Semiannual Report to the Congress

APRIL 1, 2017 – SEPTEMBER 30, 2017

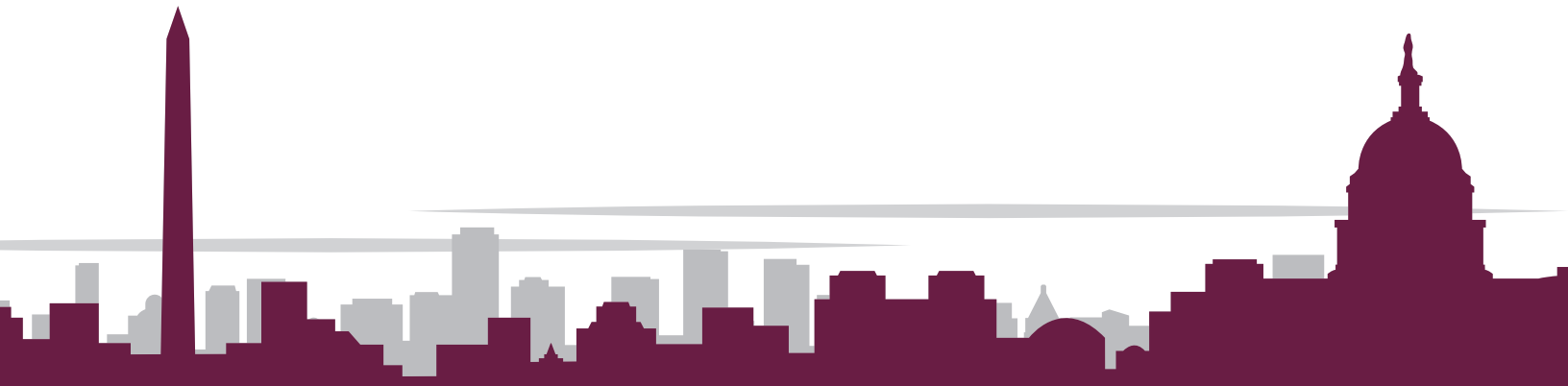
FDIC

Federal Deposit Insurance Corporation

Under the Inspector General Act of 1978, as amended, the Federal Deposit Insurance Corporation Office of Inspector General (FDIC OIG) is responsible for providing independent oversight 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 5,900 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured more than $7.0 trillion in deposits in 5,787 institutions, of which the FDIC supervised 3,711. The Deposit Insurance Fund balance totaled $87.6 billion as of June 30, 2017. Receiverships under FDIC control as of October 31, 2017, totaled 364, with about $4.6 billion in assets.



Office of Inspector General

Semiannual Report to the Congress

April 1, 2017 – September 30, 2017

Federal Deposit Insurance Corporation

Inspector General's Statement

I am pleased to submit the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) Semiannual Report for the period April 1, 2017 through September 30, 2017. The work highlighted in this Report illustrates the broad range of our oversight responsibility and the importance of our work for the FDIC, financial sector, and American people.

During the reporting period, we issued six audit and evaluation reports. These reports involved a variety of issues affecting the agency, including:

- Response to data breaches of Personally Identifiable Information (PII);
- Controls over separating employees and their access to sensitive information;
- Material Loss Review regarding the causes of failure and FDIC supervision of Seaway Bank and Trust Company; and
- Evaluation of allegations against the hiring processes for certain time-limited positions.

Our reports contained 36 recommendations for improvement to the FDIC, and its management concurred with all of our recommendations.

Our investigations also achieved significant impact resulting in 47 convictions and fines, restitution orders, and forfeitures over $156 million. In addition, our cases led to the arrest of 15 individuals and 57 indictments and informations. These cases involved former bank officers and directors who misused their positions for personal benefit; businesspersons, insiders, and professionals who fraudulently obtained funds from financial institutions; and an attorney who defrauded numerous financial institutions. In many instances, we worked these cases collaboratively with our law enforcement colleagues in conducting our investigative work. A recent example was the joint investigation of Banamex USA, a subsidiary of Citigroup, which admitted to criminal violations by willfully failing to maintain an effective anti-money laundering program and failing to file Suspicious Activity Reports. Banamex USA agreed to forfeit $97 million related to Bank Secrecy Act violations and, in a related matter, was ordered to pay a $140 million civil money penalty. The penalties for these civil and criminal violations totaled more than $237 million, and three bank executives were banned from working in the banking industry.

Also, during the reporting period, we were proud to join the Inspector General (IG) community in the launch of oversight.gov. This new website will foster greater transparency and accountability, as it maintains a central repository for all public IG reports. In addition, the site is searchable so that it allows the public to access thousands of IG reports across the Federal Government.

In closing, I appreciate the dedication and commitment of OIG personnel, whose work has had significant impact over the past 6 months. In addition, our Office relies upon the continued support of the agency and Members of Congress and staff, as well as our colleagues in the IG community. My Office remains committed to serving the American people as a recognized leader in the IG community.

