The FDIC OIG looks forward to continued collaboration with our CIGFO partners as we address the challenges of the upcoming year.

CIGFO Members

- Department of the Treasury (Chair)
- Federal Deposit Insurance Corporation
- Federal Housing Finance Agency (FHFA)
- Commodity Futures Trading Commission
- Department of Housing and Urban Development (HUD)
- Board of Governors of the Federal Reserve System (FRB) and the Bureau of Consumer Financial Protection
- National Credit Union Administration
- Securities and Exchange Commission
- Special Inspector General for the Troubled Asset Relief Program

Additional information on CIGFO is available at: **treasury.gov/about/organizational-structure/ig/Pages/Council-of-Inspectors-General-on-Financial-Oversight.aspx**

FDIC OIG Participation on the Pandemic Response Accountability Committee

The Coronavirus Aid, Relief, and Economic Security (CARES) Act and other related legislation provide approximately $2.6 trillion in federal spending to address the public health and economic crises resulting from the Coronavirus Disease 2019 (COVID-19) pandemic. 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. The Committee is responsible for, among other activities:

- Developing a strategic plan to ensure coordinated, efficient, and effective comprehensive oversight by the Committee and Inspectors General over all aspects of covered funds and the Coronavirus response;
- Reviewing the economy, efficiency, and effectiveness in the administration of, and the detection of fraud, waste, abuse, and mismanagement in, Coronavirus response programs and operations;
- Serving as a liaison to the Director of the Office of Management and Budget, the Secretary of the Treasury, and other officials responsible for implementing the Coronavirus response; and
- Expeditiously reporting to the Attorney General any instance in which the Committee has reasonable grounds to believe there has been a violation of Federal criminal law.

The PRAC has been meeting regularly as it continues its work in response to COVID-19. In June 2020, the PRAC released its first report, *Top Challenges Facing Federal Agencies: COVID-19 Emergency Relief and Response Efforts*, where 37 Inspectors General, including the FDIC OIG, reported on the top pandemic-related challenges in their agencies. The report identified common areas of concern among agencies of different sizes and with different missions:

- Financial management of CARES Act and other funds;
- Grant and guaranteed loan management;
- Information technology security and management; and
- Protecting health and safety.

The FDIC OIG identified three primary challenges facing the FDIC:

- Ensuring the FDIC's readiness for crises (including modeling potential effects on financial institutions and conducting examinations remotely).
- Resolving financial institutions (including executing off-site bank resolutions and receiverships and resolving large, complex institutions pursuant to Dodd-Frank Act responsibilities).
- Guarding against financial fraud and cybercrimes at banks.

Our Office looks forward to continuing to work with the IG community to oversee the covered funds in the CARES Act and keep the public informed, as we continue to work on this important oversight effort.

For ongoing efforts of the Committee, consult the PRAC website, pandemicoversight.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.

DOJ Press Conference on Paycheck Protection Program (PPP) Fraud

On September 10, IG Jay Lerner represented the FDIC OIG in a Department of Justice press conference announcing that over 50 individuals who allegedly committed fraud to obtain money from the PPP had been criminally charged. The cases charged involved attempts to steal over $175 million from the PPP. Because of the work of our Office of Investigations in coordination with DOJ, the FBI, and other Offices of Inspector General and law enforcement partners, over $30 million has been recovered or frozen and more work is ongoing to seize additional funds and liquidate assets that were purchased with PPP funds.

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 (OI) has been monitoring developments in order to investigate 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.

OI has been working proactively with the other OIGs, including: the FRB, Treasury, Internal Revenue Service (IRS), HUD, Small Business Administration (SBA), and Office of

the Comptroller of the Currency (OCC), among others; USAOs; and other law enforcement agencies on cases involving frauds targeting the funds distributed through the CARES Act. During the reporting period, the FDIC OIG's efforts related to the Federal Government's COVID-19 pandemic response resulted in 38 indictments/criminal complaints, 29 arrests, and 2 convictions, often involving fraud in the 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.

Delta County Bank President Guilty of Bank Fraud and Arson Violations

On June 5, 2020, Anita Gail Moody, of Cooper, Texas, pleaded guilty to conspiracy to commit bank fraud and arson.

According to information presented at court, Moody was 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.

Moody agreed to a sentence of 84 months in Federal prison and will pay $11,136,241.82 in restitution.

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

Multiple Cash Flow Employees Plead Guilty for Role in Multimillion-Dollar Loan and Securities Fraud Scheme

On June 11, 2020, Edward Espinal, of Wayne, New Jersey, pleaded guilty to orchestrating a multimillion-dollar bank fraud and securities fraud scheme. The defendant pleaded guilty to an information charging him with one count of conspiracy to commit bank fraud and one count of securities fraud.

From March through December 2019, while serving as the Chief Executive Officer of Cash Flow, Espinal led and directed a bank fraud conspiracy designed to obtain millions of dollars in loans from banks on the basis of false representations.

Employees in the sales department at Cash Flow encouraged customers to sign up for various loan programs that Cash Flow provided and to enter into contracts with Cash Flow that would allow customers to obtain loans from banks. The Cash Flow contracts permitted customers to keep a portion of the loan proceeds, and customers agreed to provide the remaining percentage of the proceeds to Cash Flow. Cash Flow agreed to pay off the loans on behalf of its customers. Cash Flow then used false information and fraudulent documents to obtain loans for its customers for which they otherwise would not have qualified, and posed as the customers in communications with the banks.

From July 2016 through September 2019, Espinal obtained more than $5 million in investments from victim investors on the basis of false and fraudulent pretenses and representations.

