OIG

Office of Inspector General

Semiannual Report to the Congress

April 1, 2019 – September 30, 2019

FDIC

Federal Deposit Insurance Corporation

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 5,750 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured $7.7 trillion in deposits in 5,303 institutions, of which the FDIC supervised 3,418. The Deposit Insurance Fund balance totaled $107.4 billion as of June 30, 2019. Active receiverships as of September 30, 2019, totaled 252, with assets in liquidation of about $577.4 million.

Office of Inspector General

Semiannual Report to the Congress

April 1, 2019 – September 30, 2019

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 of April 1, 2019 through September 30, 2019. The work highlighted in this Report illustrates the broad range of our oversight responsibilities and the importance of our work for the agency, financial sector, policymakers, and the American people.

We issued several Audit and Evaluation reports during this Semiannual Report period, including on the FDIC's Physical Security Risk Management Process, Preventing and Detecting Cyber Threats, and the FDIC's Minority Depository Institution Program.

Our evaluation on Physical Security found that the FDIC had not established an effective physical security risk management process to ensure it met Interagency Security Committee standards. In our audit of Cyber Threats, we identified weaknesses that limited the effectiveness of the FDIC's firewalls and the tool it uses to detect potential cyber threats that may have bypassed the firewalls and other security controls. Finally, while the FDIC achieved its Minority Depository Institution Program goals, it had not assessed the effectiveness of certain key program activities.

Our reports contained 24 recommendations for improvement to the FDIC's programs and operations. We are closely monitoring the FDIC's progress in implementing these OIG recommendations and actions taken to address our recommendations.

In addition, the OIG conducted significant investigations into criminal and administrative matters involving complex multi-million-dollar schemes of bank fraud, embezzlement, money laundering, and other crimes committed by corporate executives, bank insiders, and financial professionals.

For example, the Chairman and Chief Executive Officer of an international pharmaceutical company, whose criminal actions caused losses of more than $100 million to a large Puerto Rican bank, was sentenced during the reporting period. He was sentenced to 30 years in prison and was ordered to pay more than $103 million to the FDIC as receiver for Westernbank. Also, an investment advisor was sentenced to 262 months' imprisonment for wire fraud and tax evasion, and ordered to pay $7.3 million in restitution to victims and $7.3 million to the United States. In another case, a former bank employee was sentenced to 60 months' imprisonment for stealing more than $1 million from an elderly bank customer.

Our investigations during this period resulted in 35 convictions, as well as fines, restitution orders, and forfeitures over $226 million. In addition, our cases led to 19 arrests and 41 indictments and informations.

I am grateful for the hard work and dedication of the women and men of the OIG as we carry out the mission of the OIG. Notably, our Office welcomed a new Deputy Inspector General, Gale Stone, in May 2019, and her assistance has been very valuable to me over the past several months.

We appreciate the continued support of Members of Congress and staff; the FDIC Chairman, Board, and other executive leaders; as well as our colleagues within the Inspector General (IG) community. We remain committed to serving the American people as a leader in the IG community.

Jay N. Lerner
Inspector General
October 31, 2019

Table of Contents

Acronyms and Abbreviations

C&C	Cotton & Company LLP
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIOO	Chief Information Officer Organization
CISA	Cybersecurity and Infrastructure Security Agency
D&I	Diversity and Inclusiveness
DIF	Deposit Insurance Fund
DNS	Domain Name System
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOJ	Department of Justice
EA	Enterprise Architecture
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FIRREA	Financial Institutions Reform, Recovery, and Enforcement Act of 1989
FISMA	Federal Information Security Modernization Act of 2014
FSOC	Financial Stability Oversight Council

GAO	Government Accountability Office
IG	Inspector General
IRS-CI	Internal Revenue Service-Criminal Investigation
ISC	Interagency Security Committee
IT	Information Technology
ITAS	Information Technology Application Services
MDI	Minority Depository Institution
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PAE	Office of Program Audits and Evaluations
SAR	Suspicious Activity Report
SBA	Small Business Administration
SIEM	Security Information and Event Management
TMPC	Top Management and Performance Challenge
USAO	U.S. 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 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.

30 and Thriving

The FDIC OIG's conference in July 2019 acknowledged the organizational history of our Office. The OIG has evolved from its earliest composition as a group of internal audit and investigative staff to an office now headed by a Presidentially appointed and Senate confirmed IG. A highly skilled staff of auditors, evaluators, attorneys, analysts, human resource specialists, information technology professionals, Federal law enforcement agents, and others carry out the mission of the OIG at the FDIC.

On March 14, 1989, an FDIC Board resolution recognized that the Inspector General Act Amendments of 1988 required the Corporation to establish an OIG with an IG who functions under the general supervision of the Chairman, and established that position as of April 17 of that year. Robert D. Hoffman was designated Acting IG and then IG. Mr. Hoffman retired in 1993 and James A. Renick was selected by FDIC Acting Chairman Andrew "Skip" Hove to serve as IG.

Left to right: IGs Jon T. Rymer, Jay N. Lerner, and Gaston L. Gianni, Jr.

In 1993, the Congress designated the IG position at the FDIC as a Presidential appointment, and Mr. Renick was named as Acting IG. On April 29, 1996, Gaston L. Gianni, Jr. became the FDIC's first IG appointed by the President. Jon Rymer was sworn in as the second Presidentially appointed IG on July 5, 2006 and resigned to become the Department of Defense IG on September 27, 2013. Fred W. Gibson, Jr. was named Acting IG following Mr. Rymer's departure and served in that capacity for 3½ years. On January 9, 2017, Jay N. Lerner was sworn in as the FDIC's third Presidentially appointed IG.

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

Overall Results (April 1, 2019 – September 30, 2019)	
Audit, Evaluation, and Other Products Issued	5
Nonmonetary Recommendations	24
Investigations Opened	35
Investigations Closed	38
OIG Subpoenas Issued	0
Judicial Actions:	
Indictments/Informations	41
Convictions	35
Arrests	19
OIG Investigations Resulted in:	
Fines	$5,000
Restitution	$216,357,592*
Asset Forfeitures	$10,263,098
Total	$226,625,690
Referrals to the Department of Justice (U.S. Attorneys)	53
Proposed Regulations and Legislation Reviewed	3
Responses to Requests Under the Freedom of Information/Privacy Act	7

*Of this total amount, $58,548,137 was ordered joint and several with other individuals sentenced during this reporting period, and $19,196,000 was ordered joint and several with an individual 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 two audits and two evaluations during this reporting period, as summarized below. These reports contained 24 nonmonetary recommendations. 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. The Enloe State Bank failed on May 31, 2019, causing estimated losses to the DIF of $27.6 million. We conducted a failed bank review of the institution during this reporting period, as discussed below and noted in Appendix 2.