Jay N. Lerner
Inspector General
October 2017

Acronyms and Abbreviations

BOU	The Bank of Union
BSA	Bank Secrecy Act
BUSA	Banamex USA
C&C	Cotton & Company LLP
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
DATA Act	Digital Accountability and Transparency Act of 2014
DBHG	Data Breach Handling Guide
DBMT	Data Breach Management Team
DIF	Deposit Insurance Fund
DOA	Division of Administration
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOJ	Department of Justice
DRR	Division of Resolutions and Receiverships
FBDS	Failed Bank Data Services
FBI	Federal Bureau of Investigation
FCD	Federal Continuity Directive
FDIC	Federal Deposit Insurance Corporation
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
HSI	Homeland Security Investigations
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IRS-CI	Internal Revenue Service-Criminal Investigation
IT	information technology
MEF	mission essential function
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSBD	Oklahoma State Banking Department
PCA	Prompt Corrective Action
PII	personally identifiable information
PMEF	primary mission essential function
RCC	remotely created check
RMIC	Risk Management and Internal Control
RMS	Division of Risk Management Supervision
SAR	Suspicious Activity Report
SIGTARP	Office of the Special Inspector General for the Troubled Asset Relief Program
SLA	shared loss agreement
SRVB	Saddle River Valley Bank
TIBER	Casa de Cambio Tiber
TSP	technology service provider
VAT	value added tax
WiP	Work in Place

Table of Contents

Inspector General's Statement	i
Acronyms and Abbreviations	ii
Introduction and Overall Results	2
Audits, Evaluations, and Other Reviews	3
Investigations	11
Other Key Priorities	23
Reporting Requirements	28
Appendix 1 Information Required by the Inspector General Act of 1978, as amended	30
Appendix 2 Information on Failure Review Activity	42
Appendix 3 Peer Review Activity	43
Congratulations and Farewell	45

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 as "One OIG," and the results of our work during the reporting period are presented in this report within the framework of those principles. Our Guiding Principles focus on impactful Audits and Evaluations; significant Investigations; partnerships with external stakeholders (the FDIC, Congress, whistleblowers, and our fellow OIGs); efforts to maximize use of resources; Leadership skills and abilities; and importantly, Teamwork.

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

Overall Results **(April 1, 2017 – September 30, 2017)**	
Audit and Evaluation Reports Issued	**6**
Nonmonetary Recommendations	**36**
Investigations Opened	**44**
Investigations Closed	**49**
OIG Subpoenas Issued	**14**
Judicial Actions:	
Indictments/Informations	**57**
Convictions	**47**
Arrests	**15**
OIG Investigations Resulted in:	
Fines	**$99,500**
Restitution	**$56,291,413***
Asset Forfeitures	**$99,969,153**
Total	**$156,360,066**
Referrals to the Department of Justice (U.S. Attorneys)	**53**
Proposed Regulations and Legislation Reviewed	**12**
Responses to Requests Under the Freedom of Information/Privacy Act	**10**

*Of this total amount, $16,458,783 was ordered jointly and severally with other individuals sentenced during this or prior reporting periods.

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 six reports during the reporting period, as discussed below. These reports contain 36 recommendations and span various FDIC programs and activities. Our office also reviews all failed FDIC-supervised institutions causing losses to the DIF of less than the material loss threshold outlined in the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) to determine whether circumstances surrounding the failures would warrant further review. Our failed bank review activity is presented in Appendix 2.

Follow-on Audit of the FDIC's Identity, Credential, and Access Management (ICAM) Program

We issued an audit report that followed up on matters identified in a prior OIG report issued in September 2015, entitled *The FDIC's Identity, Credential, and Access Management (ICAM) Program* (the ICAM Audit Report). The prior report found that the FDIC had not achieved its goal of issuing identity credentials (known as personal identity verification (PIV) cards) to all eligible employees and contractor personnel. Such PIV cards are intended to provide a secure and reliable form of identification to allow individuals access to federally controlled facilities and information systems. In addition, our report found that the FDIC had not established appropriate governance to ensure the ICAM program's success. The prior ICAM Audit Report included recommendations for FDIC management to define the goals and approach for implementing the program and to establish appropriate governance.

In light of these concerns identified in the prior ICAM Audit Report, we conducted a follow-on audit, the objective of which was to assess the FDIC's plans and actions to address the recommendations contained in our prior report. We found that the FDIC took responsive action to address the recommendations in our prior report. However, considerable challenges and risks continued to exist. Specifically,

- The FDIC had not established corporate policies and procedures to govern the management and use of PIV cards for physical and logical access. Such policies and procedures are important for ensuring that employees and contractor personnel become aware of, and fully understand and properly carry out, their responsibilities with respect to PIV cards.

- The FDIC did not maintain current, accurate, and complete contractor personnel data needed to manage PIV cards. Absent reliable contractor personnel data, PIV cards may not be issued and revoked in a timely manner, presenting an increased risk of unauthorized access to FDIC facilities and the Corporate network.
- FDIC management had not finalized and approved a plan for retiring the FDIC's legacy PIV card system. Without such a plan, the FDIC may incur unnecessary costs associated with maintaining the system longer than needed, and sensitive information in the system may not be disposed of in a timely or safe manner.

To address these risks, our report made four recommendations. Management concurred with our recommendations.

Controls over Separating Personnel's Access to Sensitive Information

The FDIC experienced a number of data breaches in late 2015 and early 2016 that involved employees who were exiting the Corporation. Between February and May 2016, the FDIC notified Congress of seven major incidents in which departing employees inappropriately took significant quantities of sensitive information. The information taken was associated with financial institutions and their customers, creating the risk of unauthorized disclosure. 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. We reviewed procedures for separating FDIC employees and FDIC contractor employees (contractors).

We reported that the FDIC has established pre-exit clearance procedures for personnel who are separating from the FDIC. These procedures are intended to protect FDIC-owned property and interests. The FDIC has also taken steps to detect or prevent separating personnel from removing sensitive information from the Corporation, including the use of a data loss prevention tool, placing limits on the use of removable media, and the use of PIV cards to access facilities and information systems.