Espinal made a number of misrepresentations to investors, while using the investor funds to pay returns to earlier investors; to pay for personal expenses for himself, his family, and another Cash Flow employee; to perpetuate the bank fraud scheme; and to market the bank fraud and investment scheme to future victims. He also falsely claimed that Cash Flow's purported real estate fund was "licensed" by the Securities and Exchange Commission (SEC). He guaranteed monthly returns on investment based on the purported proceeds from the sale of properties in Cash Flow's investment portfolio. In reality, Espinal did not sell Cash Flow properties, so no profits were derived from the sale of Cash Flow properties.

In addition to Espinal's guilty plea in this case, Jennie Frias, an employee at Cash Flow pleaded guilty in April of 2020 for her role in creating false documentation to make customers' loan applications appear more financially viable than they actually were. Another conspirator, Raymundo Torres, also pleaded guilty to charges relating to his role in the Cash Flow bank fraud conspiracy.

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

Former Bank Executive Sentenced for Using Bank Funds for Luxury Vacations and Other Personal Expenses

On July 8, 2020, Archie G. Overby, of Waupaca, Wisconsin, was sentenced following his guilty plea to misapplication of funds by a bank officer.

Overby was the President, Chief Operating Officer, and Chairman of the Board of First National Bank in Waupaca, Wisconsin. Pursuant to a plea agreement, Overby admitted that starting in 2010 and continuing through 2013, he caused the bank to pay for $1.6 million in travel, entertainment, and other personal expenses for himself, family members, friends, and associates, all of which had no legitimate banking purpose.

Pursuant to the plea agreement accepted by the Court, Senior United States District Court Judge William C. Griesbach did not impose a prison sentence. Instead, because of Overby's age (71) and documented and significant health issues, and the potential impact of COVID-19, Overby was ordered to pay $1.6 million in restitution and forfeit $146,023.35 to the United States.

Source: Request for assistance from Treasury OIG.
Responsible Agencies: FDIC OIG and Treasury OIG.
Prosecuted by the USAO, Eastern District of Wisconsin.

Boulder Man Pleads Guilty to Nearly $32 Million Bank Fraud Scheme

On July 31, 2020, Michael Scott Leslie, of Boulder, Colorado, pleaded guilty to federal bank fraud and aggravated identity theft charges for his role to defraud an FDIC-insured bank in Texas.

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 the FDIC-insured bank.

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 (MCM). Leslie never disclosed to the victim bank that he operated MCM and Snowberry, or the fact that sales to investor MCM, 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: Department of Justice.
Responsible Agencies: FDIC OIG, HUD OIG, and FBI.

Former Banker and Mortgage Broker Sent to Prison for Defrauding California Bank

On August 6, 2020, Carlos Wydler, and Leyla Wydler, both of Houston, Texas, were sentenced to prison following their convictions on multiple counts to include conspiracy, bank fraud, false statements on credit applications, wire fraud, and mail fraud.

Carlos Wydler was sentenced to 84 months in prison and was ordered to pay $6,804,260 in restitution to the victim bank and its insurer. Leyla Wydler was sentenced to 132 months and ordered to pay the $6.8 million in restitution joint and several with her stepson.

Leyla Wydler was the owner of several Houston-area businesses including Globan Mortgage Company, Casa Milagro, and First Milagro. In the spring of 2007, Carlos Wydler went to work at a California bank as a vice president in charge of the bank's credit card department. Shortly thereafter, the Wydlers developed a scheme in which Leyla Wydler would send credit card applications to the bank for Carlos Wydler to approve. He approved the applications for high credit lines and then, calling them "balance transfers," cash advanced the entire credit line to the borrower via wire or check with Leyla Wydler taking a fee from the borrowers' loan proceeds.

During trial, the evidence demonstrated that the Wydlers were also developing a real estate project in Houston at the time and used the "balance transfer" program to finance investors in their project. The jury heard that the bank did not know or approve of the fee-sharing or real estate financing arrangements.

For approximately a year, hundreds of loan applications were faxed or emailed from Leyla Wydler's business in Houston to Carlos Wydler at the bank in California. Many of these contained falsified income information and falsified supporting documents about borrowers' employment, income, and assets. Two eyewitnesses testified they saw Leyla Wydler routinely insert falsified income numbers, sometimes using white-out, on loan applications.

Leyla Wydler skimmed more than $1.4 million from loan proceeds, with Carlos Wydler approving approximately $600,000 more in unauthorized loans to family members. More than half of the Texas borrowers run through the Wydler-family business in Houston defaulted on their loans. The bank sustained a loss of more than $6 million.

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

Seventh Conspirator Pleads Guilty in Solar Ponzi and Securities Scheme

On July 28, 2020, Alan Hansen, of Vacaville, California, pleaded guilty to his participation in a massive fraud scheme through DC Solar, a solar energy company in Benicia formerly owned and operated by Jeff and Paulette Carpoff that defrauded investors of approximately $1 billion. Hansen was the seventh person to plead guilty since October 2019. The Carpoffs pleaded guilty to their roles in the fraud conspiracy and other charges in January 2020.

Between 2011 and 2018, DC Solar manufactured mobile solar generator units–solar generators that were mounted on trailers. The company touted the versatility and environmental sustainability of the mobile units and claimed that they were used to provide emergency power to cellphone towers and lighting at sporting and other events. The Carpoffs and their co-conspirators solicited investors by claiming that there were favorable federal tax benefits associated with investments in alternative energy. In reality, at least half of the approximately 17,000 solar generators claimed to have been manufactured by DC Solar did not exist, and DC Solar paid early investors with funds contributed by later investors.