Audits

Preventing and Detecting Cyber Threats

Our Office issued an audit report assessing the effectiveness of two security controls intended to prevent and detect cyber threats on the FDIC's network: Firewalls; and the Security Information and Event Management (SIEM) tool. The FDIC's firewalls and SIEM tool operate in concert with other network security controls as part of a defense-in-depth cybersecurity strategy.

The FDIC has deployed firewalls at the perimeter and interior of its network to control the flow of information into, within, and out of the network. These network firewalls use rules to enforce what traffic is permitted. The FDIC's SIEM tool operates to analyze network activity and detect indications of potential cyber threats that may have bypassed the firewalls and other security controls. The tool runs automated queries (known as "Use Cases") to identify events or patterns of activity that may indicate a cyber attack.

We identified weaknesses that limited the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats, including:

- The majority of firewall rules were unnecessary. Also, many firewall rules did not have sufficient justification. Several factors contributed to these weaknesses, including an inadequate firewall policy and supporting procedures, and an ineffective process for periodically reviewing firewall rules to ensure their continued need.

- Firewalls did not comply with the FDIC's minimally acceptable system configuration requirements. In addition, the FDIC did not update its minimum configuration requirements in a timely manner to address new security configuration recommendations by the National Institute of Standards and Technology (NIST).

- The FDIC did not always require administrators to uniquely identify and authenticate when they accessed network firewalls.

We found that the FDIC properly set up the SIEM tool to collect audit log data from key network information technology (IT) devices. In addition, the SIEM tool effectively formatted the data to allow for analysis of potential cyber threats. However, the FDIC did not have a written process to manage the ongoing identification, development, implementation, maintenance, and retirement of Use Cases for the SIEM tool.

We made 10 recommendations intended to strengthen the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats. The FDIC concurred with our recommendations.

The FDIC's Actions to Mitigate the Risk of Domain Name System Infrastructure Tampering

During this reporting period, our Office conducted an audit to determine whether the FDIC took responsive actions to address the requirements of Emergency Directive 19-01 to mitigate Domain Name System (DNS) infrastructure tampering.

On January 22, 2019, the U.S. Department of Homeland Security issued an Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*, to all Federal Executive Branch Departments and Agencies, following a series of computer security incidents referred to as "Domain Name System infrastructure tampering." DNS infrastructure tampering occurs when an attacker intercepts or redirects an organization's web or email traffic to a separate IT infrastructure that the attacker controls, which allows the attacker to inspect and manipulate the traffic, exposing the organization's sensitive information and allowing the attacker to disrupt critical operations or perpetrate other malicious activity.

The Directive required agencies, including the FDIC, to take four specific actions to mitigate the risk of DNS infrastructure tampering. Agencies had 10 business days to complete these actions. The following four actions had to be taken:

1. Audit DNS Records;
2. Change DNS Passwords;
3. Implement Multi-Factor Authentication; and
4. Monitor Certificate Transparency Logs.

In addition to these four steps, the directive required agencies to notify the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) with status and completion reports covering the four actions.

Our Office found that the FDIC took responsive actions to address the requirements in Emergency Directive 19-01, and completed these actions by the end of the 10 days as required in the Directive. The FDIC also provided CISA with timely status and completion reports as they related to the four items above. We did not make any recommendations to the FDIC.

Evaluations

FDIC's Physical Security Risk Management Process

We conducted an evaluation to determine the extent to which the FDIC's physical security risk management process met Federal standards and guidelines. We issued the results of that work during this reporting period.

The FDIC employs approximately 6,000 individuals and has about 3,000 contractor personnel who conduct their work at 94 FDIC-owned or leased facilities throughout the country. FDIC facilities house highly sensitive banking and personally identifiable information, mission-critical systems, and valuable equipment. The FDIC must ensure its employees, contractors, resources, and assets are safe and secure.

In 1995, the President issued an Executive Order that created the Interagency Security Committee (ISC). This Committee has issued Government-wide standards, policies, and best practices applicable to all buildings and facilities occupied by Federal employees for non-military activities. The ISC standards provide a structured methodology for helping to ensure the safety of employees, contractors, and facilities by assessing facility risk, assigning facility security levels, and determining whether implemented countermeasures effectively mitigate risk. The FDIC adopted the recommended minimum security standards issued by the ISC for all FDIC facilities where practical.

Our evaluation determined that the FDIC had not established an effective physical security risk management process to ensure that it met ISC standards and guidelines. While FDIC management has indicated that there have been no major incidents or threats to any FDIC facility over the past 10 years, we found that the FDIC's physical security risk management process needed improvement:

- The FDIC had not developed adequate policies and procedures, quality control standards, training requirements, or record keeping standards. FDIC officials responsible for the Physical Security Program had not emphasized compliance with the ISC standards, and instead placed priority attention on other security initiatives.

- The FDIC did not conduct key activities in a timely and thorough manner for determining facility risk level, assessing security protections in the form of countermeasures, and mitigating and accepting risk.

- The FDIC did not adequately address countermeasures or track recommendations for minimum security protections. At some facilities, these countermeasures remained outstanding for more than 4 years, and in some cases, the FDIC could not provide the resolution status of recommendations.

- In certain instances, the FDIC was not able to provide justification for significant expenditures for countermeasures beyond recommended security protections.

- The FDIC had not developed goals and performance measures to help ensure its physical security program was effective.

Our evaluation did not assess the safety of FDIC personnel and its facilities. Nevertheless, without a more robust physical security risk management process, the FDIC cannot be certain that it has taken appropriate and cost-effective measures commensurate with risk and aligned with ISC standards.

We made nine recommendations to address the weaknesses in the FDIC's physical security risk management process; the FDIC concurred with these recommendations. We believe that the planned corrective actions are significant undertakings by the Agency and, once implemented, are likely to achieve important improvements towards the efficiency and effectiveness of its risk management process for physical security.