While the FDIC has established and implemented various control activities for the employee pre-exit clearance process, we found the following:

- **Weaknesses existed in the design of certain controls:** The FDIC did not review certain pre-exit clearance records until after employees had separated; often did not use the data loss prevention tool to examine employee network activity until after employee separation; and relied heavily on employee assertions about their handling of sensitive information, using some forms that did not warn against making false statements.
- **Divisions were not always following procedures:** In the sample we reviewed, division and office records liaisons did not review data questionnaires before employees separated in 20 of 49 cases or 41 percent of the time.
- **The FDIC should strengthen the pre-exit clearance process:** No single FDIC official was responsible for the overall program; division and office representatives needed to assume a more active role in managing the process; and the FDIC did not require divisions and offices to assess risks to sensitive information when they became aware of individuals separating from the FDIC.

We further concluded that separating 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 increase risks related to protecting sensitive information when contractors separate. We also found that the FDIC was not consistently following its pre-exit clearance procedures with respect to separating contractors. Specifically, oversight managers signed clearance records prior to contractor separation 29 percent of the time. Records liaisons signed contractor data questionnaires prior to contract separation 6 percent of the time.

To strengthen its process, the FDIC needed to ensure consistency between employee and contractor pre-exit clearance processes, reiterate responsibilities and expectations for oversight managers and records liaisons, and require timely notice of separating contractors.

As designed, the program controls did not provide reasonable assurance that the pre-exit clearance process would identify unauthorized access to, or inappropriate removal and disclosure of, sensitive information in a timely or effective manner.

We made 11 recommendations to address the weaknesses we identified. The FDIC concurred with the recommendations.

The FDIC's Processes for Responding to Breaches of Personally Identifiable Information

As with the previously discussed evaluation of separating employees' access to sensitive information, we also conducted an audit in response to concerns raised by the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs regarding the series of data breaches reported by the FDIC in late 2015 and early 2016. We focused on the FDIC's processes for responding to such breaches.

Implementing proper controls to safeguard personally identifiable information (PII) and respond to breaches when they occur is critical to maintaining stability and public confidence in the nation's financial system and protecting consumers from financial harm. Our audit assessed the adequacy of the FDIC's processes for evaluating the risk of harm to individuals potentially affected by a breach involving PII and notifying and providing services to those individuals, when appropriate. Our review sample included 18 of 54 suspected or confirmed breaches involving PII that the FDIC discovered during the period January 1, 2015 through December 1, 2016. The breaches we reviewed potentially affected over 113,000 individuals.

We reported that the FDIC had established formal processes for evaluating the risk of harm to individuals potentially affected by a breach involving PII and providing notification and services to those individuals, when appropriate. However, the implementation of these processes was not adequate. Specifically:

- **FDIC Did Not Complete Key Breach Investigation Activities and Notify Affected Individuals Timely.** The FDIC did not complete key breach investigation activities (i.e., impact/risk assessments and/or convene the Data Breach Management Team or DBMT) within the timeframes established in the FDIC's Data Breach Handling Guide (DBHG) for 13 of 18 suspected or confirmed breaches that we reviewed. In addition, the FDIC did not notify potentially affected individuals in a timely manner for the incidents we reviewed. Specifically, it took an average of 288 days (more than 9 months) from the date the FDIC discovered the breaches to the date that the Corporation began to notify individuals.
- **FDIC Did Not Adequately Document Key Assessments and Decisions.** Our review of 18 suspected or confirmed breaches found that Incident Risk Analysis (IRA) forms did not clearly explain the rationale behind the overall impact/risk levels assigned to the incidents. Some IRA forms were not substantially complete prior to convening the DBMT. The underlying analysis used to support assigned impact/risk levels for three breaches was inconsistent with the methodology in the DBHG. The overall risk ratings recorded in the IRA forms for five breaches were not consistent with the risk mitigation actions taken by the FDIC.
- **FDIC Needed to Strengthen Controls Over the DBMT.** Although the DBHG describes the role and activities of the DBMT, the FDIC had not established a formal charter or similar mechanism for the DBMT that defines its purpose, scope, governance structure, and key operating procedures. The FDIC had also not developed a process for briefing DBMT members on the outcome of their recommended actions. Such a process would allow DBMT members to more effectively leverage lessons-learned for future breach response decision-making and promote consistency in the process. In addition, the FDIC did not provide DBMT members with specialized training to help ensure the successful implementation of their responsibilities.
- **FDIC Did Not Track and Report Key Breach Response Metrics.** The DBHG identifies key categories of qualitative and quantitative metrics for benchmarking, tailoring, and continuously improving the FDIC's breach prevention and response capabilities. However, the FDIC generally did not track or report the metrics in the DBHG for the suspected or confirmed breaches we reviewed.

We made seven recommendations to address the issues we identified. The FDIC concurred with the recommendations.

The FDIC's Controls over the Information Technology Hardware Asset Management Program

The FDIC uses information technology (IT) hardware assets, among other things, for personal computing throughout the Corporation, supporting network operations, and providing communications connectivity. At the time of our fieldwork, the FDIC had 38,796 IT hardware items in inventory, including laptops, workstations, desktops, tablets, printers, scanners, servers, drives, routers, mainframes, and other equipment. IT hardware assets are vulnerable to several risks, including inefficient or costly procurement, delays in deployment, equipment theft and obsolescence, and data loss. We evaluated the FDIC's controls over its IT hardware asset management program.

We reported that the FDIC had established some key controls over the IT hardware asset management program, including policies and procedures that specified roles and responsibilities for employees and contractors. However, we found that the FDIC needed to update its policies and procedures and strengthen its controls in most aspects of the program. Further, data needed to manage the program was frequently unreliable. Collectively, these weaknesses created an environment in which the FDIC was vulnerable to ineffectively managing IT hardware assets or having them lost or stolen.