Hansen was an employee of a telecom company with which DC Solar had done business. He accepted $1 million from co-conspirators at DC Solar to fraudulently sign a false contract that those co-conspirators later used to induce investments by victims. Hansen later joined DC Solar as an executive, where he and a co-conspirator agreed to share $20,000 to sign another, related false contract, using a fake name. That contract was also used to induce investments. Hansen was paid for signing the first false contract through a series of interstate wire transfers into an account he set up in the name of a consulting company. He knew the money he was paid came from payments by investors who had been deceived by DC Solar. Still, Hansen provided a co-conspirator with information to complete those wire transfers, intending to commit money laundering.

Investor losses of $1 billion resulted from investment transactions totaling about $2.5 billion.

Source: Based on information from the FBI and the SEC.
Responsible Agencies: FDIC OIG, FBI, and IRS-Criminal Investigation.
Prosecuted by the USAO, Eastern District of California, Sacramento.

Arkansas Project Manager Pleads Guilty to Bank Fraud and False Statements in Connection with COVID-Relief Fraud

On August 6, 2020, Benjamin Hayford, of Centerton, Arkansas, pleaded guilty to one count of bank fraud and four counts of false statements to a financial institution for his role in filing fraudulent bank loan applications seeking more than $8 million in forgivable PPP loans guaranteed by the Small Business Administration under the CARES Act.

As part of his guilty plea, Hayford admitted that he sought millions of dollars in forgivable PPP loans from multiple banks by claiming fictitious payroll expenses. To support his applications, Hayford provided lenders with fraudulent payroll documentation purporting to establish payroll expenses that were, in fact, non-existent. In addition, Hayford admitted to making false representations to a financial institution concerning the date that a Limited Liability Partnership for which he applied for relief was established.

Source: Department of Justice.
Responsible Agencies: FDIC OIG, FHFA OIG, and SBA OIG.

Former Bank Vice President Sentenced in Federal Court After Conspiring to Lie to His Employer

On August 27, 2020, Dan Raduns, 66, from Dubuque, Iowa, was sentenced to 3 years of probation for his guilty plea to one count of conspiracy to make a false statement to a financial institution.

Evidence and information disclosed during court hearings showed that between 2007 and 2009, Raduns worked as a vice president at a bank in Dubuque. During that time, he conspired with another person to lie to the bank about how money the bank was loaning to the other person was being used.

Specifically, they lied about using the money to complete a particular construction project when, instead, it was being used elsewhere. Ultimately, the bank lost over $320,000 in loans made on the construction project.

Source: FDIC RMS.
Responsible Agencies: FDIC OIG with assistance from the FBI.
Prosecuted by the USAO, Northern District of Iowa.

Former Foreign Exchange Trader Sentenced to Prison for Price Fixing and Bid Rigging

On September 17, 2020, Akshay Aiyer, a former currency trader at a major multinational bank, was sentenced to serve 8 months in jail and ordered to pay a $150,000 criminal fine for his participation in an antitrust conspiracy to manipulate prices for emerging market currencies in the global foreign currency exchange (FX) market.

On November 20, 2019, Aiyer was convicted for conspiring to fix prices and rig bids in Central and Eastern European, Middle Eastern, and African (CEEMEA) currencies, which were generally traded against the U.S. dollar and the euro, from at least October 2010 through at least January 2013.

According to evidence presented at trial, the defendant engaged in near-daily communications with his co-conspirators by phone, text, and through an exclusive electronic chat room to coordinate their trades of the CEEMEA currencies in the FX spot market. Aiyer and his co-conspirators manipulated exchange rates by agreeing to withhold bids or offers

to avoid moving the exchange rate in a direction adverse to open positions held by co-conspirators and by coordinating their trading to manipulate the rates in an effort to increase their profits.

By agreeing not to buy or sell at certain times, the conspiring traders protected each other's trading positions by withholding supply of or demand for currency and suppressing competition in the FX spot market for emerging market currencies. The defendant and his co-conspirators took steps to conceal their actions by, among other steps, using code names, communicating on personal cell phones during work hours, and meeting in person to discuss particular customers and trading strategies.

Source: DOJ Antitrust Division.
Responsible Agencies: FDIC OIG and FBI.
Prosecuted by DOJ's Antitrust Division and DOJ's Criminal Division, Fraud Section.

Multiple Defendants Plead Guilty to Defrauding First NBC Bank

In August and September 2020, three separate defendants pleaded guilty to working with bank executives to defraud First NBC Bank out of over $123 million.

On August 26, Gary R. Gibbs pleaded guilty to conspiracy to defraud First NBC Bank. Gibbs and his entities were regularly unable to pay existing loans or overdrafts on their accounts. Bank President Ashton Ryan Jr., Chief Credit Officer William Burnell, and Executive Vice President Robert Calloway, who were all charged on July 10 in a 46-count indictment, disguised Gibbs's and his entities' true financial condition by making new loans to pay Gibbs's existing loans and to cover his overdrafts. They falsely stated in loan documents that Gibbs was able to pay his loans with cash generated by his businesses, and they hid from the First NBC Bank Board of Directors, auditors, and examiners that he was only making his existing loan payments by getting new loans from First NBC.

Ryan, Burnell, and Calloway hid the fact that they actually made loans to Gibbs to keep him and his entities off of month-end reports to the Board, auditors, and examiners. These month-end reports listed borrowers who were not paying their loans or whose accounts were overdrawn. By keeping Gibbs and his entities off of those reports, Ryan, Burnell, and Calloway were able to hide their scheme to keep lending to Gibbs despite his inability to pay his loans. Over the course of several years, Gibbs's debt to First NBC ballooned to $123 million, excluding nominee loans.