Minority Depository Institution Program at the FDIC

Minority Depository Institutions (MDI) play a vital role in assisting minority and under-served communities and are resources to foster the economic viability of these communities. During this reporting period, we issued the results of our evaluation of the FDIC's MDI Program.

The FDIC considers an institution to be an MDI if it is a Federally-insured depository institution where a majority of a bank's voting stock is owned by minority individuals; or a majority of the institution's Board of Directors is minority and the institution serves a predominantly minority community.

The Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) required the Secretary of the Treasury to consult with the FDIC on methods for best achieving the five statutory goals aimed at preserving and promoting MDIs. In keeping with the requirements of FIRREA, the FDIC adopted an MDI Policy Statement describing its interpretation of ways to preserve and promote MDIs and implement the goals.

We concluded that the FDIC achieved its program goals as outlined in the MDI Policy Statement. That is, the FDIC took actions to preserve and promote MDIs, and preserve the minority character of MDIs; provided technical assistance to MDIs; encouraged the creation of new MDIs; and provided MDI training sessions, education, and outreach efforts.

Notwithstanding these efforts, we found that the FDIC did not evaluate the effectiveness of key MDI Program activities. Specifically, the FDIC did not assess the effectiveness of its supervisory strategies and MDI technical assistance. We also determined that the FDIC should further assess the effectiveness of its MDI training sessions, education, and outreach, including the benefit and value that they provide.

The FDIC also 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.

Our report contained five recommendations to improve the FDIC's MDI Program. FDIC management concurred with the recommendations.

Failed Bank Review

Failed Bank Review of The Enloe State Bank

We issued a memorandum report indicating that we would proceed with an in-depth review of why The Enloe State Bank in Cooper, Texas, failed in May 2019. According to a press release issued by the Texas Department of Banking, it was forced to close the bank due to insider abuse and fraud by former officers. The FDIC's Division of Finance estimated that the loss to the DIF as a result of the failure was $27.6 million, or 75 percent of the bank's $37.0 million in total assets. We determined that proceeding with an in-depth review of the loss was warranted given the extent of irregular loans and the extraordinarily high estimated loss rate. Our Office plans to complete the in-depth review within 6 months of announcing that engagement.

****

Ongoing Work

Ongoing audit and evaluation reviews at the end of this reporting period were addressing such issues as the FDIC's cost benefit analysis process for rulemaking, the FDIC's allocation and retention of safety and soundness examination staff, contract oversight management, the FDIC's Information Security Program, the FDIC's Anti-Sexual Harassment Program, and FDIC readiness for the next crisis, among others. These ongoing reviews are also listed on our website and, when completed, their results will be presented in an upcoming semiannual report.

CIGFO Issues TMPCs Facing Financial-Sector Regulatory Organizations

The Inspectors General within the Council of Inspectors General on Financial Oversight (CIGFO) report annually on the Top Management and Performance Challenges (TMPC) facing their respective Financial-Sector Regulatory Organizations. In July 2019, CIGFO issued its second report reflecting the collective input from the Inspectors General in CIGFO and identifying cross-cutting Challenges facing multiple Financial-Sector Regulatory Organizations:

- Enhancing Oversight of Financial Institution Cybersecurity
- Managing and Securing Information Technology at Regulatory Organizations
- Sharing Threat Information
- Ensuring Readiness for Crises
- Strengthening Agency Governance
- Managing Human Capital
- Improving Contract and Grant Management

It is important to address the Challenges in this report because financial-sector activities – such as consumer and commercial banking, and funding, liquidity and insurance services – were identified by the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, as National Critical Functions. Those functions are so vital to the United States that any disruption, corruption, or dysfunction would have a debilitating effect on U.S. security, the national economy, and/or public health and safety.

Although Financial-Sector Regulatory Organizations have individual missions, this report emphasizes the importance of addressing challenges holistically through coordination and information sharing. Considering issues on a whole-of-Government approach versus a siloed, agency-by-agency basis allows for more effective and efficient means to address Challenges through a coordinated approach.

By consolidating and reporting these Challenges, CIGFO aims to inform the Financial Stability Oversight Council, regulatory organizations, Congress, and the American public of the cross-cutting challenges facing the financial sector.

CIGFO Issues Audit of the Financial Stability Oversight Council's Monitoring of International Financial Regulatory Proposals and Developments

In May, CIGFO issued an audit of the Financial Stability Oversight Council's (FSOC) Monitoring of International Financial Regulatory Proposals and Developments.

The audit determined that FSOC had a process for monitoring international financial regulatory proposals and developments. All of FSOC's members or representatives who offered an opinion about FSOC monitoring described the monitoring process as adequate, while also offering suggestions for enhancing the process. The CIGFO working group that performed this audit encouraged FSOC to consider incorporating some of those suggestions into the monitoring, so long as those suggestions were consistent with FSOC's focus on identifying and addressing threats to the financial system.

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 Offices of Inspector General; 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. A recent 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 this reporting period. They are the result of efforts by FDIC 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.

Former Bank Employee Sentenced to 60 Months' Imprisonment for Stealing over $1 Million from Elderly Bank Customer

On September 19, 2019, Paola Gallego, of Round Rock, Texas, was sentenced to 5 years' imprisonment for stealing over $1 million from an elderly bank customer.

Beginning in April 2014, Gallego began servicing the Capital One accounts of an elderly couple and informed one of her victims that should the spouse die, another family member could take control of the $4.4 million in their joint bank account. In September 2016, the victim took $400,000 and opened a new account at Wells Fargo Bank with the help of Gallego. Gallego then used those funds on personal and family expenditures. When Wells Fargo closed the account on suspicions of elder abuse, Gallego and her victim opened another account at J.P. Morgan Chase. From October 14, 2016 until April 20, 2017, Gallego's victim withdrew $1.2 million from the joint Capital One account and was under the impression that Gallego would deposit the funds into their joint account at Chase. Instead, Gallego transferred the money into her own personal account and used the funds for personal expenses.

In addition to the 5-year sentence, Gallego was ordered to pay a monetary judgment forfeiture of $1.2 million and ordered to pay $1,403,979.13 in restitution to Capital One Bank, which had reimbursed the victims for their losses. She also will be placed on supervised release for 4 years after completing her sentence.