To illustrate:

- Information in the Corporation's IT asset management system and reports generated by the system were not always accurate. As a result, the FDIC was unable to accurately value its IT assets or evaluate the timeliness of receiving assets and providing them to users.
- With respect to tracking and protecting IT assets, the system showed 40 of the 178 employees (22 percent) who had separated from the Corporation over a 4-month period still had at least one IT asset assigned to them in the system.
- The contractor responsible for forms used to assign asset custody had not uploaded the equipment hand receipts for 15 of 36 laptops that we tested, and hand receipt dates were missing for 33 percent of deployed laptops and 46 percent of deployed desktops.
- The FDIC needed to establish procedures for using its technology refresh schedule along with data in its IT asset management system to make informed decisions about an asset's useful life.

We made nine recommendations for the FDIC to enhance asset management life cycle policies and procedures to reflect current practices; strengthen controls to better ensure program objectives are met; and improve the IT asset management tracking system data entry, reliability, and reporting to support IT asset management and decision-making. The FDIC concurred with our recommendations.

The FDIC's Process for Filling Certain Division of Resolutions and Receiverships (DRR) Time-Limited Positions

The OIG received three Hotline complaints in June and December 2015 alleging that certain DRR vacancy announcements posted in 2015 were too restrictive, resulting in the exclusion of veterans and other applicants from meeting required qualification factors. The complainants also alleged that DRR's hiring process was not carried out in a fair and equitable manner. The hiring process is a joint responsibility between the FDIC's Division of Administration (DOA) human resources personnel and DRR program officials, and both divisions need to ensure the hiring process is fair, follows FDIC policies, and helps defend against complaints or criticisms. In response to the allegations, we evaluated the FDIC's process for filling certain time-limited positions in DRR.

We substantiated aspects of the OIG Hotline allegations and identified weaknesses in the FDIC's process for filling certain time-limited positions. For example:

- We identified several weaknesses in DOA and DRR's review of applications. These weaknesses were related to potential conflicts of interest, maintaining confidentiality, ensuring adequate segregation of duties between DOA and DRR personnel, and non-compliance with DOA's procedures for reviewing vacancy announcements.
- We identified process-related matters that were inconsistent with procedures; could have given applicants the perception that DRR, and not DOA, was administering the application review process; and/or posed risks that applicants could be erroneously included or excluded from certificates. In these instances, DRR subject-matter experts performed applicant qualification reviews before DOA human resources staff determined which applicants met eligibility requirements. DOA officials also did not consistently document their concurrence with subject-matter expert review decisions, as required by FDIC policy.
- We found that some qualification factors in 8 of the 13 vacancy announcements that we reviewed were not reflected in the related position descriptions, as required by FDIC policy. Using qualification factors that are grounded in position descriptions helps ensure that applicants are judged on factors that are fundamental to the position being filled and consistency in candidate evaluation and selection decisions.
- We noted that qualification factors in five vacancy announcements were narrowly written and limited the number of qualified applicants. For example, qualifications such as experience as a program administrator for developing a specific DRR system or being a member of a specific committee appeared to us to be narrowly focused and not essential to the related positions. Fewer qualified applicants were included in a certificate for these five announcements than for the eight announcements with qualification factors that we determined were not so specific.

Finally, we were not able to substantiate allegations that qualification factors were too restrictive because there was an absence of sufficient criteria for doing so. Also, based on information we gathered, we were not able to substantiate an allegation that DRR attempted to exclude qualified veterans from certificates.

We made five recommendations to DOA to address these findings. DOA concurred with our recommendations.

Material Loss Review of Seaway Bank and Trust Company, Chicago, Illinois

Prior to passage of the Dodd-Frank Act, in the event of an insured depository institution failure, the Federal Deposit Insurance Act required the appropriate regulatory OIG to perform a review when the Deposit Insurance Fund (DIF) incurs a material loss, defined previously as a loss to the insurance fund exceeding $25 million or 2 percent of the failed institution's total assets. With passage of the Dodd-Frank Act, the loss threshold was increased to $200 million through December 31, 2011, $150 million for losses that occurred for the period January 1, 2012 through December 31, 2013, and $50 million thereafter. The FDIC OIG performs the review if the FDIC is the primary regulator of the institution. The Department of the Treasury OIG and the OIG at the Board of Governors of the Federal Reserve System perform reviews when their agencies are the primary regulators.

During the reporting period, we issued a material loss review report on the failure of Seaway Bank and Trust Company, Chicago, Illinois, an institution that failed on January 27, 2017, resulting in a $57.2 million loss to the DIF. Our report discusses the causes of Seaway Bank's failure and the resulting material loss to the DIF, and evaluates the FDIC's supervision of Seaway, including the FDIC's implementation of the Prompt Corrective Action (PCA) provisions of section 38 of the Federal Deposit Insurance Act. The scope of our review included 2009 through Seaway's failure. Reviewing this period allowed us to evaluate Seaway's history before and after it acquired assets from two failed banks and changes that occurred to Seaway's Board of Directors and management.

We concluded that Seaway failed as a result of poor corporate governance and risk management practices. The Board and management were unable to effectively address a number of problems that began escalating following the death of the bank's long-time Chairman in April 2013, when his widow assumed a 51-percent controlling interest in Seaway's holding company. Examiners had identified these issues, which included accounting problems related to the assets Seaway acquired in 2010 and 2011 from the FDIC as Receiver and the Board's not being aware of the true financial condition and performance of the bank for most of 2013. While the Board took steps to address examiner findings in 2014, including dismissing the officials responsible for the bank's deteriorated financial condition and accounting problems, Seaway faced another problem—finding qualified individuals willing to work for a troubled institution.

