FDIC Office of Inspector General

Semiannual Report to the Congress

October 1, 2019 – March 31, 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 5,590 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured more than $7.8 trillion in deposits in 5,177 institutions, of which the FDIC supervised 3,338. The Deposit Insurance Fund (DIF) balance totaled $110.3 billion as of December 31, 2019. Active receiverships as of that date totaled 248, with assets in liquidation of about $524 million.

Office of Inspector General

Semiannual Report to the Congress

October 1, 2019 – March 31, 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 October 1, 2019 to March 31, 2020.

During the reporting period, we identified the Top Management and Performance Challenges facing the FDIC:

- Keeping Pace with Emerging Financial Technologies;
- Enhancing the FDIC's Information Technology Security Program;
- Ensuring the FDIC's Readiness for Crises;
- Sharing Threat Information with Banks and Examiners;
- Strengthening the Governance of the FDIC;
- Overseeing Human Resources;
- Keeping FDIC Facilities, Information, and Personnel Safe and Secure;
- Administering the Acquisition Process; and
- Measuring Costs and Benefits of FDIC Regulations.

Our assessment is based upon our observations and experience from oversight work, as well as reports from other Government agencies and officials, relevant academic literature, and private-sector entities.

We also issued the results of several audits and evaluations during the reporting period. For example, we found that the FDIC's Contract Oversight Management system had limited data and reporting capabilities for Agency-wide oversight of its contract portfolio. In another evaluation report, we determined that the FDIC's Cost Benefit Analysis process for rulemaking was not consistent with recognized best practices. Also, we reported that the FDIC did not fully integrate privacy considerations into its risk management framework.

In addition, the OIG worked closely with our law enforcement partners in investigating criminal matters involving complex schemes of bank fraud, embezzlement, money laundering, and other financial crimes. In one of our cases, Wells Fargo agreed to pay $3 billion to resolve criminal and civil investigations into sales practices involving the opening of millions of accounts without customer authorization. In another case, a former Executive Director at a major multinational bank was convicted by a jury for his participation in an antitrust conspiracy to manipulate prices in the foreign currency exchange market. In yet another case, top executives of a solar generator company pleaded guilty to participating in a billion-dollar Ponzi scheme.

Importantly, our Office has been invited to become a member of the recently-formed 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 to oversee $2.4 trillion in Federal emergency relief. We look forward to working with our counterparts in the IG community on this important oversight initiative.

Also, we are pleased to welcome a new Deputy Inspector General to our executive leadership team, Tyler Smith. Mr. Smith brings a wealth of experience from his background in the Inspector General community, and he will be a great asset in building relations with our external stakeholders. In addition, I am personally grateful for the hard work and dedication of the women and men of the OIG, particularly during a time when our Nation is undergoing the unique challenges of this pandemic.

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 unprecedented times.

Jay N. Lerner
Inspector General
April 30, 2020

Table of Contents

Inspector General's Statement	i
Introduction and Overall Results	3
Audits, Evaluations, and Other Reviews	4
Investigations	11
Other Key Priorities	18
Reporting Requirements	23
Appendix 1: Information Required by the Inspector General Act of 1978, as Amended	25
Appendix 2: Information on Failure Review Activity	37
Appendix 3: Peer Review Activity	38
Congratulations and Farewell	40

Acronyms and Abbreviations

AIG	Assistant Inspector General
CB&T	Citizens Bank and Trust
C&C	Cotton & Company LLP
CEEMEA	Central and Eastern European, Middle Eastern, and African
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
D&I	Diversity and Inclusiveness
DATA Act	Digital Accountability and Transparency Act of 2014
DIF	Deposit Insurance Fund
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOJ	Department of Justice
GAO	Government Accountability Office
ECU	Electronic Crimes Unit
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act of 2014
FX	Foreign Exchange
IG	Inspector General
IT	Information Technology
MDI	Minority Depository Institution
NASA	National Aeronautics and Space Administration
OIG	Office of Inspector General
OIT	Office of Information Technology
OM	Oversight Manager
OMB	Office of Management and Budget
PAE	Office of Program Audits and Evaluations
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SAR	Suspicious Activity Report
Treasury	U.S. Department of the Treasury
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 (October 1, 2019 – March 31, 2020)	
Audit, Evaluation, and Other Products Issued	**7**
Nonmonetary Recommendations	**37**
Investigations Opened	**55**
Investigations Closed	**42**
Judicial Actions:	
Indictments/Informations	39
Convictions	27
Arrests	21
OIG Investigations Resulted in:	
Fines of	$ 695,500
Restitution of	$ 3,070,232,728*
Asset Forfeitures of	$ 4,692,600
Total	**$ 3,075,620,828**
Referrals to the Department of Justice (U.S. Attorney)	**134**
Proposed Regulations and Legislation Reviewed	**2**
Responses to Requests Under the Freedom of Information/Privacy Act	**11**

* Restitution this period includes a $3.0 billion negotiated monetary settlement with Wells Fargo Bank. Additionally, of the total amount, $1,734,156 was ordered joint and several with other individuals sentenced during this period, and $863,418 was ordered joint and several with individuals sentenced in a prior period.

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.

We issued the results of three audits and three evaluations during the reporting period, as summarized below. These reports contained 37 nonmonetary recommendations. Additionally, we issued our assessment of the *Top Management and Performance Challenges Facing the FDIC*. 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. During the reporting period, we were informed of two failures: Louisa Community Bank, Louisa, Kentucky, and Ericson State Bank, Ericson, Nebraska. These failures did not cause a material loss to the DIF; however, we will conduct failed bank reviews of the institutions, as noted in Appendix 2.

Audits and Evaluations

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. The Administrative Procedure Act defines a rule as the whole or part of an agency statement "designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency." Rulemaking is the "agency process for formulating, amending, or repealing a rule."

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 would be the most cost effective.