Responsible Agencies: *FDIC OIG, FBI, and Texas Department of Public Safety. Prosecuted by the USAO, Western District of Texas.*

Investment Advisor Sentenced to 262 Months' Imprisonment for Multi-Million Dollar Investment Fraud Scheme and Income Tax Evasion

On August 29, 2019, Treyton Thomas was sentenced to 262 months' imprisonment for wire fraud and 60 months' imprisonment for income tax evasion, to run concurrently.

Thomas was first charged with 21 counts of wire fraud, bank fraud, and money laundering in 2016, when it was discovered that he defrauded his father's used car warranty company, NC & VA Warranty of Roxboro, N.C.; several of its customers; his wife; and his father-in-law. Through the use of an online brokerage firm, he used the defrauded funds to conduct risky trades in the commodities and futures market and then concealed the scheme by providing victims and financial institutions with sales information and fabricated bank and brokerage statements. To obtain additional funds, Thomas then used the same false information and statements to defraud financial institutions out of $1.9 million in loan proceeds. He also spent more than $1.6 million to pay personal expenses.

In 2018, Thomas was then charged with six counts of income tax evasion for the calendar years 2010-2015 and two counts of failing to disclose his interest in and authority over foreign bank accounts. According to court evidence, the defendant failed to file income tax returns or pay taxes for 20 years, and he concealed his income through offshore entities in the Cayman Islands, British Virgin Islands, and Nevis. He also had employees from offshore corporation management companies act as his nominee in multiple business ventures. In addition, the defendant created "ghost" employees to make it seem as though he operated a large, successful investment fund. He used aliases or variations of his own name to conceal his identity.

He was ordered to pay approximately $7.3 million in restitution to the victims of the schemes, the Internal Revenue Service, and the USAO. Additionally, he had to forfeit $7.3 million to the United States.

Source: *USAO, Eastern District of North Carolina.*
Responsible Agencies: *FDIC OIG, Internal Revenue Service-Criminal Investigation (IRS-CI), and U.S. Secret Service. Prosecuted by the USAO, Eastern District of North Carolina.*

Former CEO and Chairman of Bankrupt Pharmaceutical Company Sentenced to 30 Years in Prison

Jack Kachkar, former Chief Executive Officer and Chairman of now-bankrupt Inyx Inc., a multinational pharmaceutical company, was sentenced on July 2, 2019, to 30 years in prison, followed by 5 years of supervised release for his role in a $100 million scheme to defraud Westernbank of Puerto Rico. The losses from the scheme led to the eventual insolvency and collapse of Westernbank. Kachkar was also ordered to pay $103,490,005 in restitution to the FDIC, as receiver for Westernbank.

Evidence presented at trial showed that Kachkar orchestrated the scheme to defraud Westernbank by causing Inyx employees to make tens of millions of dollars-worth of fake customer invoices payable by customers in multiple countries including the United Kingdom and Sweden. Those fake invoices were presented by the defendant to Westernbank to be valid. He also made false and fraudulent representations to Westernbank executives about purported and imminent repayments from lenders in other countries in order to convince Westernbank to continue lending money to Inyx.

Kachkar then made false and fraudulent representations to Westernbank executives stating that he had additional collateral, including mines in Mexico and Canada worth hundreds of millions of dollars, to persuade Westernbank to lend additional funds.

As a result of the scheme, Kachkar caused Westernbank to lend him approximately $142 million based on false and fraudulent invoices from customers. He used those funds for his own personal benefit.

Source: *The FDIC's Division of Resolutions and Receiverships.*
Responsible Agencies: *FDIC OIG. Prosecuted by the USAO, Southern District of Florida.*

District Man Sentenced to 10 Years in Prison for Multi-Million Dollar Fraud and Money Laundering Schemes

On June 21, 2019, Michael A. Orji of Washington, D.C., was sentenced to 10 years in prison for his role in at least seven fraud schemes affecting at least 10 victims, and resulting in more than $5.7 million in intended losses.

Orji pled guilty in October 2018 to one count of conspiracy to commit bank fraud and one count of conspiracy to commit money laundering. Orji was also ordered to pay restitution of $905,274.98 divided among five victims. He also agreed to forfeit $75,254 in previously seized funds and pay a forfeiture money judgment of $1,705,320.03.

According to a statement from Orji, from August 2015 - November 2017, he participated in an ongoing conspiracy to commit multiple financial frauds involving stolen checks and business email compromise schemes. He also laundered the proceeds through a network of fraudulent bank accounts, shell corporations, and co-conspirators in Washington, D.C. and other areas.

During the course of the scheme, Orji participated in at least seven bank fraud schemes involving 10 victims and 15 fraudulent accounts that were opened and controlled by the defendant under a false identity. As a result of the scheme, losses resulted in $905,274.98 and there was $5,717,596.23 in intended losses.

The victims of his scheme included: a public school system, a medical center, small-and-medium sized companies, an individual who had called the bank to take precautions before an international trip, an individual attempting to buy a home, and an individual saving for retirement.

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

Bank Fraud Schemers Sentenced to Prison and Ordered to Pay $14.3 Million in Restitution

On April 5, 2019, Charnpal Ghuman and Aga Khan, two business partners from Bloomingdale, Illinois, were sentenced for their role in a bank fraud scheme and obtaining fraudulent loans from American Enterprise Bank.

From 2006 to 2009, Ghuman and Khan flipped gas stations by purchasing them and re-selling them to buyers who the defendants knew were not qualified to obtain bank financing. The duo arranged for financing of the buyers through falsified loan applications through American Enterprise Bank loans. The two defendants also solicited inside help from an accountant and a loan officer inside the bank.

Over the course of the scheme, Ghuman and Khan obtained more than $40 million in loan proceeds. The two business partners were ordered to jointly pay $9,843,899 in restitution, while also receiving individual sentences.

Ghuman was sentenced to 5 years and 6 months in prison, and ordered to pay an additional $2 million owed personally, and also received a concurrent sentence of 3 years in prison and ordered to pay an additional $1,952,653 to the Internal Revenue Service after pleading guilty to filing a false tax return.

Khan was sentenced to 3 years in prison and was ordered to pay restitution of $10,843,899, of which $1 million is owed personally and the remainder is owed jointly with Ghuman.