The management void at the bank hampered the Board's efforts to effectively address shared loss agreement (SLA)-related issues and an increasing number of non-performing loans within its portfolio. Problem assets were concentrated in bank-originated commercial real estate loans, particularly faith-based and SLA loans. Without a cohesive management team in place, the bank's risk management practices became inadequate relative to its condition. Further, the Board relied heavily on consultants, which created excessive overhead expenses and negatively impacted earnings. From 2013 through its failure in January 2017, losses associated with bank-originated and SLA assets, coupled with high overhead expenses, critically depleted Seaway's capital and viability.

With respect to supervision, we found that the FDIC conducted examination activities, as required, and properly implemented applicable PCA provisions. The report does not contain any formal recommendations, but we concluded that it would have been prudent for the Division of Risk Management Supervision (RMS) to have participated in a 2012 state examination of Seaway or conducted a separate visitation in 2012 to assess Seaway's accounting for the acquired failed bank assets. While it was permissible by the FDIC Rules and Regulations for RMS to forego participation in the state examination, in our opinion, RMS missed an opportunity to see firsthand how the institution was managing and accounting for its acquisition of failed bank assets at a critical time.

****

At the end of the reporting period, we were continuing to monitor the FDIC's progress in implementing agreed-upon corrective actions in response to OIG recommendations to determine whether the FDIC's actions are sufficiently responsive to close the recommendations. We coordinate this activity with FDIC management and the Corporation's Risk Management and Internal Control branch of the Division of Finance. We have posted monthly updates on our Website to keep the public informed of the status of recommended actions. Additional information on unimplemented recommendations is contained in Appendix 1.

Ongoing audit and evaluation reviews at the end of the reporting period were addressing such issues as the FDIC's governance of IT initiatives, controls for preventing and detecting cyber threats, the FDIC's physical security risk management, the FDIC's compliance with the Digital Accountability and Transparency Act of 2014 (DATA Act), the FDIC's implementation of forward-looking supervision, the FDIC's Claims Administration System functionality, and a material loss review of a failed FDIC-supervised institution. These ongoing reviews are also listed on our Website and, when completed, their results will be presented in an upcoming semiannual report.

Investigations

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

- Conducting thorough investigations consistent with the highest professional standards and best practices.
- Working on important and relevant cases that have 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.
- Developing expertise to shape the character of the OIG's investigative component and its Field Offices.

The cases discussed below are illustrative of some of the OIG's investigative success during the reporting period. Special agents in headquarters, regional offices, and the OIG's Electronic Crimes Unit are responsible for these results. These cases reflect the cooperative efforts of OIG investigators, FDIC divisions and offices, other OIGs, U.S. Attorneys' Offices, and others in the law enforcement community throughout the country, as illustrated at the end of this section of our report. 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.

Co-conspirator Pleads Guilty in Casa De Cambio Tiber Case

On September 26, 2017, a co-conspirator in a currency exchange case pleaded guilty to one count of money laundering (18 U.S.C.1956) for his role in a trade based money laundering scheme to defraud the Mexican Government of a value added tax (VAT). He was arrested on a complaint on October 31, 2016 and has been scheduled for sentencing on February 23, 2018.

This investigation was initiated by Homeland Security Investigations (HSI) as a spin-off of an HSI investigation into a series of bank accounts owned by casa de cambios (currency exchanges) located in Mexico moving large sums of currency through a small community bank, Saddle River Valley Bank (SRVB), located in Saddle River, New Jersey. These casa de cambios caused approximately $1.5 billion in wires to move through SRVB from approximately November 2009 through May 2011. Case agents identified "Casa de Cambio Tiber" (TIBER) as one of the main entities involved in these wire transactions. Deutsche Bank was the correspondent bank for the TIBER accounts at SRVB and subsequently Bethex Federal Credit Union. A review of the wire transfer activity identified a series of wire transfers between TIBER and a group of cellular telephone companies.

This trade based scheme exploits the U.S. banking system by moving funds in a circular fashion between shell companies located in Mexico and the U.S. to defraud the Mexican Government of VAT. The companies/individuals in this scheme obtain fraudulent VAT refunds by creating false invoices created by these shell companies showing that the cell phones were "sold" in the U.S. and then submitting these false invoices to the Mexican Government. The phones are never sold in the U.S., but rather exported back to Mexico to further facilitate the scheme. To date, agents have identified approximately $300 million that has been wired between the shell companies in Mexico and the U.S. through the TIBER account at Deutsche Bank and approximately $25 million of fraudulently obtained VAT refunds. Eight individuals have been arrested during the course of the investigation. The co-conspirator opened shell companies and bank accounts in the U.S. and created false invoices for the import and export of cell phone between the U.S. and Mexico.

Source: *This investigation was initiated based on a request for assistance from HSI and the U.S. Attorney's Office for the Southern District of New York.*
Responsible Agencies: *This is a joint investigation with the FDIC OIG, HSI, Internal Revenue Service Criminal Investigation (IRS-CI), Drug Enforcement Administration, and U.S.Customs and Border Patrol, with cooperation from the Mexican authorities. This case is being prosecuted by the U.S. Attorney's Office for the Southern District of New York.*

Attorney Sentenced to 40 Months in Prison

On September 1, 2017, an attorney from Pensacola Beach, Florida, was sentenced to 40 months in prison and ordered to pay more than $3.7 million in restitution for conspiracy to commit bank and mail fraud; making false statements to a federally insured financial institution; nine counts of money laundering; and two counts of theft, embezzlement or misapplication by a person connected with a financial institution.