We found that the FDIC's cost benefit analysis process was not consistent with widely recognized best practices that we identified, as noted below:

- The FDIC had not established and documented a process to determine when and how to perform cost benefit analyses. As a result, the FDIC's process did not ensure the appropriate depth of analyses was performed; resulted in inconsistent analyses; and limited public awareness and transparency.
- The FDIC did not leverage the expertise of its Regulatory Analysis Section economists during initial rule development.
- The FDIC did not require the Chief Economist to review and concur on the cost benefit analyses performed, which is an important quality control.
- The FDIC was not always transparent in its disclosure of cost benefit analyses to the public. The FDIC did not publish why a cost benefit analysis was or was not performed; the reason for the depth of analysis performed; the scope and methodology used; and the analysis performed.
- The FDIC did not perform cost benefit analyses after final rule issuance. Absent such analyses, the FDIC may not identify duplicative, outdated, or overly burdensome rules in a timely manner and may not ensure that its rules are effective and have achieved their intended objectives or outcomes.

We made five recommendations designed to improve the FDIC's cost benefit analysis process. Management concurred with four recommendations and partially concurred with one recommendation.

Offsite Review Program

The Federal Deposit Insurance Act requires onsite examinations of FDIC-insured financial institutions at least once during each 12-month period. Between onsite examinations, an institution's financial condition may change. Therefore, the FDIC designed the Offsite Review Program to identify emerging supervisory concerns and potential problems between onsite examinations so that it could adjust supervisory strategies appropriately.

We evaluated whether (1) the Offsite Review Program identified highly rated institutions (those rated "1" and "2") with emerging supervisory concerns; (2) the 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 by Regional Offices. However, the FDIC should:

- Evaluate additional methods and new technologies to identify institutions with other types of emerging supervisory concerns. These could include concerns related to internal controls, credit administration, and management practices;
- Enhance the Offsite Review Procedures to provide detailed guidance for Case Managers regarding the offsite review process, such as determining the scope and methodology of offsite reviews; and
- Provide Case Managers with training to ensure consistent application of offsite review procedures.

When an emerging supervisory concern was identified for highly rated institutions, we found that the FDIC appropriately adjusted its supervisory strategy in a timely manner; and the adjusted supervisory strategies were effective.

We made three recommendations to improve the Program. Management agreed with all recommendations.

The FDIC's Privacy Program

The FDIC collects and maintains significant quantities of Personally Identifiable Information (PII) on bankers, financial institution customers, FDIC employees, and contractors. As of June 2018, the FDIC reported that it maintained 338 information systems containing PII. The significant amount of 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.

We conducted an audit to assess the effectiveness of the FDIC's Privacy Program and practices. The audit focused on the FDIC's compliance in eight of the nine privacy control areas established within Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*.

We found that the Privacy Program controls and practices we assessed were effective in four of eight areas examined. However, privacy controls and practices with respect to the Risk Management Framework; Privacy Roles and Responsibilities; Managing PII; and Privacy Impact Assessments (PIA) were either partially effective or not effective. The FDIC's Privacy Program in these areas did not comply with all relevant privacy laws and/or OMB policy and guidance.

Specifically, we found that the FDIC did not:

- Fully integrate privacy considerations into its risk management framework designed to identify and address privacy risks;
- Adequately define or implement certain privacy responsibilities; or
- Effectively manage or secure PII stored in network shared drives and in hard copy.

During our audit, we alerted FDIC management to instances of both electronic and hard copy records containing sensitive PII that lacked appropriate access restrictions, prompting urgent action.

Further, we found that the FDIC did not dispose of PII within established timeframes, and it did not ensure that the Agency always completed, monitored, and retired PIAs in a timely manner.

Our report contained 14 recommendations intended to strengthen the effectiveness of the FDIC's Privacy Program and records management practices. FDIC management concurred with all of the recommendations.

Contract Oversight Management

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. The average annual awarded amount by the FDIC for contractor services over these 5 years was approximately $640 million.

We examined the FDIC's oversight and monitoring of contracts using its contracting management information system, the capacity of Oversight Managers (OM) to oversee assigned contracts, OM training and certifications, and security risks posed by contractors and their personnel.

We reported that the FDIC must strengthen its contract oversight management. For four sampled contracts, we found that the FDIC received goods and services as specified in the contracts and complied with its security requirements for contractors and their personnel.

In addition, we found that the FDIC needed to improve its contract management information system, contract documentation, workload capacity of OMs for one Division, and the training and certification of certain OMs. Specifically, we found that:

- The FDIC's contracting management information system had limited data and reporting capabilities for Agency-wide oversight of its contract portfolio;
- The FDIC's contract files were missing certain required documentation such as contract inspection and acceptance documentation;
- PII was improperly stored in the FDIC's electronic contract file due to a contradiction between FDIC policy and instructions to OMs;
- Some OMs within the FDIC's Division of Information Technology lacked the workload capacity to oversee contracts; and
- Certain OMs were not properly trained or certified as prescribed by FDIC policy.

We made 12 recommendations to improve the FDIC's contract oversight management. Management concurred with 10 of the 12 recommendations and partially concurred with the remaining 2 recommendations.

The FDIC's Information Security Program—2019

The OIG engaged a contract firm to evaluate the effectiveness of the FDIC's information security program and practices, as required by the Federal Information Security Modernization Act of 2014 (FISMA). The FDIC's overall information security program was operating at a Maturity Level 3 (Consistently Implemented) on a scale of 1-5. Programs operating below a Maturity Level 4 are not considered effective.

The FISMA report describes security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. The six highest risk weaknesses are briefly described below.

Risk Management. The FDIC had not yet completed an inventory of risks facing the FDIC, or a Risk Profile to help manage and prioritize risk mitigation activities. The FDIC also needed to develop a method and strategy to classify risk ratings and risk profiles of applications and systems, and develop and communicate the FDIC's information security Risk Tolerance level and Risk Profile.

Network Firewalls. In a previous report, we found that many of the FDIC's network firewall rules that controlled the flow of inbound and outbound traffic lacked a documented justification and the majority were unnecessary. The FDIC took steps to address these weaknesses, but further actions were needed.