The loan officer in the case, Akash Brahmbhatt, was sentenced to 3 years in prison and ordered to pay restitution of $10,843,899, of which $1 million is owed personally and the remainder owed jointly with Ghuman.

Shital Mehta, the accountant in the case, was sentenced to one year and one day in prison and owes $500,000 in restitution personally.

Source: *Request for assistance from the FBI and Small Business Administration (SBA) OIG.*
Responsible Agencies: *FDIC OIG, SBA OIG, FBI, and IRS-CI. Prosecuted by the USAO, Northern District of Illinois.*

Former Bank Executive Found Guilty in $15 Million Construction Loan Fraud Scheme

On August 19, 2019, a former Kansas bank executive was found guilty of four counts of bank fraud and two counts of making false statements.

According to evidence presented at trial, Troy A. Gregory, during his time as a bank executive and loan officer, had made millions of dollars in loans to a group of borrowers who struggled to pay off the loans. In 2007, the defendant began making a $15.2 million construction loan, shared by his own bank and 26 other Kansas banks, to those same borrowers, to build an apartment complex.

Throughout the scheme, Gregory made and caused others to make false statements to banks about the strength of the borrowers, the debt status of the apartment property, and the existence of approximately $1.7 million in certificates of deposit for collateral on the loan, all to get the loan approved.

As evidence showed, instead of using the loan to build the apartment complex, the former bank executive diverted over $1 million of the loan to pay for part of the certificates of deposit pledged as collateral, pay off debt on the apartment property, and make payments on unrelated loans.

As a result of the scheme, the banks ultimately wrote off millions of dollars on the $15.2 million construction loan. Sentencing is scheduled for January 28, 2020.

Source: *IRS-CI.*
Responsible Agencies: *FDIC OIG, IRS-CI, FBI, Federal Housing Finance Agency OIG, and Federal Reserve Board OIG. Prosecuted by the Securities and Financial Fraud Unit, Fraud Section, Department of Justice.*

Ex-Bank Executive Sentenced to More than 5 Years in Prison for Loan Fraud

On May 20, 2019, the former chief marketing officer at the now-failed Mirae Bank was sentenced to 70 months in federal prison and ordered to pay $7,519,084 for his role in a scheme which caused Mirae Bank to issue more than $15 million in fraudulent loans.

From 2005 until 2007, Ataollah Aminpour represented himself as a successful business man who could help people obtain financing for gas station and car wash businesses. He used his role as a senior bank executive to submit and cause others to submit false information about the true purchase price of the business and also about the assets of the borrowers and the finances of the business that was purchased. Aminpour also had the borrowers transfer money into escrow accounts so that it would falsely appear to the bank that borrowers were making large down payments. This allowed borrowers to acquire businesses with little to no money down and allowed Aminpour to earn commissions and misappropriate the excess loan proceeds for himself. Aminpour admitted that six different loan applications with false statements, totaling $16.7 million, were submitted between 2005 and 2007.

According to court documents, Aminpour also referred about $150 million in loans to Mirae Bank and those loans largely contributed to the bank's collapse in 2009.

The FDIC and Wilshire Bank, which acquired Mirae's assets after its collapse, suffered more than $33 million in losses combined as a result of the ex-bank executive's scheme.

Source: *The FDIC's Division of Resolutions and Receiverships and Division of Risk Management Supervision.*
Responsible Agencies: *FDIC OIG, FBI, Special IG for the Troubled Asset Relief Program, and Federal Housing Finance Agency OIG. Prosecuted by the USAO, Central District of California.*

Farmer Pleads Guilty to Making False Statements to the Commodity Credit Corporation

On July 15, 2019, Thomas Dickerson pleaded guilty to lying to over seven financial institutions, insurance providers, and government entities in order to obtain almost $17 million.

During the 2015 crop year, Dickerson used at least 13 farming entities he owned or was a part of to certify farming acreage in multiple parts of Louisiana and Arkansas. During this time, he also applied for crop production and grain storage loans from AG Resource Management, farm operating loans from 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 by overstating or understating the amount of crops produced or using crops as collateral when he had already sold the crops or did not possess them. During the course of his scheme, Dickerson stole $16,985,409.71. Dickerson faces up to 10 years in prison, 3 years of supervised release, restitution, and a $10,000 fine.

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

Former Iowa Bank Vice President Sentenced for Obstructing an FDIC Examination

On June 13, 2019, Martin J. Smith, former vice president of Center Point Bank & Trust, Center Point, Iowa, was sentenced to 12 months and one day in federal prison followed by 3 years of supervised release. He was ordered to pay a $100 special assessment fine and $1,270,132.97 in restitution in connection with his prior guilty plea to obstructing an examination of a financial institution.

From in or about 2009 and continuing until in or about 2012, the former bank vice president abused his position as a loan officer, vice president and board member at the bank to extend loans to small businesses beyond legal lending limits, issued and extended loans without the knowledge of the loan committee, and falsified bank records to mask the actual condition and status of these credit relationships. Smith also performed loan file maintenance in the core processing system to suppress problem loans from appearing on monitoring reports to the bank's Board or regulators. In addition, during the course of an FDIC examination, Smith created a fictitious participation agreement falsely showing that a non-performing loan, issued in excess of state lending limits, had been syndicated with an affiliated bank, and then presented the backdated participation agreement to FDIC bank examiners in an attempt to evade discovery.

Source: *The FDIC's Division of Risk Management Supervision.*
Responsible Agencies: *FDIC OIG and U.S. Secret Service. Prosecuted by the USAO, Northern District of Iowa.*

Strong Partnerships with Law Enforcement Colleagues

The OIG has partnered with various U.S. Attorneys' Offices 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 U.S. Attorneys' Offices 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 this reporting period, we partnered with U.S. Attorneys' Offices in the following areas: Alabama, Arkansas, California, Colorado, District of Columbia, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Puerto Rico.

We also worked closely with the Department of Justice; FBI; other OIGs; other Federal, state, and local law enforcement agencies; and FDIC Divisions and Offices as we conducted our work during this 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 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; Eastern District of New York SAR Meeting Group; 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 BSA 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; Maryland Association for Bank Security; International Association of Financial Crimes Investigators.
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.
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.
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.
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; Hurricane Harvey Working Group.
Electronic Crimes Unit	Washington Metro Electronic Crimes Task Force; High Technology Crime Investigation Association; Cyberfraud Working Group; Council of the Inspectors General on Integrity and Efficiency Information Technology Subcommittee; National Cyber Investigative Joint Task Force; FBI Washington Field Office Cyber Task Force.