On September 2, another defendant in the case, Warren G. Treme pleaded guilty to conspiracy to defraud First NBC Bank. Treme had a banking relationship with First NBC Bank individually and through various entities he controlled. He also co-owned several entities with Ashton Ryan, the bank's President. Throughout Treme's borrowing relationship at First NBC Bank, Treme lacked sufficient income and cash flow from his businesses to pay his loans and personal expenses. Ryan and Burnell disguised Treme's true financial condition by making new loans to pay Treme's existing loans. Rather than using the $400,000 to pay down an outstanding loan debt owed by Treme and his business partners, Ryan and Burnell gave $300,000 to Treme. Treme spent the money on gambling, a trip to the Caribbean, and expenses related to a real estate development company Treme co-owned with Ryan. During a subsequent Board meeting, Ryan and Burnell falsely stated that the $300,000 was used to pay down the outstanding loan debt owed by Treme and his business partners.

A third borrower in the case, Arvind "Mike" Vira pleaded guilty on September 17, to conspiracy to defraud First NBC Bank. In 2006, Ryan lobbied Vira to move his business accounts to First NBC Bank and Vira agreed. Thereafter, Ryan provided Vira with preferential treatment. Although Vira was assigned another loan officer, Ryan acted as his de facto loan officer at the bank and provided Vira with low interest rates for Vira's loans, and he ensured that Vira received high interest rates on his savings and checking accounts. Ryan personally approved 3 percent interest rates for savings and checking accounts held by Vira, his businesses, and his family members. Ryan instructed Vira to inflate his assets on bank loan documents, and Vira complied by claiming to have substantial real estate and outside bank accounts that did not exist. Vira, in turn, provided personal loans to Ryan at Ryan's request. Ryan, knowing that such a loan relationship was prohibited by banking regulations, instructed Vira to conceal this personal loan relationship from First NBC Bank employees. In order to further conceal the loans that he made to Ryan, Vira misrepresented or omitted the interest payments he received from Ryan on his personal tax returns from 2011 through 2015. From 2011 through 2017, Vira received approximately $1,220,271.07 in profits from Ryan's interest payments and from Ryan's preferential treatment at First NBC Bank.

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

Raleigh County Pharmacist Pleads Guilty to Wire Fraud and Money Laundering

On September 21, 2020, Natalie Cochran, of Daniels, West Virginia, pleaded guilty to wire fraud and money laundering and agreed to pay nearly $2.6 million in restitution to her victims and forfeit her interest to the United States in the assets she obtained through her fraudulent activities.

Cochran admitted that from approximately June 2017 through at least August 22, 2019, she knowingly defrauded and took money and property from individuals, a financial institution, and several other companies. Cochran induced them to invest in Technology Management Solutions and Tactical Solutions Group and in phony government contracts by making false representations regarding her and her companies' experience and purported success as government contractors. Cochran also admitted that she convinced at least 11 people to invest approximately $2.5 million in alleged government contracts. She further admitted she never invested the money she received but put it into her personal and business bank accounts for personal purposes unrelated to investments. Cochran admitted to using investor funds to make numerous purchases over $10,000, including withdrawing $37,500 to purchase a 1965 Shelby Cobra.

In addition, she admitted to knowing at least one of her investors suffered a financial hardship as a result of her scheme. In order to keep up appearances, Cochran admitted to using some investors' funds to pay other investors a partial return on their investment.

Source: USAO for the 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.

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	Virginia Crime Analysts Network; New York FBI Cyber Task Force; 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; National Crime Prevention Council, Philadelphia Chapter; Northern Virginia Financial Initiative SAR Review Team; NJ COVID-19 Fraud Task Force.
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; Richmond Tidewater Financial Crimes Task Force; Western District of North Carolina Financial Crimes Task Force; Middle District of North Carolina Financial Crimes Task Force. COVID Working Groups for: Southern District of Florida, Middle District of Florida, Northern District of Florida; SAR review groups for: Miami, Palm Beach, Treasure Coast Financial Crimes Review Team, Key West/Monroe County.
Kansas City Region	Kansas City SAR Review Team; St. Louis SAR Review Team; Minnesota Inspector General Council; Minnesota Financial Crimes Task Force; Nebraska SAR Review Team; Southern District of Iowa SAR Review Team.
Chicago Region	Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Central District of Illinois Financial Fraud Working Group; Northern District of Illinois SAR Review Team; 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.
Electronic Crimes Unit	Washington Metro Electronic Crimes Task Force; High Technology Crime Investigation Association; Council of the Inspectors General on Integrity and Efficiency (CIGIE) Information Technology Subcommittee; 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 relations with partners and stakeholders, resource administration, and 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, 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 Majority staff of the House Financial Services Committee on the *FDIC's Readiness for Crises* and the *FDIC's Top Management and Performance Challenges*. Briefed Majority and Minority staff of the Senate Committee on Banking, Housing, and Urban Affairs on the *FDIC's Readiness for Crises* and *Preventing and Addressing Sexual Harassment*, as well as OIG activities related to the pandemic.
- 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), Audit Committee, Inspection and Evaluation Committee, IT Subcommittee, Investigations Committee, Professional Development Committee, Assistant Inspectors General for Investigations, 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 Act, and coordinated with the IGs on that Council. This Council facilitates sharing of information among CIGFO member Inspectors General and discusses ongoing work of each member IG as it relates to the broader financial sector and ways to improve financial oversight. Provided input on such FDIC OIG work for CIGFO's Annual Report, issued in July 2020.
- Coordinated with the Government Accountability Office (GAO) on ongoing efforts related to the annual financial statement audit of the FDIC and the FDIC's Annual Report, in particular with respect to the risk of fraud at the FDIC.
- 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 COVID-related working groups nationwide.
- Promoted transparency to keep the American public informed through three main means: the FDIC OIG website to include, for example, summaries of completed work, listings of ongoing work, and information on unimplemented recommendations; Twitter communications to immediately disseminate news of report and press release issuances and other news of note; and 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.
- Participated as a member of the Pandemic Response Accountability Committee.
- Participated in a press conference with the U.S. Department of Justice and other law enforcement partners announcing charges against individuals who sought to defraud the Paycheck Protection Program.
- Coordinated with the FDIC Chairman on Whistleblower Appreciation Day to communicate the important rights, duties, and protections of whistleblowers.
- Informed stakeholders of the role and impact of our Office of Investigations through the development and distribution of an informative flyer.
- Added a new region to the organization of our Office of Investigations for increased geographical coverage of cases.