Privileged Account Management. Hackers and other adversaries target administrative accounts to perform malicious activity, such as exfiltrating sensitive information. Our report identified vulnerabilities related to these accounts that increased the risk of unauthorized network access or malicious activity.

Protection of Sensitive Information. We conducted unannounced walkthroughs of selected FDIC facilities and identified significant quantities of sensitive hard copy information stored in unlocked filing cabinets and boxes in building hallways. We also identified instances in which sensitive information stored on internal network shared drives was not restricted to authorized users.

Security and Privacy Awareness Training. FDIC employees and contractor personnel with network access must complete security and privacy awareness training within 1 week of employment, and annually thereafter. If not, their network access is revoked. We identified 29 network users who did not satisfy the FDIC's awareness training requirement but still had access to the network.

Security Control Assessments. Our report discusses instances that occurred in 2016 and 2017 in which security control assessors did not test the implementation of security controls, when warranted. Instead, assessors relied on narrative descriptions of controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel.

The FDIC was working to address six recommendations from prior FISMA audit reports to strengthen controls in the areas of risk management, contactor-provided services, Plans of Action and Milestones, and vulnerability and compliance scanning. This FISMA report contained three new recommendations to ensure employees and contractor personnel properly safeguard sensitive electronic and hardcopy information, and network users complete required security and privacy awareness training. The FDIC concurred with these three recommendations.

The FDIC's Compliance with the Digital Accountability and Transparency Act of 2014
The Digital Accountability and Transparency Act of 2014 (DATA Act) expanded the Federal Funding Accountability and Transparency Act of 2006 to increase accountability and transparency in Federal spending. The DATA Act directs Federal IGs to review a statistically valid sample of spending data submitted by their agency and to report the results to Congress.

We conducted an audit to assess the (1) completeness, timeliness, quality, and accuracy of the financial and award data submitted for the first quarter of Fiscal Year 2019 and published on USASpending.gov; and (2) FDIC's implementation and use of the Government-wide financial data standards established by OMB and the Department of the Treasury (Treasury).

We found that the FDIC's financial and award data submitted for the first quarter of Fiscal Year 2019 was complete, timely, of sufficient quality, and accurate. We determined that all required transactions and events were recorded in the proper period and within the reporting schedule established by the DATA Act. In addition, we evaluated the FDIC's use of the Government-wide financial data standards and determined that the Agency's definitions of the data standards complied with OMB and Treasury guidance. We also found that the FDIC had established controls to promote complete, accurate, timely, and quality reporting under the DATA Act. Such controls included written procedures to comply with the DATA Act and the designation of a DATA Act Senior Accountability Official.

Additionally, the FDIC implemented a quality assurance process that segregated data preparation and review duties, and documented each level of review. We concluded that the FDIC could reasonably rely on its source financial system for the DATA Act submission for the first quarter of Fiscal Year 2019.

We made no recommendations in this report.

Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

The FDIC plays a critical role in maintaining safety and soundness at financial institutions, and the stability of our financial system. At the time of our assessment, the Agency insured more than $7.7 trillion in deposits at about 5,250 financial institutions and directly supervised approximately 3,380 of these banks.

Pursuant to the Reports Consolidation Act of 2000, we identified the following Top Management and Performance Challenges facing the FDIC. Our assessment is based upon the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and other relevant literature, perspectives from Government agencies and officials, and information from private-sector entities.

Keeping Pace with Emerging Financial Technologies: Emerging technologies promise potential benefits but also introduce risk. Increased digital interconnections with multiple avenues to access banking systems elevate cybersecurity risk because an incident at one digital juncture has the potential to infect the banking system. The FDIC's challenge is keeping pace with new technology and the associated risks to banks, third-party service providers, and the banking system.

Enhancing the FDIC's Information Technology (IT) Security Program: As of June 2018, the FDIC had 338 IT systems that collect, store, or process PII and sensitive information. The FDIC also has legacy systems that are becoming difficult and expensive to maintain. The FDIC is modernizing its technology and must maintain the security of information within its systems as the IT environment evolves.

Ensuring the FDIC's Readiness for Crises: The FDIC identified two important lessons learned following the recent financial crisis: (i) the importance of crisis readiness planning; and (ii) quickly addressing emerging supervisory risks. Best practices identify the principles and elements of effective preparedness that collectively provide a framework for crisis planning efforts. Adopting such a framework strengthens the FDIC's ability to respond to a crisis in a timely and effective manner.

Sharing Threat Information with Banks and Examiners: Federal Government agencies gather a substantial volume of information related to the safety and soundness of financial institutions in the United States. Bankers need to receive actionable information in order to respond to threats in a timely manner. FDIC examiners responsible for supervised institutions should be aware of threats directed toward those institutions to understand their impact and make necessary supervisory adjustments. FDIC policy makers should be aware of emerging threats to ensure that relevant threat information is disseminated to banks and examiners, and to be able to adjust examination policy and procedures, and supplement or modify the regulatory scheme.

Strengthening the Governance of the FDIC: The Federal Deposit Insurance Act vests the management of the FDIC in its Board of Directors. The FDIC Board delegates authority to FDIC senior leaders to fulfill the Agency's mission, including implementation of its Enterprise Risk Management program. The FDIC should ensure that it is identifying and managing risks, and making data-driven acquisition decisions.

Overseeing Human Resources: Within the next few years, the FDIC will need to navigate a potential wave of retirements, reverse attrition trends among its core examination workforce, and hire staff with skills to match technology innovation. Effective management of these challenges limits the impact of leadership and skill gaps, and the loss of institutional experience and knowledge due to retirements.

Keeping FDIC Facilities, Information, and Personnel Safe and Secure: The FDIC is responsible for protecting approximately 6,000 employees and 3,000 contract personnel who work at 94 FDIC-owned or leased facilities throughout the country. The FDIC also has significant responsibility for its systems containing PII and sensitive PII related to employees, contractors, bank management, and deposit holders. The challenge for the FDIC is to maintain appropriate processes to safeguard facilities, information, and personnel.