While working as a title attorney, he facilitated a bank and mail fraud conspiracy by handling a number of closings that defrauded Bank of America, Beach Community Bank, and the now defunct Premier Community Bank. These financial institutions sustained losses totaling in excess of $2.3 million from the conspiracy.

Additionally, beginning in December 2010, while acting as an escrow agent for Beach Community Bank, he embezzled and misapplied in excess of $400,000 that was being held at Beach Community Bank. Thereafter, between December 2010 and March 2011, the attorney conducted a series of financial transactions laundering the funds he had embezzled. In September 2011, Beach Community Bank personnel contacted him to determine where the money was located. Unbeknownst to Beach Community Bank, the attorney then obtained money from a third party to replace the funds he had embezzled. However, a short time after placing the third party's money into the Beach Community Bank account, he embezzled in excess of $237,000 from the same account.

In addition to defrauding the financial institutions and embezzling from Beach Community Bank, the government's evidence also showed that in August 2011, the attorney stole approximately $36,000 from four homeowners/condominium associations that he had been entrusted to oversee.

Source: *FDIC RMS.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, IRS-CI, Special Inspector General for the Troubled Asset Relief Program (SIGTARP), and Okaloosa County Sheriff's Office as part of the Northwest Florida Financial Crimes Task Force. The case is being prosecuted by the U.S. Attorney's Office for the Northern District of Florida.*

Bank Officer Sentenced for Fraud, Identity Theft Scheme

On August 25, 2017, a former loan and compliance officer at Community Bank, NA (acquired by Security Bank of the Ozarks), Summersville, Missouri, was sentenced to serve 24 months in prison to be followed by 60 months of supervised release. The court also entered a final order of forfeiture in the amount of $151,040. The former bank officer pleaded guilty on April 17, 2017, to a criminal Information charging him with making false statements on a loan application and aggravated identity theft.

The former bank officer admitted that he took out numerous loans in the names of several bank customers without their authorization. He submitted loan applications for varying amounts, totaling $81,040, between 2015 and June 2016. He used the personal identification information of bank customers, including their bank account information and social security numbers, to falsely submit the loan applications. In addition, he used his mother's and brother's personal information to apply for approximately $70,000 in loans without their knowledge or approval in 2010 and 2011. He approved the loans and deposited the proceeds from the fake bank loans into his personal bank account to pay for his gambling addiction.

Source: *This investigation was OIG/OI initiated.*
Responsible Agencies: *The FDIC OIG conducted the investigation with assistance from the Federal Housing Finance Agency OIG and Federal Bureau of Investigation (FBI). The case is being prosecuted by the U.S. Attorney's Office for the Western District of Missouri.*

California Payment Processing Company President Sentenced for Fraud Scheme

On July 6, 2017, the president of a payment processing company was sentenced to serve 15 months in prison, followed by one year of supervised release. He was also ordered to pay a $50,000 fine, and the judge entered a $100,000 forfeiture money judgment against him.

The company president used his Santa Ana, California, processing company, Check Site Inc., to assist at least two fraudulent merchants. The merchants operated or worked with Websites that purportedly offered subscriptions, clubs, sweepstakes, or payday loans. But in many cases, the Websites were a ruse to collect consumers' bank account information. Instead of providing consumers with payday loans or other services advertised, the merchants operating the Websites used the bank information provided by the consumers to withdraw money from the consumers' bank accounts. Using Check Site, the president knowingly processed the merchants' fraudulent withdrawals and provided the merchants with access to the banking system.

The company president admitted to using payment devices called remotely created checks (RCCs) to facilitate fraud schemes. Once the fraudulent merchants had obtained consumer names and bank account information, the merchants created RCCs, which Check Site submitted through the banking system to the consumers' banks. Unlike an ordinary check, an RCC is generally honored without the signature of the account holder. When the RCCs were processed, Check Site kept a fee and transferred the remainder of the withdrawals to the merchants.

According to charging documents, the president used banks that were willing to facilitate these transactions and ignore the red flags that these transactions raised. The charges also alleged that he helped the fraudulent merchants stay off the radar of bank employees and regulators so that the fraud could continue. For example, he advised merchants on how to change the names of their companies and set up the facade of a legitimate company to defeat banks' attempts at due diligence.

In an email message quoted in the charging documents and referenced in a Department of Justice (DOJ) press release, the payment processing company advised a fraudulent merchant that *"the lesson we have learned is that we must trick the [bank] folk. It means you need to set up some type of website front. What we need to do is set up a legitimate website selling anything you can think of – that is what you get approved on. It is irrelevant if anything is ever sold there – just so it exists. . . . In the mean time we set up false credit card approval etcetera. It is this we use to run the transactions. Yes, there will be a lot of returns, but what we do is send through transactions over the next few weeks that don't have high returns. They stop looking and then we can run the regular stuff. . . . [A]fter several months we junk that company and go to another company."*

Source: *FBI Philadelphia Field Office.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, FBI, Federal Trade Commission, and DOJ Civil Division's Consumer Protection Branch. The case is being prosecuted by the U.S. Attorney's Office for the Eastern District of Pennsylvania.*

Businessman Sentenced to 180 Months in Prison for Orchestrating $70 Million Ponzi Scheme

On June 30, 2017, an Ohio businessman was sentenced to 180 months in prison, followed by 3 years of supervised release, and was ordered to pay restitution of $32,767,578. Earlier, on October 29, 2015, the businessman and his wife were indicted on one count of conspiracy to commit mail and wire fraud, 8 counts of mail fraud, 13 counts of wire fraud, 2 counts of money laundering, and one count of theft or embezzlement from an employee benefit plan.