Other Key Priorities

In addition to the audits, evaluations, investigations, and other reviews conducted during this 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 some of the OIG's key stakeholders, including the United States Attorney for the District of Maryland and FDIC executives as Keynote Speakers at the OIG All-Hands conference in July.
- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
- Informed stakeholders about the impact of our investigations at the FDIC Accounting and Auditing Conference in September through presentations led by members of our Office of Investigations.
- 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 U.S. Attorneys' Offices 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 Corporation and tailor OIG work accordingly.

- Maintained congressional working relationships by communicating with various Committee staff on issues of interest to them; providing them our semiannual report to the Congress; notifying interested congressional parties regarding the OIG's completed audit and evaluation work; monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the FDIC's Office of Legislative Affairs on any Congressional correspondence pertaining to the OIG.

- 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; commenting on various legislative matters through CIGIE's Legislation Committee; and hosting a meeting for the IG community's AIGs for Management.

- Participated on 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. Contributed to CIGFO's joint assignment on the Financial Stability Oversight Council's Monitoring of International Financial Regulatory Proposals and Developments. Provided input to the CIGFO Annual Report and coordinated issuance of the Top Management Challenges Facing Financial-Sector Regulatory Organizations.

- Coordinated with the Government Accountability Office (GAO) on ongoing efforts related to the annual financial statement audit of the FDIC and the FDIC's Annual Report, including meeting with GAO staff to share views on the risk of fraud at the FDIC.

- Coordinated with the Office of Management and Budget to address budget matters of interest.

- Worked closely with representatives of the DOJ, including the Main Justice Department, FBI, and U.S. Attorneys' Offices, 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.

- Continued our outreach efforts by sharing the findings in our report on *Preventing and Detecting Cyber Threats* during a radio interview.

- 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.

- Developed the OIG strategic plan which highlights the goals of the Office as we look to promote efficiency and effectiveness at the FDIC and maximize performance of our operations, and the objectives needed to meet our goals.

- Continued efforts by the OIG's Office of Information Technology to coordinate a strategic approach to facilitate the integration of technology in OIG processes. This group is responsible for the OIG's enterprise architecture, and IT governance and related policies and procedures.

- Conducted training for OIG staff on Basic Cyber Hygiene as part of our ongoing Security Training efforts.

- Took steps to coordinate with FDIC officials on Emergency Preparedness for the OIG, including plans for emergency notifications and continuity of operations in the event of unforeseen circumstances. Tested our emergency alerts system as part of our Emergency Preparedness efforts.

- Relied on the OIG's General Counsel's Office to ensure the Office complied with legal and ethical standards, rules, principles, and guidelines; provide legal advice and counsel to teams conducting audits and evaluations; and support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.

- Continued to review and update a number of OIG internal policies related to audit, evaluation, investigation, management operations, and administrative processes of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the office.

- Carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. In addition to a new Deputy IG, positions filled during the reporting period included several Auditors, and Special Agents in the OIG's Regional Offices and Electronic Crimes Unit.

- 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, track, and control OIG spending, with particular attention to expenses involved in procuring equipment, software, and services to improve the OIG's IT environment.

Exercising leadership skills and promoting teamwork.

- Welcomed a new Deputy Inspector General to our staff.
- Held an FDIC OIG All-Hands conference which featured leadership panels representing both the current and future leaders in our organization.
- Continued biweekly OIG senior leadership meetings to affirm the OIG's unified commitment to the FDIC IG mission and to strengthen working relationships and coordination among all FDIC OIG offices.
- Supported efforts of the IG Advisory Council, now known as the Workforce Council, a cross-cutting group of OIG staff whose mission is to monitor FDIC OIG culture and morale, and make and track recommended improvements; and recruited new members to join the Council.
- Leveraged the OIG's Data Analytics capabilities to assist audit and evaluation staff and improve the overall efficiency and effectiveness of the OIG's audit and evaluation assignments.
- Kept OIG staff informed of Office priorities and key activities through regular meetings among staff and management, bi-weekly updates from senior management meetings, and issuance of OIG newsletters.
- Offered multiple POWER Lunch and Learn sessions to all OIG staff to enhance their knowledge of such areas as the FDIC's Worklife and retirement program, the impact of mentoring, and the impact of recent investigation accomplishments in our Office.
- Enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities.
- Carried out monthly coordination meetings for audit, evaluation, and investigation leadership to better communicate, coordinate, and maximize the effectiveness of ongoing work.
- Acknowledged individual and group accomplishments through an ongoing awards and recognition program, and an awards ceremony at the OIG All-Hands conference.

- Continued to support members of the OIG pursuing professional training and certifications or attending graduate banking school programs to enhance the OIG staff members' expertise and knowledge.

- Sponsored training sessions during our OIG All-Hands conference on the topics of adapting to change, effective listening, and building trust.

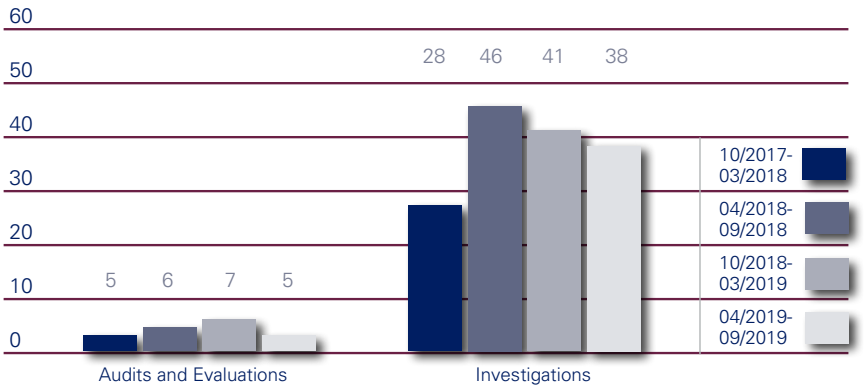
- Fostered a sense of teamwork and mutual respect through various activities of the OIG's Diversity and Inclusiveness (D&I) Working Group. These included an interactive diversity collage banner at our OIG Conference, a D&I update and activity at our OIG conference, a training session about generational diversity, 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.