Administering the Acquisition Process: In 2018, the FDIC spent nearly $500 million on contracts, with the largest expenditures for IT and administrative support services. The FDIC was overseeing acquisitions on a contract-by-contract basis—rather than on a portfolio-wide basis—and it did not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency and did not maintain certain key data elements. FDIC contract oversight should also include consideration of supply chain risks.

Measuring Costs and Benefits of FDIC Regulations: The FDIC did not have a consistent process in place to determine when and how to conduct cost benefit analysis in order to ensure that the benefits of a regulation justified its costs. Further, the FDIC did not have criteria in place to distinguish among rules that were sufficiently "significant" to require cost benefit analysis. We also noted that conducting retrospective cost benefit analyses on existing rules would help the FDIC ensure that its rules were currently effective and achieved their intended objectives and outcomes.

Ongoing audit and evaluation reviews at the end of the reporting period were addressing such issues as the FDIC's readiness for crises, the FDIC's allocation and retention of safety and soundness examination staff, the FDIC's Anti-Sexual Harassment Program, and security of the FDIC's mobile devices, among others. These ongoing reviews are also listed on our website and, when completed, their results will be presented in an upcoming semiannual report.

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. An increased area of focus for our investigations has been partnering with other regulatory agencies to identify fraud in the guaranteed loan portfolios of FDIC-supervised banks. Such fraud schemes can affect the financial condition of banks and the financial services industry.

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 OIG Special Agents in Headquarters, Regional Offices, and the OIG's Electronic Crimes Unit. 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.

Wells Fargo Agrees to Pay $3 Billion to Resolve Criminal and Civil Investigations into Sales Practices Involving the Opening of Millions of Accounts Without Customer Authorization

On February 21, 2020, Wells Fargo & Company and its subsidiary, Wells Fargo Bank, N.A., agreed to pay $3 billion to resolve their potential criminal and civil liability stemming from a practice between 2002 and 2016 of pressuring employees to meet unrealistic sales goals, through a "cross-sell strategy" to sell existing customers additional products. The pressure faced under this sales practice led to thousands of employees providing millions of accounts or products to customers under false pretenses or without consent, often through falsifying bank records and identity theft.

As part of its agreements with various USAOs, the Commercial Litigation Branch of the Civil Division, and the Securities and Exchange Commission (SEC), Wells Fargo admitted that for years, it collected millions of dollar in fees and interest to which it was not entitled; harmed credit ratings of certain customers; and illegally misused customers' sensitive personal information, including customers' means of identification. The criminal investigation into false bank records and identity theft is being resolved with a deferred prosecution agreement in which Wells Fargo will not be prosecuted during the 3-year term of the agreement if it abides by certain conditions, including continuing to cooperate with further government investigations.

Responsible Agencies: FDIC OIG, FBI, Federal Reserve Board and Consumer Financial Protection Bureau OIG, Federal Housing Finance Agency OIG, and U.S. Postal Inspection Service. Prosecuted by the USAO, Central District of California.

Delhi Farmer Sentenced for Lying to Various Business and Government Entities to Steal Nearly $18 Million

On November 7, 2019, Thomas A. Dickerson of Delhi, Louisiana, was sentenced to 10 years in federal prison followed by 3 years of supervised release, and ordered to pay $18,048,304.71 in restitution to his victims, as a result of lying to more than seven financial institutions, insurance providers, and government entities in an effort to obtain over $18 million illegally.

According to documents and information presented at court, Dickerson was a Franklin Parish Louisiana farmer who, during the 2015 crop year, used at least 13 farming entities he was either a part of or was the sole owner of to certify farming acreage in Catahoula, Franklin, Tensas, Richland, Madison, and Morehouse parishes in Louisiana, as well as Ashley, Chicot, and Drew Counties in Arkansas. He applied for crop production and grain storage loans from AG Resource Management; farm operating loans from various FDIC-insured banking entities; credit from seed and chemical dealers such as Greenpoint AG, LLC and Jimmy Sanders Seed; advances on contracts with Kennedy Rice Dryers; insurance policies and claims from Producers Agriculture Insurance Company and CGB Insurance Company; and several marketing assistance loans from the Commodity Credit Corporation.

Dickerson lied on many of these applications in order to obtain loans and other compensation by overstating or understating the amount of crops produced, or claiming crops as collateral when he had already sold the crops or did not possess them.

Source: DOJ.
Responsible Agencies: FDIC OIG, U.S. Department of Agriculture OIG, and FBI.
Prosecuted by the USAO, Western District of Louisiana.

Former Trader for Major Multinational Bank Convicted for Price Fixing and Bid Rigging in Foreign Exchange (FX) Market

On November 20, 2019, Akshay Aiyer, a former executive director at a major multinational bank, was convicted for his participation in an antitrust conspiracy to manipulate prices for emerging market currencies in the global FX market.

From at least October 2010 through at least January 2013, Aiyer conspired 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.

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 also 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 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, FBI, DOJ Antitrust Division, and DOJ Criminal Division, Fraud Section. Prosecuted by the USAO, Southern District of New York.

Former Executives and Employees of Health Technology Start-Up Charged in a $1 Billion Scheme to Defraud Clients, Lenders, and Investors

On November 25, 2019, four former executives and two former employees of Outcome Health were charged for their alleged roles in a fraud scheme that targeted the company's clients, lenders, and investors, and involved approximately $1 billion in fraudulently obtained funds.

Rishi Shah, 33, of Chicago, the co-founder and chief executive officer of Outcome Health; Shradha Agarwal, 34, of Chicago, the president of Outcome Health; Brad Purdy, 30, of San Francisco, the chief operating officer and chief financial officer; and Ashik Desai, 26, of Philadelphia, the executive vice president of business operations and the chief growth officer of Outcome; were charged in a superseding indictment.