Administering resources prudently, safely, securely, and efficiently.

- Continued efforts by the OIG's Office of Information Technology (OIT) to coordinate a strategic approach to facilitate the integration of technology in OIG processes. This group is responsible for the OIG's enterprise architecture, and IT governance and related policies and procedures.
- Continued pursuing component office implementation plans designed to achieve the OIG's Strategic Goals, Guiding Principles, and Vision for 2020.
- Continued our work in developing a new case management system for our Office of Investigations.
- Provided support to OIG staff on conversion to Windows 10 and conducted training on the secure use of MS Teams for OIG collaboration.
- Upgraded OIG mobile devices and laptops, to meet the technology demands of the Office.
- 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, management operations, and administrative processes of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the Office.
- Carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. Positions filled during the reporting period included the Director of OIT, Special Agent in Charge of the ECU, Engagement and Learning Officer, 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 for such activities as travel and training.
- Integrated MS Teams into our Office to increase virtual collaboration and communication, particularly during this current time of the pandemic, when mandatory telework is in place.
- Held town halls to discuss the ongoing pandemic, update staff on the FDIC's efforts, and convey our Office's return to work strategy.

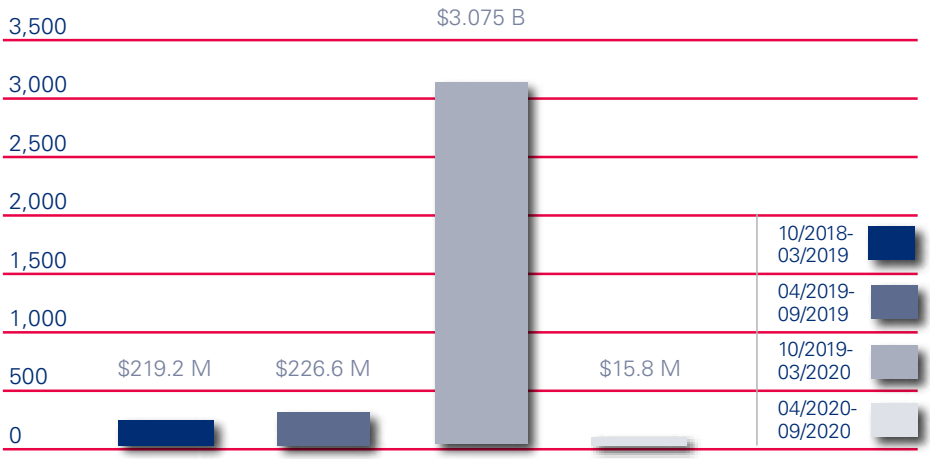
Exercising leadership skills and promoting teamwork.

- 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.
- Leveraged the OIG's Data Analytics capabilities to assist audit and evaluation staff.
- Kept OIG staff informed of Office priorities and key activities through regular meetings among staff and management, updates from senior management meetings, and issuance of OIG newsletters.
- Enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities.
- 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 during the first virtual OIG Awards ceremony.
- 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 training on Understanding and Addressing Sexual Harassment.
- Welcomed a new Deputy Inspector General to the OIG's Immediate Office.
- Brought on-board an Engagement and Learning Officer to work across the organization and assist with employee engagement and career development.
- Promoted many staff members across component offices to leadership positions.
- 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.

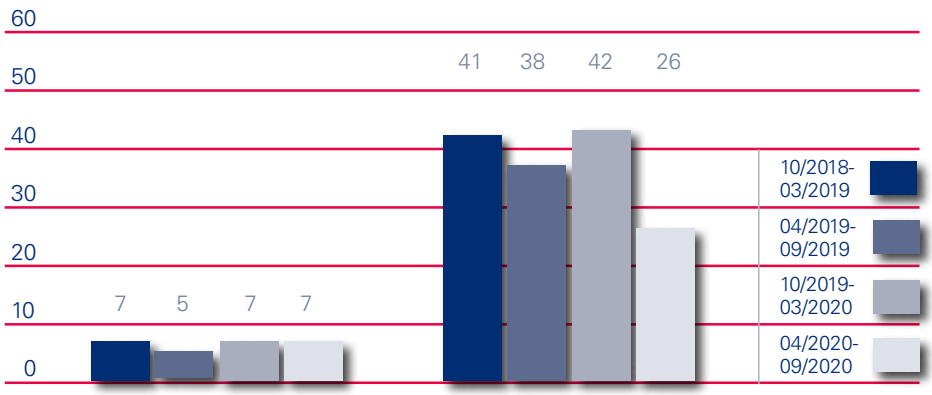
Cumulative Results (2-year period)

Nonmonetary Recommendations	
October 2018 - March 2019	24
April 2019 - September 2019	24
October 2019 - March 2020	37
April 2020 - September 2020	44