From 2009 to 2014, the couple orchestrated a Ponzi scheme in the Dayton, Ohio, area. Nearly 480 investors lost approximately $30 million as a result of the scheme. The businessman operated multiple investment and asset management companies and falsely reported that he was a registered securities broker. His wife operated multiple companies that transferred investor funds to companies her husband controlled. The couple recruited investors from 37 states to invest in two of their companies, Midwest Green Resources and WMA Enterprises. The investors were told their funds would be used for acquiring investment securities, purchasing real estate, providing loans, and purchasing precious metals. Rather than investing the money, the couple used it to purchase personal luxury items.

When the couple was late on interest payments to the investors, the investors were given multiple explanations such as that their bank accounts had been hacked, a bank mistakenly failed to wire payments, or the deal was temporarily on hold.

In addition to the businessman's sentencing, the government has seized two racehorses, vehicles, jewelry, artwork, and cash totaling almost $650,000 from the couple.

Source: *FBI.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, FBI, U.S. Postal Inspection Service, U.S. Department of Labor OIG, and IRS-CI. The case is being prosecuted by the U.S. Attorney's Office, Southern District of Ohio.*

Former GulfSouth Private Bank President and Two Others Sentenced

On June 28, 2017, the former president of the failed GulfSouth Private Bank (GulfSouth), Destin, Florida, was sentenced to 63 months of incarceration followed by 5 years of supervised release. Previously, he was found guilty on one count of conspiracy to commit bank fraud, five counts of bank fraud, and one count of mail fraud after a jury trial that ended on March 10, 2017. He was also ordered to pay $2,421,414 in restitution, jointly and severally with the other subjects in the case.

The former senior vice president of GulfSouth was sentenced to 3 months of incarceration, followed by 5 years of supervised release. He entered a guilty plea to one count of conspiracy to commit bank fraud and five counts of bank fraud on February 27, 2017. The short sentence was partly due to the substantial assistance he provided and his testimony at trial against the former bank president. He was also ordered to pay $2,421,414 in restitution, jointly and severally with the other subjects in the case.

A Florida developer was sentenced to one day in prison followed by 5 years of supervised release with the first 6 months to be served as home confinement. He was ordered to pay $627,850 in restitution, jointly and severally with the former bank president and former senior vice president. He had entered a guilty plea to conspiracy to commit bank fraud and one count of making false statements to a federally insured financial institution on March 13, 2017.

According to the allegations in the indictment, between December 1, 2007, and February 1, 2012, the two former bank officers of GulfSouth conspired with other persons, including the developer, to hide non-performing loans in the names of nominees or "straw men." This assisted in making the bank look more financially stable. It also kept the loans "alive" long enough so funds from the Troubled Asset Relief Program (TARP) could be used to write off some of the losses. Specifically, the former bank officers solicited four bank customers to obtain loans from GulfSouth totaling over $3.8 million and to purchase three luxury condominium units for over $1 million each. The units were located on Perdido Key, just west of Pensacola, Florida. In support of the scheme, the former bank officers created and approved false loan documents.

The developer obtained moneys from GulfSouth by false and fraudulent pretenses for the purchase of a condominium unit in Pensacola, Florida. The developer acted as a straw man on two loans from GulfSouth for $290,000 and $1,064,200, with the assistance of the former bank officers.

The two former bank officers also misled another financial institution (Gulf Coast Community Bank) into releasing their interest in two of the condominiums through deceptive communications. And finally, the former bank president also sent a fraudulent Satisfaction of Mortgage via the mail to release an encumbered property for one of the straw men, causing the mail fraud count.

Previously, the three other straw men involved in the scheme entered guilty pleas and have begun serving their sentences.

Source: *This case was initiated based on information received from GulfSouth Private Bank.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG and SIGTARP. The case is being prosecuted by the U.S. Attorney's Office in the Northern District of Florida (Pensacola Division).*

Former Certified Public Accountant Pleads Guilty to Fraud Schemes

On June 12, 2017, a former certified public accountant (CPA), pleaded guilty to a Criminal Information charging him with embezzlement and failure to pay taxes.

According to the Information, while serving on the board of directors of Alternative Opportunities (AO), a not-for-profit company that provides mental and behavioral treatment and counseling in addition to other medical services, the former CPA embezzled $1,965,476. He did so by causing the organization to issue checks payable to himself and others, which he deposited into his personal checking account. He also embezzled $1,029,000 from another business, Carnahan-White, while employed as a consultant. In addition, he admitted he failed to disclose $776,340 of income when he filed his 2013 tax return and did not file returns for 2011, 2012, 2014, and 2015.

Source: *U.S. Attorney's Office, Western District of Missouri.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, IRS-CI, and FBI. The case is being prosecuted by the U.S. Attorney's Office for the Western District of Missouri.*

Banamex USA Enters into a Non-Prosecution Agreement and Agrees to Forfeit $97.44 Million

Banamex USA (BUSA) agreed to forfeit $97.44 million and entered into a non-prosecution agreement to resolve an investigation into BUSA's Bank Secrecy Act (BSA) violations.