Kathryn Choi, 29, of New York, a senior analyst at Outcome; and Oliver Han, 29, of Chicago, an analyst at Outcome, were charged in an information filed.

The former executives and employees allegedly perpetrated a fraudulent scheme by selling clients advertising inventory the company did not have and then under-delivered on its advertising campaigns. Despite those under-deliveries, the company invoiced its clients as if it had delivered in full.

To conceal the under-deliveries, the former executives and employees allegedly falsified affidavits and proofs of performance to make it appear the company was delivering advertising content to the number of screens in its clients' contracts, and also inflated patient engagement metrics regarding how frequently patients engaged with Outcome's tablets. One of the employees also allegedly altered a number of studies that were presented to clients to make it appear that the campaigns were more effective than they actually were.

The under-deliveries resulted in a material overstatement of Outcome's revenue for 2015 and 2016. Purdy, Desai, Choi, and Han fabricated data to conceal the under-deliveries to get the outside auditor to sign off on the 2015 and 2016 revenue numbers. Outcome's executives used those inflated figures in the 2015 and 2016 audited financial statements to raise $110 million in debt financing in April 2016, $375 million in debt financing in December 2016, and $487.5 million in equity financing in early 2017.

Shah, Agarwal, and Purdy are each charged with various counts of mail fraud, wire fraud, and bank fraud. Purdy is also charged with one count of false statements to a financial institution, and Shah is also charged with two counts of transactions in criminal proceeds. Desai is charged with one count of wire fraud, and Choi and Han are each charged with one count of conspiracy to commit wire fraud.

Source: The FDIC's Division of Resolutions and Receiverships.
Responsible Agencies: FDIC OIG, with assistance from the U.S. Secret Service.
Prosecuted by the USAO, Northern District of Illinois.

Former Citizens Bank and Trust President, Co-Conspirators Involved In $5+ Million Fraud Scheme Sentenced to Prison, Ordered to Pay Back Millions

Between December 16, and December 17, 2019, three co-conspirators were sentenced for their role in a multi-million dollar scheme to defraud millions from Citizens Bank and Trust (CB&T), Eastman, Georgia.

McDonald Hardin, former president of CB&T, was sentenced to 60 months imprisonment, 3 years of supervised release, and ordered to pay $1,437,651.07 in restitution to CB&T and $1,900,000 in restitution to Progressive Insurance after pleading guilty to one count of conspiracy to commit bank fraud. Steve Stokeling was sentenced to 78 months of imprisonment, 5 years of supervised release, and ordered to pay $28,832.15 in restitution to CB&T after pleading guilty to one count of bank fraud. The third conspirator, Joseph Askew, was sentenced to 18 months of imprisonment, 1 year of supervised release, and ordered to pay $1,437,651.07 in restitution to CB&T and $120,765.10 in restitution to Progressive Insurance, after pleading guilty to one count of conspiracy to commit bank fraud.

Between 2008 and 2010, Hardin participated in a loan scheme designed to generate loan proceeds from fraudulent loans to Stokeling and Askew, their friends and family members, and borrowers recruited by Stokeling and Askew, who would sign loan documents without any expectation of receiving the loan proceeds. Hardin approved the loans and the bank would issue checks. The loan money was then distributed to various persons for personal use, and not used for the intended purposes of the loan. As a result of the scheme, CB&T was defrauded of $5,067,333.17.

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

Former Bank President Who Aided the Obstruction of an FDIC Examination Sentenced

On December 17, 2019, Cecil Capper, 74, from Marion, Iowa, was sentenced to 5 years' probation and ordered to pay more than $460,000 in restitution for aiding in the obstruction of an FDIC examination.

Information at sentencing showed that Capper worked as a bank president from 2009-2013, and that in December 2010, Capper prepared a handwritten memo and made an entry in the bank's computer system purporting to show that Capper's bank had assumed a $500,000 loan from another affiliated bank. Capper did so in order to aid in concealing underlying delinquent loans from FDIC scrutiny.

The bank ended up being unable to collect on the majority of the $500,000 loan, ultimately losing $462,304.84.

Source: DOJ, Criminal Fraud Section.
Responsible Agencies: FDIC OIG and FBI. Prosecuted by the USAO, Northern District of Illinois, and the DOJ, Criminal Fraud Section. The SEC is litigating the civil investigation.

Top Executives Plead Guilty to Participating in a Billion-Dollar Ponzi Scheme – the Biggest Criminal Fraud Scheme in the History of the Eastern District of California

On January 24, 2020, the owners of DC Solar, a Benicia-based company, pleaded guilty to charges related to a billion-dollar Ponzi scheme–the biggest criminal fraud scheme in the history of the Eastern District of California.

Jeff Carpoff, 49, of Martinez, pleaded guilty to conspiracy to commit wire fraud and money laundering. Paulette Carpoff, 46, pleaded guilty to conspiracy to commit an offense against the United States and money laundering.

According to documents presented at court, between 2011 and 2018, DC Solar manufactured mobile solar generator units, solar generators that were mounted on trailers that were promoted as able to provide emergency power to cell phone towers and lighting at sporting events. The defendants pulled off their scheme by selling solar generators that did not exist to investors, making it appear that solar generators existed in locations that they did not; creating false financial statements; and obtaining false lease contracts, among other efforts, to conceal the fraud. At least half of the approximately 17,000 solar generators claimed to have been manufactured by DC Solar, did not exist.

The government's investigation into this case has resulted in the largest criminal forfeiture in the history of the Eastern District of California with over $120 million in assets forfeited that will go to victims and $500 million that has been returned to the United States Treasury.

Four other defendants have also pleaded guilty to federal criminal charges related to the fraud scheme, and a seventh co-conspirator was scheduled to plead guilty in February.

Source: FBI and SEC.
Responsible Agencies: FDIC OIG, FBI, and Internal Revenue Service-Criminal Investigation. Prosecuted by the USAO, Eastern District of California, Sacramento.