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.	29
Section 5(a)(1):	Significant problems, abuses, and deficiencies.	4-9
Section 5(a)(2):	Recommendations with respect to significant problems, abuses, and deficiencies.	4-9
Section 5(a)(3):	Significant recommendations described in previous semiannual reports on which corrective action has not been completed.	30-31
Section 5(a)(4):	Matters referred to prosecutive authorities.	41
Section 5(a)(5):	Summary of each report made to head of establishment regarding information or assistance refused or not provided.	41
Section 5(a)(6):	Listing of audit, inspection and evaluation reports by subject matter with monetary benefits.	39
Section 5(a)(7):	Summary of particularly significant reports.	4-9
Section 5(a)(8):	Statistical table showing the total number of audit, inspection, and evaluation reports and the total dollar value of questioned costs.	40
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.	40
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	41
	• no establishment comment was received within 60 days of providing the report	41
	• there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.	32-38
5(a)(11):	Significant revised management decisions during the current reporting period.	41
Section 5(a)(12):	Significant management decisions with which the OIG disagreed.	41
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.	43-44

Section 5(a)(17):	Statistical tables showing, for the reporting period:	
	• number of investigative reports issued	41
	• number of persons referred to the DOJ for criminal prosecution	41
	• number of persons referred to state and local prosecuting authorities for criminal prosecution	41
	• number of indictments and criminal informations.	41
Section 5(a)(18):	A description of metrics used for Section 5(a)17 information.	41
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.	41
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.	41
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.	41
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.	41

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 CIGIE Legislation Committee. Much of the FDIC OIG's activity reviewing legislation and regulation occurs in connection with that Committee. Some of the CIGIE Legislation Committee's current priority areas include: testimonial subpoena authority, Program Fraud Civil Remedies Act amendments, statutory exclusion from receiving government contracts or grants for convicted fraud felons, and clarifying the whistleblower rights for employees of subcontractors and subgrantees.

Of note during the reporting period, our Office reviewed and commented, as appropriate, on the following:

- **Securing Inspector General Independence Act of 2020:** Our Office provided several specific technical edits and suggestions regarding the draft bill, primarily related to prudent implementation, should this bill become law.
- **Accountability and Transparency for Federally Funded Facial Recognition Technology Act:** We commented and raised questions regarding what role, if any, IGs would play in overseeing an Agency's compliance in the event this bill was enacted into law.

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

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

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

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

Report Number, Title, and Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
Management Action in Process		
AUD-18-004 **The FDIC's Governance of Information Technology Initiatives** July 26, 2018	**7**	As part of the Chief Information Officer Office's (CIOO) ongoing Enterprise Information Technology (IT) Maturity Program, the CIOO will develop a workforce planning process that will ensure the identification and documentation of the IT resources and expertise needed to execute the FDIC's IT Strategic Plan.
EVAL-20-001 **Contract Oversight Management** October 28, 2019	**1**	The Acquisition Services Branch will coordinate with the Division of Information Technology's Business Intelligence Service Center (BISC) to develop reports that identify the original contract award amount and original period of performance and changes to these key data fields that occur over the life of the award; capture automated procurement system data associated with modified contracts, including the original contract award amount and original period of performance; and, in coordination with BISC, develop reports that identify contract ceiling and period of performance changes.

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 (PCM) program that aligns with OMB Circular A-130 and ensures privacy controls are regularly assessed for effectiveness. The FDIC plans to implement the PCM 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.

* Implementation scheduled for a future date.

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-17-001 **Audit of the FDIC's Information Security Program - 2016** November 2, 2016	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct a performance audit to evaluate the effectiveness of the FDIC's information security program and practices. C&C found that the FDIC had established a number of information security program controls and practices that were generally consistent with Federal Information Security Modernization Act (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 (2016) FISMA audit and the remaining 11 were identified in prior OIG or GAO 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 (CIO) to improve the effectiveness of the FDIC's information security program and practices.	6	1	NA
AUD-18-004 **The FDIC's Governance of Information Technology Initiatives** July 26, 2018	Federal statutes and OMB policy require federal agencies to establish and implement fundamental components of information technology (IT) governance. These components include IT strategic planning, which defines the overall direction and goals for the agency's IT program, and an enterprise architecture, which describes the agency's existing and target architecture and plan to achieve the target architecture. The OIG conducted an audit to identify key challenges and risks that the FDIC faced with respect to the governance of its IT initiatives.	8	1	NA

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
	We found that the FDIC faced a number of challenges and risks with respect to the governance of its IT initiatives. Specifically, the FDIC had not fully developed a strategy to migrate IT services and applications to the cloud or obtained the acceptance of key business stakeholders before taking steps to initiate cloud projects. In addition, the FDIC had not implemented an effective enterprise architecture to govern its IT decision-making or completed needed revisions to its IT governance processes to ensure sufficiently robust governance for all of its IT initiatives. The FDIC had also not fully integrated security within its IT governance framework or acquired the resources and expertise needed to support the adoption of cloud solutions. Further, the FDIC did not use complete cost information or fully consider intangible benefits when evaluating cloud solutions. The FDIC took a number of actions to strengthen its IT governance during and after our audit. The report contained eight recommendations to improve upon these efforts.			
AUD-19-003 **Payments to Pragmatics, Inc.** December 10, 2018	The FDIC OIG initiated an audit in response to a complaint received through the OIG's Hotline. The complaint alleged that an employee working for a subcontractor of Pragmatics, Inc. (Pragmatics) under the FDIC's Information Technology Application Services (ITAS) II contract billed the FDIC for labor hours that the employee did not actually work. The complaint also alleged that Pragmatics and one of its subcontractors may have inappropriately billed the FDIC for contractor employee labor hours. The audit objective was to determine whether certain labor charges paid to Pragmatics were adequately supported, allowable under the contract, and allocable to their respective task orders.	7	4	$47,489

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
	We found that $47,489 (approximately 10 percent of the labor charges we reviewed) were either unsupported or unallowable. Of this amount, $7,510 was unsupported because the employees who billed the hours did not access the FDIC's network or facilities on the days they charged the hours. The report contained seven recommendations to: determine the portion of the $47,489 in labor charges that should be disallowed and recovered; assess whether additional labor charges not covered by the audit should be disallowed and recovered; and improve the FDIC's administration of the ITAS II contract.			
AUD-20-001 **The FDIC's Information Security Program - 2019** October 23, 2019	The FDIC OIG engaged the professional services firm of 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
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	14	12	NA