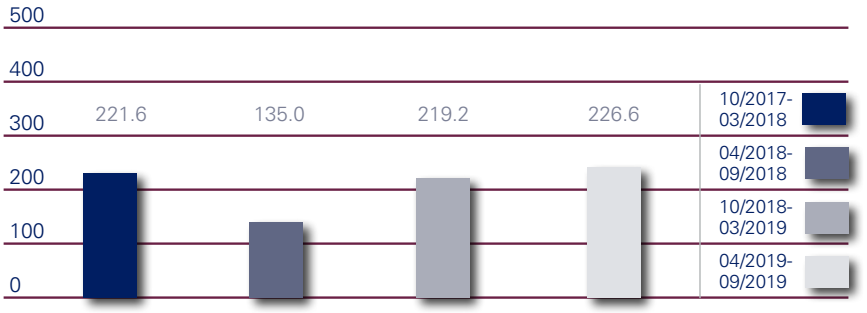
Cumulative Results (2-year period)

Nonmonetary Recommendations	
October 2017 – March 2018	33
April 2018 – September 2018	33
October 2018 – March 2019	24
April 2019 – September 2019	24

Products Issued and Investigations Closed



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



Reporting Requirements

Index of Reporting Requirements - Inspector General Act of 1978, as amended

Reporting Requirements	Page
Section 4(a)(2) Review of legislation and regulations.	35
Section 5(a)(1) Significant problems, abuses, and deficiencies.	6-14
Section 5(a)(2) Recommendations with respect to significant problems, abuses, and deficiencies.	6-14
Section 5(a)(3) Significant recommendations described in previous semiannual reports on which corrective action has not been completed.	36
Section 5(a)(4) Matters referred to prosecutive authorities.	50
Section 5(a)(5) Summary of each report made to the head of the establishment regarding information or assistance refused or not provided.	49
Section 5(a)(6) Listing of audit, inspection, and evaluation reports by subject matter with monetary benefits.	46
Section 5(a)(7) Summary of particularly significant reports.	6-14
Section 5(a)(8): Statistical table showing the total number of audit, inspection, and evaluation reports and the total dollar value of questioned costs.	47
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.	48
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	49
• no establishment comment was received within 60 days of providing the report to management	49
• there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.	37-45
Section 5(a)(11) Significant revised management decisions during the current reporting period.	49

Reporting Requirements (continued)	Page
Section 5(a)(12) Significant management decisions with which the OIG disagreed.	49
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.	52
Section 5(a)(17): Statistical tables showing, for the reporting period: • number of investigative reports issued • number of persons referred to the DOJ for criminal prosecution • number of persons referred to state and local prosecuting authorities for criminal prosecution • number of indictments and criminal Informations.	50
Section 5(a)(18) A description of metrics used for Section 5(a)17 information.	50
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.	50
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.	50
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.	50
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.	50

Appendix 1

Information Required by the Inspector General Act of 1978, as Amended

Review of Legislation and Regulations

The FDIC OIG's review of legislation and regulations during the past 6-month period involved continuing efforts to monitor and/or comment on enacted law or proposed legislative matters. In March 2019, Inspector General Lerner became Vice Chair of the Council of the Inspectors General on Integrity and Efficiency Legislation Committee. Much of the FDIC OIG's activity reviewing legislation and regulations occurs in connection with that Committee.

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

- A draft amendment to H.R. 1847, *Inspector General Protection Act*, which would amend the Vacancies Act to restrict who may be appointed as an Acting IG.
- A views letter sent by CIGIE regarding H.R. 2500, the *National Defense Authorization Act*. This letter related to the requirement for IGs to disclose the names of subjects of investigations who are in the Senior Executive Service or military officers in the grade of 0-7 and above.
- Draft *Whistleblower Protection Improvement Act* of 2019.

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

This table shows the corrective actions management has agreed to implement but has not completed, along with associated monetary amounts. In some cases, these corrective actions are different from the initial recommendations made in the audit 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 Control, 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: (two recommendations 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.

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

Report Number, Title, and Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
Management Action in Process		
AUD-18-004 **The FDIC's Governance of Information Technology Initiatives** July 26, 2018	**3***	The Chief Information Officer Organization (CIOO) will complete the target state architecture and associated roadmaps and align these enterprise architecture (EA) components with the FDIC's Information Technology (IT) Modernization Plan. Specifically, the IT Modernization Plan will be used to: update and replace the EA Blueprint, establish a target state for people, processes, and technology; define a 5-year execution timeframe and implementation roadmaps with required IT projects and cost estimates to migrate from the current state to the target state architecture; and identify human capital needs, including resources to achieve the target state architecture.
	7	As part of the CIOO's 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.

*The OIG has not completed the evaluation of management's actions in response to the OIG's recommendation.

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods

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

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-17-007 **Controls over Separating Personnel's Access to Sensitive Information** September 18, 2017	The FDIC experienced a number of data breaches in late 2015 and early 2016 that involved employees who were exiting the Corporation. In response, the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs requested that the FDIC OIG examine issues related to the FDIC's policies governing departing employees' access to sensitive financial information. The OIG conducted an evaluation to determine the extent to which the FDIC had established controls to mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel. While the FDIC had established and implemented various control activities, we found that there were weaknesses in the design of certain controls, Division and Office records liaisons were not always following procedures, and opportunities existed to strengthen the pre-exit clearance process. As designed, the program controls did not provide reasonable assurance that the pre-exit clearance process would timely or effectively identify unauthorized access to, or inappropriate removal and disclosure of, sensitive information by separating employees. We noted that separating contractor employees (contractors) may present greater risks than separating FDIC employees. We found several differences between the pre-exit clearance process for FDIC employees and contractors that increased risks related to protecting sensitive information when contractors separated. We also found that the FDIC was not consistently following its pre-exit clearance procedures with respect to separating contractors, and we identified several opportunities for strengthening the contractor pre-exit clearance process. The report contained 11 recommendations to provide the FDIC with greater assurance that its controls mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel.			