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	Louisiana	Ohio
Arkansas	Maryland	Oklahoma
California	Massachusetts	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 Jersey	Virginia
Iowa	New York	Washington
Kansas	North Carolina	West Virginia
Kentucky	North Dakota	Wisconsin

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	Washington Field Office Financial Crimes Task Force; 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.
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.
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; High Intensity Financial Crime Area 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; 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 key 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 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.
- Welcomed the Comptroller of the Currency, Honorable Joseph M. Otting, in November to speak to OIG staff about his perspectives as an FDIC Director and his thoughts on the state of the banking industry today.
- Met with representatives from the International Monetary Fund (IMF) and discussed our work that was relevant to the topics that will be covered in the 2020 IMF Financial Sector Assessment Program (FSAP) review.
- Presented on the topics of OIG/Electronic Crimes Unit (ECU) capabilities and coordination, and developing a working relationship and information sharing, at the FDIC IT Examiner Conference in November.
- 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 routinely informed the Chairman and FDIC Director of such releases.
- Attended FDIC Board Meetings and certain other senior-level management meetings to monitor or discuss emerging risks at the Agency 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.

- 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 Committee, Investigations Committee, Professional Development Committee, Assistant Inspectors General (AIG) 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; hosting a meeting of the CIGIE Investigations Subcommittee; 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.
- Coordinated with the Government Accountability Office (GAO) on ongoing efforts related to the annual financial statement audits of the FDIC and the FDIC's Annual Report.
- Coordinated with OMB 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, and cyber fraud-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 certain investigative cases and related actions, in addition to posting our audits and evaluations.

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.
- Developed 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.

- Conducted training for OIG staff on Windows 10 as part of our ongoing IT Training efforts.
- 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 audits, evaluations, investigations, 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 several Special Agents in the OIG's Regional Offices.
- 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.

Exercising leadership skills and promoting teamwork.

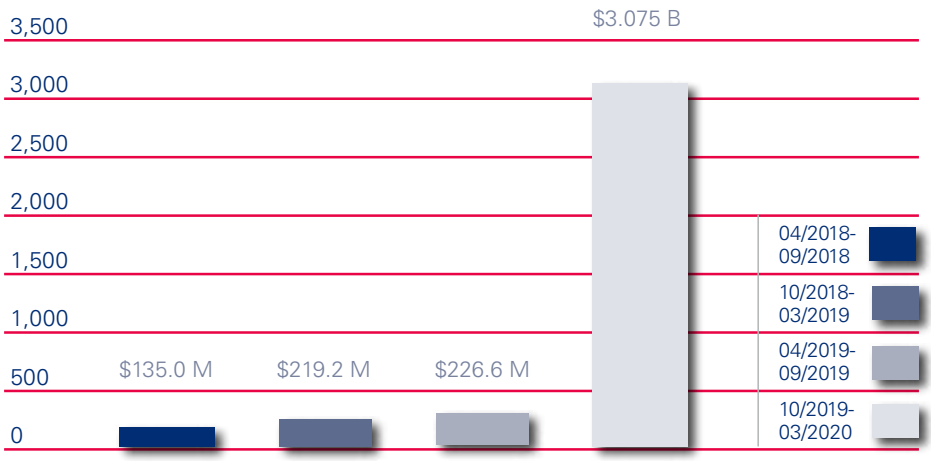
- Continued biweekly OIG senior leadership meetings to affirm the OIG's unified commitment to the FDIC OIG mission and to strengthen working relationships and coordination among all FDIC OIG offices.
- Supported efforts of the Workforce Council as it began its work to form "Tiger Teams" to solicit staff input on a variety of topics, including rewards and recognition and work/life balance.
- Continued discussions with our OIG culture facilitators as we continue to address employee engagement efforts in our Office.
- Offered a Lunch and Learn organized by our OIT to brief OIG staff about OIT's implementation plan; OIT's areas of expertise, and the upcoming projects in OIT for 2020.
- Convened an OIG-wide Town Hall Meeting in October, where the OIG held a facilitated discussion on Office culture and employee engagement initiatives.
- Held an OIG-wide Town Hall Meeting on March 30, where the OIG discussed the Coronavirus pandemic and its effects on our Office's work environment.
- Kept the Office informed about the OIG's vision and course of action for 2020 through a video that featured updates from each component office's executive or manager, and the OIG's Workforce Council.

- 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.
- Continued to support members of the OIG pursuing professional training and certifications to enhance the OIG staff members' expertise and knowledge.
- Held investigative training at the Federal Law Enforcement Training Center in Glynco, Georgia.
- Fostered a sense of teamwork and mutual respect through various activities of the OIG's Diversity and Inclusiveness (D&I) Working Group. These included welcoming members of the OIG staff to attend D&I meetings, and bi-monthly D&I Working Group updates in our newsletters to staff.
- Responded to suggestions received through the OIG Solutions Box, which provides all staff a mechanism to suggest positive improvements to the workplace, and developed an electronic portal on our Intranet site to increase transparency and update staff relating to the disposition of those suggestions.

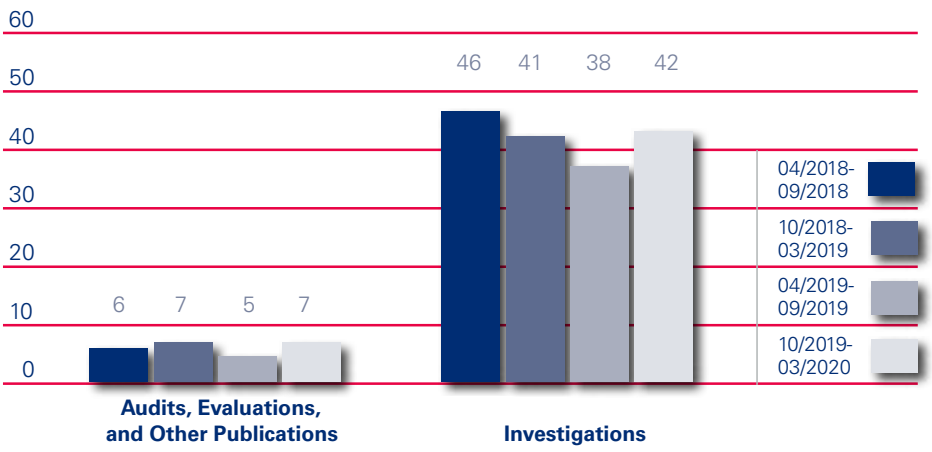
Cumulative Results (2-year period)