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
	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.			
EVAL-19-001 **The FDIC's Physical Security Risk Management Process** April 9, 2019	The FDIC OIG evaluated the FDIC's physical security risk management process. President Clinton, by Executive Order, created the Interagency Security Committee (ISC) in order to issue standards, policies, and best practices to enhance the quality and effectiveness of security in non-military Federal facilities in the United States. Our evaluation objective was to determine the extent to which the FDIC's physical security risk management process met Federal standards and guidelines. We concluded that the FDIC had not established an effective physical security risk management process to ensure that it met ISC standards and guidelines. While the FDIC had not identified any major incidents or threats to its facilities, we found that the FDIC's physical security risk management process needed improvement. Decisions regarding facility security risks and countermeasures were frequently undocumented and not guided by defined policy or procedure. As a result, the FDIC did not conduct key activities in a timely or thorough manner for determining security	9	1	NA

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
	risk level, assessing security protections in the form of countermeasures, mitigating and accepting risk, and measuring program effectiveness. The report contained nine recommendations aimed at improving the FDIC's physical security risk management process.			
EVAL-19-002 **Minority Depository Institution Program at the FDIC** September 24, 2019	In 1989, the Financial Institutions Reform, Recovery, and Enforcement Act required the Secretary of the Treasury to consult with ... the Chairperson of the Board of Directors of the FDIC on the methods for best achieving five goals aimed at preserving and promoting Minority Depository Institutions (MDI). The FDIC OIG conducted an evaluation to examine the FDIC's actions to preserve and promote MDIs and assess whether the MDI Program is achieving its goals. We concluded that the FDIC achieved its program goals as outlined in the FDIC's MDI Policy Statement. Notwithstanding these efforts, we found that the FDIC did not evaluate the effectiveness of some key MDI Program activities. We also found that FDIC Headquarters did not define the types of activities that it considered to be MDI technical assistance, as distinct from training, education, and outreach events. Additionally, while the FDIC provided training, education, and outreach events, the MDI banks, FDIC Regional Coordinators for MDIs, and representatives from MDI trade associations requested that the FDIC provide more such events. The report contained five recommendations to improve the FDIC's MDI Program.	5	2	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	12	6	NA

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
	contracting management information system, the capacity of Oversight Managers (OMs) to oversee assigned contracts, OM training and certifications, and security risks posed by contractors and their personnel. We concluded that the FDIC must strengthen its contract oversight management. Specifically, we found that the FDIC was overseeing its contracts on a contract-by-contract basis rather than a portfolio basis and did not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency. We also found that the FDIC's contracting files were missing certain required documents, Personally Identifiable Information was improperly stored, some OMs lacked workload capacity to oversee contracts, and certain OMs were not properly trained or certified. The report contained 12 recommendations to strengthen contract oversight.			
EVAL-20-002 **Offsite Reviews of 1- and 2- Rated Institutions** December 15, 2020	The FDIC designed the Offsite Review Program to identify emerging supervisory concerns that may occur at insured depository institutions between onsite examinations so that supervisory strategies can be adjusted appropriately. The FDIC OIG conducted an evaluation of Offsite Reviews of 1- and 2-Rated Institutions. The objectives of our evaluation were to assess whether (1) the Offsite Review Program identified 1- and 2-rated institutions with emerging supervisory concerns; (2) the Offsite Review Program resulted in the FDIC appropriately adjusting the supervisory strategies for these institutions in a timely manner; and (3) the adjusted supervisory strategies were effective. We found that the Offsite Review Program identified 1- and 2-rated institutions with emerging supervisory concerns related to rapid growth, noncore funding, deteriorating financial trends, or those identified and added by the Regional Offices. However, the FDIC should evaluate additional methods and new technologies to identify institutions with other types	3	1	NA

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
	of emerging supervisory concerns, such as those related to internal controls, credit administration, and management practices. We also found that offsite reviews were inconsistent in terms of the amount of time Case Managers spent, as well as the depth and coverage, due to a lack of guidance regarding the scope and methodology for conducting offsite reviews. In addition, conflicting perspectives existed between Case Managers and RMS senior managers on the importance of conducting offsite reviews of institutions that recur on the Offsite Review List. The report contained three recommendations aimed at improving the FDIC's offsite review process.			
EVAL-20-003 **Cost Benefit Analysis Process for Rulemaking** February 4, 2020	The FDIC OIG conducted an evaluation of the FDIC's Cost Benefit Analysis Process for Rulemaking. Through the Banking Act of 1933, Congress provided the FDIC with the authority to promulgate rules to fulfill the goals and objectives of the Agency. A cost benefit analysis informs the agency and the public whether the benefits of a rule are likely to justify the costs, or determines which of various possible alternatives is most cost effective. Our evaluation objective was to determine if the FDIC's cost benefit analysis process for rules was consistent with best practices. We found that the FDIC's cost benefit analysis process was not consistent with widely recognized best practices identified by the OIG. Specifically, we found that the FDIC had not established and documented a process to determine when and how to perform cost benefit analyses. We also found that the FDIC did not leverage the expertise of its Regulatory Analysis Section economists during initial rule development; did not require the Chief Economist to review and concur on the cost benefit analyses performed, which is an important quality control; was not always transparent in its disclosure of cost benefit analyses to the public; and did not perform cost benefit analyses after final rule issuance. The report contained five recommendations to improve the FDIC's cost benefit analysis process.	5	5	NA