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-18-001 **Audit of the FDIC's Information Security Program – 2017** October 25, 2017	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (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. 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 Government Accountability Office. 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	5	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-18-004 **The FDIC's Governance of Information Technology Initiatives** July 26, 2018	Federal statutes and Office of Management and Budget policy require federal agencies to establish and implement fundamental components of information technology (IT) governance. These components include IT strategic planning, which defines the overall direction and goals for the agency's IT program, and an enterprise architecture, which describes the agency's existing and target architecture and plan to achieve the target architecture. The OIG conducted an audit to identify key challenges and risks that the FDIC faced with respect to the governance of its IT initiatives. 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.	8	3	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
EVAL-18-004 **Forward-Looking Supervision** August 8, 2018	The FDIC adopted a risk-focused supervision program in 1997, and in 2011, the FDIC implemented a Forward-Looking Supervisory initiative as part of its risk-focused supervision program. The goals of this supervisory approach are to identify and assess risk before it impacts a financial institution's financial condition and to ensure early risk mitigation. The OIG conducted an evaluation to determine whether the Forward-Looking Supervision approach achieved its outcomes–the Division of Risk Management Supervision pursued supervisory action upon identifying risks and the financial institutions implemented corrective measures. We found that the FDIC did not have a comprehensive policy guidance document on Forward-Looking Supervision. In addition, we identified instances in which examiners did not always document certain Forward-Looking Supervision concepts consistent with examiner guidance, when planning an examination and when reporting examination results. The report contained four recommendations to improve implementation of Forward-Looking Supervision.	4	1	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-19-001 **The FDIC's Information Security Program – 2018** October 25, 2019	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct an audit to evaluate 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 Chief Information Officer 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	2	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-19-002 **Controls Over System Interconnections with Outside Organizations** December 4, 2018	The FDIC exchanges significant amounts of data with outside organizations, including Federal agencies and non-governmental entities, through system interconnections. Such data includes personally identifiable information, confidential bank examination information, and sensitive financial data. The National Institute of Standards and Technology (NIST) has defined a lifecycle framework to assist federal agencies in managing and securing their interconnected systems. The NIST framework consists of four phases: planning, establishing, maintaining, and terminating interconnections. The OIG conducted an audit to assess the FDIC's controls for managing system interconnections with outside organizations. Although the FDIC issued certain policies, procedures, and templates for establishing system interconnections, we identified control weaknesses in each of the four phases of the NIST lifecycle framework. We also noted that the FDIC should establish policies and procedures to govern the secure transfer of data outside of the FDIC using technologies for data exchange that do not meet NIST's definition of a system interconnection. The report contained seven recommendations to strengthen controls related to the management of the FDIC's system interconnections.	7	3	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-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

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-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. 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.	8	3	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-19-002 September 24, 2019	*Minority Depository Institution Program at the FDIC*			
Information Technology and Cybersecurity				
AUD-19-005 May 28, 2019	*Preventing and Detecting Cyber Threats*			
AUD-19-006 September 24, 2019	*The FDIC's Actions to Mitigate the Risk of Domain Name System InfrastructureTampering*			
Resource Management				
EVAL-19-001 April 9, 2019	*The FDIC's Physical Security Risk Management Process*			
Totals for the Period		**$0**	**$0**	**$0**

Other products issued:

- *Failed Bank Review:*
  The Enloe State Bank, Cooper, Texas (FBR-19-001)
  September 23, 2019

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 had 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 is performing additional and more in-depth analysis of the charges, and then plans to pursue negotiations with the contractor. The FDIC plans to have management decisions by March 31, 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	38
Number of Persons Referred to the Department of Justice for Criminal Prosecution	53
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	0
Number of Indictments and Criminal Informations	41

Description of the metrics used for the above information: Reports issued reflects case closing memorandums issued to FDIC management. With respect to the 53 referrals to the Department of Justice, the total represents 51 individuals and 2 business entities. Our total indictments and criminal informations includes indictments, informations, and superseding indictments, as applicable.

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

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

Table XIII: Instances of Whistleblower Retaliation

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

Table XIV: Instances of Agency Interference with OIG Independence

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

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

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

Appendix 2

Information on Failure Review Activity (required by the Dodd-Frank Wall Street Reform and Consumer Protection Act)

FDIC OIG Review Activity for the Period April 1, 2019 through September 30, 2019 (for failures that occur on or after January 1, 2014 causing losses to the Deposit Insurance Fund of less than $50 million)

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

The FDIC OIG issued a Failed Bank Review memorandum on September 23, 2019, regarding our intent to conduct an in-depth review of The Enloe State Bank, located in Cooper, Texas. According to the Texas Banking Department, it was forced to close the bank on May 31, 2019, due to insider abuse and fraud by former officers. The FDIC estimated a loss to the DIF of $27.6 million. We plan to complete the in-depth review within 6 months of announcing that engagement.

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.

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.

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.

- The U.S. Railroad Retirement Board OIG conducted a peer review of the FDIC OIG's audit organization and issued its system review report on November 14, 2016. In the Railroad Retirement Board OIG's opinion, the system of quality control for our audit organization in effect for the year ending March 31, 2016, had been suitably designed and complied with to provide our office with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. We received a peer review rating of pass.

- The report's accompanying letter of comment contained recommendations that, while not affecting the overall opinion, were designed to further strengthen the system of quality control in the FDIC OIG Office of Audits and Evaluations.

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 Office of Inspector General, the U.S. Department of Education Office of Inspector General, and the U.S. Nuclear Regulatory Commission Office of Inspector General.

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 contributions to the FDIC OIG over the years, congratulate them on their Federal service, and wish them well in future endeavors.

David L. Anderson
Special Agent in Charge, Office of Investigations, Kansas City Region.

Michael Wixted
Special Agent, Office of Investigations, San Francisco Region.

****

Stephen Beard
Deputy Inspector General for Strategy and Performance.

During this reporting period, Stephen Beard left the FDIC OIG to become a Deputy Director in the Division of Administration at the FDIC. Steve served as the Deputy Inspector General for Strategy and Performance for 2½ years, and has served in numerous other leadership positions in the FDIC OIG. He was central in leading the OIG's Material Loss Reviews during the most recent financial crisis. The FDIC OIG wishes him continued success in his new role.

Keep Informed

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

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

OIG HOTLINE

The Office of Inspector General 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.

DESIGN: FDIC/DOA/CSB/GRAPHIC DESIGN AND PRINTING UNIT

FDIC-040-2019