Nonmonetary Recommendations	
April 2018 - September 2018	29
October 2018 - March 2019	24
April 2019 - September 2019	24
October 2019 - March 2020	37

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.	25
Section 5(a)(1)	Significant problems, abuses, and deficiencies.	4-10
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies.	4-10
Section 5(a)(3)	Significant recommendations described in previous semiannual reports on which corrective action has not been completed.	26
Section 5(a)(4)	Matters referred to prosecutive authorities.	36
Section 5(a)(5)	Summary of each report made to the head of the establishment regarding information or assistance refused or not provided.	35
Section 5(a)(6)	Listing of audit, inspection, and evaluation reports by subject matter with monetary benefits.	33
Section 5(a)(7)	Summary of particularly significant reports.	4-10
Section 5(a)(8)	Statistical table showing the total number of audit, inspection, and evaluation reports and the total dollar value of questioned costs.	34
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.	34
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 • no establishment comment was received within 60 days of providing the report • there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.	 35 35 27-32
Section 5(a)(11)	Significant revised management decisions during the current reporting period.	35
Section 5(a)(12)	Significant management decisions with which the OIG disagreed.	35
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.	38-39

Section 5(a)(17)	Statistical tables showing, for the reporting period:	
	• number of investigative reports issued	36
	• number of persons referred to the DOJ for criminal prosecution	36
	• number of persons referred to state and local prosecuting authorities for criminal prosecution	36
	• number of indictments and criminal informations.	36
Section 5(a)(18)	A description of metrics used for Section 5(a)(17) information.	36
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.	36
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.	36
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.	36
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.	36

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.

Our Office reviewed and commented, as appropriate, on the following:

- A legislative proposal that would amend 5 U.S.C. 1213, or alternatively IG Act section 6, to allow an Inspector General to receive allegations referred by the Office of Special Counsel that involve an OIG.
- The "Oversight.gov Authorization Act of 2020:" To authorize the establishment and maintenance of a website and provide adequate financial resources for a more transparent Inspector General community.

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: (one recommendation from one report)

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 Organization's (CIOO) ongoing Enterprise 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.

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-16-001 **FDIC's Information Security Program – 2015** October 28, 2015	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. Overall, C&C concluded that the FDIC's information security program and practices were generally effective and noted several important improvements in the FDIC's information security program over the past year. However, C&C noted that the FDIC had not assessed whether Information Security Managers had requisite skills, training, and resources. Also, the FDIC had not always timely completed outsourced information service provider assessments or review of user access to FDIC systems. Other findings involved control areas of risk management and configuration management. The report contained six recommendations to improve the effectiveness of the FDIC's information security program controls and practices.	6	1	NA
AUD-17-001 **Audit of the FDIC's Information Security Program – 2016** November 2, 2016	The FDIC OIG engaged the professional services firm of 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 FISMA requirements, OMB policy and guidelines, and applicable National Institute of Standards and Technology standards and guidelines. However, C&C described security control weaknesses that impaired the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at elevated risk. C&C reported on 17 findings, of which 6 were identified during the current year FISMA audit and the remaining 11 were identified in prior OIG or 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.	6	1	NA

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
	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.			
AUD-18-001 **Audit of the FDIC's Information Security Program – 2017** October 25, 2017	The FDIC OIG engaged the professional services firm of C&C to conduct an audit to evaluate the effectiveness of the FDIC's information security program and practices. The audit included a review of selected security controls related to three general support systems, one business application, and the FDIC's risk management activities pertaining to four outsourced information service providers. As part of its work, C&C developed responses to security-related questions contained in the Department of Homeland Security's document, entitled *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V 1.0,* dated April 17, 2017 (the IG FISMA Reporting Metrics). C&C's report describes security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. C&C reported a total of 19 findings, of which 14 were identified during the current year FISMA audit and the other 5 were identified in prior reports issued by the OIG or the GAO. The report contained 18 recommendations addressed to the FDIC's Chief Information Officer that were intended to improve the effectiveness of the FDIC's information security program and practices.	18	4	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 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	2	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-19-001 **The FDIC's Information Security Program – 2018** October 25, 2019	The FDIC OIG engaged the professional services firm of C&C to audit the effectiveness of the FDIC's information security program and practices. C&C's report describes security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. In many cases, these security control weaknesses were identified by other ongoing OIG audits, or through security control assessments completed by the FDIC. Although the FDIC was working to address these previously identified control weaknesses, the FDIC had not yet completed corrective actions at the time of this audit. Accordingly, these security control weaknesses continued to pose risk to the FDIC. The report contained four new recommendations addressed to the CIO that were intended to improve the effectiveness of the FDIC's information security program and practices. These recommendations focused on improving controls in the areas of risk management, configuration management, and vulnerability scanning.	4	1	NA

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
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. 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.	7	4	$47,489
AUD-19-004 **Security Configuration Management of the Windows Server Operating System** January 16, 2019	The FDIC OIG audited the FDIC's security configuration management of the Microsoft Windows Server operating system. The FDIC uses this system to store and process a significant volume of sensitive information and support mission-critical functions. Accordingly, a service disruption to this system could impair the FDIC's ability to fulfill its mission of maintaining stability and public confidence in the Nation's financial system. The audit objective was to determine whether the FDIC established and implemented controls for managing changes to its Windows Server operating system that were consistent with Federal requirements and guidelines.	8	1	NA