Table III: Audit and Evaluation Reports Issued by Subject Area

Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	**Title**	**Total**	**Unsupported**	
Supervision				
EVAL-20-007 September 30, 2020	In-Depth Review of Enloe State Bank, Cooper, Texas			
Information Technology and Cybersecurity				
AUD-20-004 June 23, 2020	Security Controls Over the Federal Deposit Insurance Corporation's Regional Automated Document Distribution and Imaging System			
Resource Management				
EVAL-20-004 April 7, 2020	The FDIC's Readiness for Crises			
EVAL-20-005 July 8, 2020	The FDIC's Implementation of Enterprise Risk Management			
EVAL-20-006 July 10, 2020	Preventing and Addressing Sexual Harassment			
Totals for the Period		**$0**	**$0**	**$0**

Other Products Issued - Failed Bank Reviews:

- Louisa Community Bank, Louisa, Kentucky (FBR-20-001) April 14, 2020
- Ericson State Bank, Ericson, Nebraska (FBR-20-002) August 17, 2020

Table IV: Audit and Evaluation Reports Issued with Questioned Costs

	Questioned Costs		
	Number	Total	Unsupported
A. For which no management decision has been made by the commencement of the reporting period.	1	$47,489	$7,510
B. Which were issued during the reporting period.	0	$0	$0
Subtotals of A & B	**1**	**$47,489**	**$7,510**
C. For which a management decision was made during the reporting period.	1	$47,489	$7,510
(i) dollar value of disallowed costs.	1	$47,489	$7,510
(ii) dollar value of costs not disallowed.	0	$0	$0
D. For which no management decision has been made by the end of the reporting period.	0	$0	$0
Reports for which no management decision was made within 6 months of issuance.	0	$0	$0

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

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

Table VI: Status of OIG Recommendations Without Management Decisions

During this reporting period, there were no recommendations more than 6 months old without management decisions.

Table VII: Status of OIG Reports Without Comments

During this reporting period, there were no reports where comments were received after 60 days of providing the report to management.

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	26
• Number of Persons Referred to the Department of Justice for Criminal Prosecution	209
• Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	0
• Number of Indictments and Criminal Informations	77

Description of the metrics used for the above information: Reports issued reflects case closing memorandums issued to FDIC management. With respect to the 209 referrals to DOJ, the total represents 161 individuals and 48 business entities. 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, audits, or investigations involving senior government employees that were closed and not disclosed to the public.

Appendix 2

Information on Failure Review Activity

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

FDIC OIG Review Activity for the Period April 1, 2020 Through September 30, 2020 (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 (DIF) 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 two Failed Bank Reviews during the reporting period. As of the end of the reporting period, the FDIC OIG was conducting the following Failed Bank Review. Results of this review will be included in an upcoming semiannual report.

The First State Bank
Barboursville, West Virginia

Closed:	April 3, 2020
Estimated Loss to the DIF:	$46.8 million

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

Congratulations to FDIC OIG Award Recipients: Awards for Excellence from the Council of the Inspectors General on Integrity and Efficiency

Award for Excellence-Audit – Preventing and Detecting Cyber Threats

The team's work identified weaknesses that limited the effectiveness of the FDIC's network firewalls and Security Information and Event Management tool in preventing and detecting cyber threats. This audit report and its recommendations have led to significant improvements to reduce the risk of a cyber threat impacting the FDIC's network.

Joe Nelson	**Sharon Tushin**
Judy Hoyle	**Stacey Luck**
Jin Zhu	**Cam Thurber**
Alexander Kreckel	**Tom Ritz**

Award for Excellence-Investigations – Inyx, Inc. Case

This case involved a former Chief Executive Officer and Chairman of the now-bankrupt Inyx, Inc., a multinational pharmaceutical company. The defendant caused Westernbank, one of the largest banks in Puerto Rico at the time, to lend him approximately $142 million based on false and fraudulent invoices from customers, and he used those funds for his personal gain. The losses from this scheme led to the eventual insolvency and collapse of Westernbank, and the defendant was sentenced to 30 years in prison.

Gary Sherrill	**Greg Coats**
Sean Stephenson	**Margaret Faden**
Fran Mace	**Regina Sandler**

In addition, the following individuals were recognized at the Awards Ceremony:

Kelvin Zwiefelhofer (OIG/OI-San Francisco)

Kelvin was a member of the team investigating the activities of Wells Fargo and Co. and its subsidiary. These entities agreed to pay $3 billion to resolve matters stemming from a years-long practice of pressuring employees to meet unrealistic sales goals. Such pressure tactics led employees to provide millions of accounts or products to customers under false pretenses or without consent, often by creating false records or misusing customers' identities. Wells Fargo admitted that it collected millions of dollars in fees and interest to which the company was not entitled, harmed the credit ratings of customers, and unlawfully misused customers' sensitive personal information.

Joe Moriarty (OIG/OI-Chicago)

Joe was a member of the team that investigated Country Bank (Aledo, Illinois). The investigation uncovered $23 million in fraud committed by a founder/Chief Lending Officer, a loan officer, and Vice President of Community Lending. One defendant was sentenced to 5 years in prison and ordered to pay $23.5 million in restitution, in addition to other convictions and sentences in the case.

Roger W. Jones Award from American University

Matthew Alessandrino, the FDIC OIG Assistant Inspector General for Investigations, received the Roger W. Jones Award. Since 1978, the Roger W. Jones Award has annually recognized Federal career executives who have demonstrated superior leadership in achieving their agency's mission and developing future managers. This year, Matthew was among five senior Federal executives who were honored on October 21, 2020 at a virtual ceremony for their commitment to developing and inspiring those whom they lead, consistent with extraordinary public service.

Farewell to OIG Retirees

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.

Trina Petty
Director of Human Resources

David Rubin
Auditor

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 73 Federal OIGs on the IG Community's website

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**