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
	The FDIC established various controls to manage changes to its Windows Server operating system that were consistent with Federal requirements and guidelines. However, our audit identified findings with respect to (i) outdated policies and procedures for managing changes to the Windows Server operating system, (ii) a lack of independence of the organization that conducted security control assessments of the system, (iii) inadequate depth and coverage of security assessments, and (iv) inaccurate information in the system security plan. The report contained eight recommendations.			
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 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.	9	4	NA

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
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 the 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	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-20-002 December 18, 2019	Offsite Reviews of 1- and 2-Rated Institutions			
EVAL-20-003 February 4, 2020	Cost Benefit Analysis Process for Rulemaking			
Information Technology and Cybersecurity				
AUD-20-001 October 23, 2019	The FDIC's Information Security Program-2019			
AUD-20-002 October 30, 2019	The FDIC's Compliance with the Digital Accountability and Transparency Act of 2014			
AUD-20-003 December 18, 2019	The FDIC's Privacy Program			
Resource Management				
EVAL-20-001 October 28, 2019	Contract Oversight Management			
Totals for the Period		**$0**	**$0**	**$0**

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.	0	$0	$0
(i) dollar value of disallowed costs.	0	$0	$0
(ii) dollar value of costs not disallowed.	0	$0	$0
D. For which no management decision has been made by the end of the reporting period.	1	$47,489	$7,510
Reports for which no management decision was made within 6 months of issuance.	1	$47,489	$7,510

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 four recommendations more than 6 months old without management decisions. In our *Payments to Pragmatics, Inc.* report (AUD-19-003), dated December 10, 2018, we found that $47,489 (approximately 10 percent of labor charges we reviewed) were either not adequately supported 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. Both FDIC staff and Pragmatics personnel informed us that the nature of the work required access to the FDIC's network. We determined that the remaining $39,979 was unallowable because the work was performed off site (away from FDIC facilities). The FDIC's contract with Pragmatics required the contractor to perform all work at the FDIC's facilities, absent a site visit and approval by the FDIC to perform the work at an alternate location.

As of the end of the semiannual period, management had not made a management decision on four of the recommendations in the report. Specifically, we recommended that the Deputy to the Chairman and Chief Operating Officer: (1) determine the portion of the $7,510 in unsupported questioned costs that should be disallowed and recovered; (2) determine whether other labor charges billed by Pragmatics are unsupported and should be disallowed and recovered; (3) determine the portion of the $39,979 in unallowable questioned costs that should be disallowed and recovered; and (4) determine whether additional labor charges billed by Pragmatics for work conducted off site should be disallowed and recovered.

The FDIC informed us that the management decisions are delayed due to a review of voluminous material in order to determine appropriate labor charges. The FDIC collected information and has completed analysis to address all four recommendations as well as additional issues raised by the FDIC's Audit Committee. The FDIC is considering the results of the analysis and consulting with Chief Information Officer staff, and expects to have management decisions by April 30, 2020.

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	42
Number of Persons Referred to the Department of Justice for Criminal Prosecution	134
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	3
Number of Indictments and Criminal Informations	39

Description of the metrics used for the above information: Reports issued reflects case closing memorandums issued to FDIC management. With respect to the 134 referrals to DOJ, the total represents 112 individuals and 22 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

The FDIC OIG investigated alleged improprieties relating to the award of an IT security contract. The investigation uncovered information suggesting that a Senior IT Specialist involved in the award of the contract may have had an apparent conflict of interest. We referred the case to DOJ on February 28, 2019 and it was declined on that date. The OIG provided an investigative report to FDIC management for consideration. On February 11, 2020, FDIC management sent a letter to the Senior IT Specialist removing the employee from the employee's position and Federal service. Based on this action, the FDIC OIG closed its investigation.

Table XIII: Instances of Whistleblower Retaliation

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

Table XIV: Instances of Agency Interference with OIG Independence

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

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

During this reporting period, there were no evaluations or audits closed and not disclosed to the public. As noted in Table XII above, we conducted one investigation of a senior government employee and closed that investigation without disclosing it to the public at the time.

Appendix 2

Information on Failure Review Activity

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

FDIC OIG Review Activity for the Period October 1, 2019 through March 31, 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 of the end of the current reporting period, the FDIC OIG was conducting the following two Failed Bank Reviews. Results of those reviews will be included in an upcoming semiannual report.

Louisa Community Bank
Louisa, Kentucky

Closed:	October 25, 2019
Estimated Loss to the DIF:	$4.5 million

Ericson State Bank
Ericson, Nebraska

Closed:	February 14, 2020
Estimated Loss to the DIF:	$14.1 million

Appendix 3

Peer Review Activity

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

Definition of Audit Peer Review Ratings

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

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

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

Audit Peer Reviews

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

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

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

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

Inspection and Evaluation Peer Reviews

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

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

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

Investigative Peer Reviews

Quality assessment peer reviews of investigative operations are conducted on a 3-year cycle. Such reviews result in a determination that an organization is "in compliance" or "not in compliance" with relevant standards. These standards are based on Quality Standards for Investigations and applicable Attorney General Guidelines, and Section 6(e) of the Inspector General Act of 1978, as amended.

- The Department of the Treasury OIG conducted a peer review of our investigative function and issued its final report on the quality assessment review of the investigative operations of the FDIC OIG on May 9, 2019. The Department of the Treasury OIG reported that in its opinion, the system of internal safeguards and management procedures for the investigative function of the FDIC OIG in effect for the year ending October 31, 2018, was in compliance with quality standards established by CIGIE and the other applicable Attorney General guidelines and statutes noted above. These safeguards and procedures provided reasonable assurance of conforming with professional standards in the planning, execution, and reporting of FDIC OIG investigations and in the use of law enforcement powers.

Congratulations and Farewell

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

John Almand
Senior Audit Specialist

Matthew Bullwinkel
Special Agent

Patrick Collins
Special Agent

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

OVERSIGHT.GOV
ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE

PANDEMIC RESPONSE
ACCOUNTABILITY COMMITTEE

pandemic.oversight.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**