In its agreement with the Department of Justice, BUSA admitted to criminal violations by willfully failing to maintain an effective anti-money laundering (AML) compliance program with appropriate policies, procedures, and controls to guard against money laundering and willfully failing to file Suspicious Activity Reports (SARs). According to admissions contained in the agreement and the accompanying statement of facts, from at least 2007 until at least 2012, BUSA processed more than 30 million remittance transactions to Mexico with a total value of more than $8.8 billion. During the same period, BUSA's monitoring system issued more than 18,000 alerts involving more than $142 million in potentially suspicious remittance transactions. BUSA, however, conducted fewer than 10 investigations and filed only 9 SARs in connection with these 18,000-plus alerts, filing no SARs on remittance transactions between 2010 and 2012. BUSA also admitted that, for several years, BUSA recognized that it should have improved its monitoring of money service business remittances but failed to do so. BUSA employed a limited and manual transaction monitoring system, running only two scenarios to identify suspicious activity on the millions of remittance transactions it processed. These two scenarios produced paper reports that were intended to be reviewed by hand by the two employees assigned to perform the BSA functions of the bank, in addition to time-consuming non-BSA responsibilities. As BUSA began to expand its remittance processing business in 2006, BUSA understood the need to enhance its anti-money laundering efforts, yet failed to make necessary improvements to its transaction monitoring controls or to add staffing resources.

> ***Source:*** *The investigation was initiated based on information provided by the FDIC's RMS.*
> ***Responsible Agencies****: This case was investigated by the Drug Enforcement Administration, IRS-CI, and FDIC OIG. The case was prosecuted by the Department of Justice Money Laundering and Asset Recovery Section and the U.S. Attorney's Office for the District of Massachusetts.*

Former Vice President of Maryland Bank Sentenced to 3 Years in Federal Prison for Scheme to Steal Over $1.8 Million from Bank Customers

A former vice president and Bank Secrecy Act officer of a Maryland bank was sentenced to 3 years in prison, followed by 3 years of supervised release. She was also ordered to pay restitution of $1,611,108. She had pleaded guilty on January 25, 2017, to wire fraud and bank embezzlement, arising from a 6-year scheme to steal over $1.8 million from bank customers at the bank where she worked.

According to her plea agreement, from April 2010 through July 2016, she was senior vice president at Hopkins Federal Savings Bank in Maryland, which had branches in Pikesville and Highlandtown. In that role, she was responsible for managing the bank's savings department, including overseeing deposits and Individual Retirement Accounts for every customer. In addition, as the bank's BSA officer, she was responsible for filing Currency Transaction Reports and SARs for any transactions that were deemed to be suspicious or potentially illegal.

The former vice president admitted that she used her position of trust at the bank to cause more than 200 unauthorized transfers and withdrawals of funds from six customers' bank accounts to pay for mortgages, credit card bills, and property tax bills that she and her family members had amassed. Three of the six victim customers were at least 80 years old, and for two of the accounts, the customers were deceased.

In carrying out her scheme, for example, the former vice president would use her supervisory override function on the bank's electronic banking system to facilitate unauthorized transfers between the victim customers' accounts to accounts associated with her; forged the signature of one victim customer in order to complete an unauthorized transaction from that person's bank account to an American Express account associated with her; and caused unauthorized transfers of funds between the victim customers' accounts to replace the monies she stole and to conceal those thefts.

Source: *U.S. Attorney's Office for the District of Maryland.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG and FBI. The case is being prosecuted by the U.S. Attorney's Office for the District of Maryland.*

Bank Customers Sentenced in Money Laundering Conspiracy

On August 17, 2017, a married couple who were customers of Plains State Bank, Plains, Kansas, were sentenced to 3 years of probation for their role in a money laundering conspiracy. The two were ordered to forfeit approximately $201,060 and their home located in Meade, Kansas. Additionally, the husband was ordered to pay a money judgment in the amount of $1,535,879.

Beginning on an unknown date until August 2014, the couple transported U.S. currency and checks from Mexico into the United States and deposited them into their Plains State Bank (and other) accounts. When transporting these funds into the U.S., on most occasions, they did not report this money as required by U.S. law. The couple did not know the individuals or businesses from whom they received the checks, nor had they conducted business with them, but the two knew that the money they received represented proceeds from some form of unlawful activity. After depositing the funds into their accounts, funds were transferred out-of-state to purchase genetically modified corn seed that was shipped to the U.S./Mexican border and subsequently delivered into Mexico at the instruction of the husband. The couple acknowledged that they received approximately $1.6 million in U.S. currency and $5 million in checks, representing the proceeds of unlawful activity.

Source: *FDIC RMS.*
Responsible Agencies: *This is a joint investigation by the Drug Enforcement Administration, IRS-CI, and FDIC OIG. The case is being prosecuted by the U.S. Attorney's Office for the District of Kansas.*

Former Bank President Pleads Guilty to Making a False Statement to the FDIC

On September 18, 2017, the former president, chief executive officer, and chairman of the board of The Bank of Union (BOU), El Reno, Oklahoma, pleaded guilty to an Information charging him with making a false statement on a Consolidated Report of Condition and Income (Call Report) submitted to the FDIC. He was previously charged in December 2016 in a 23-count indictment with conspiracy to commit bank fraud, bank fraud, misapplication of bank funds, bank false entries, false statements in connection with loan applications, false statement to the FDIC, wire fraud, and money laundering. The former president is the sixth defendant to be charged and convicted in this case.

The investigation was initiated based on a referral from the FDIC's RMS regarding allegations of suspicious activity in connection with millions of dollars in fraudulent loans originated by the former bank president on behalf of BOU. He served as the president, chief executive officer, chairman of the board, and a loan officer at BOU from approximately 1997 until his resignation on November 30, 2013. BOU was closed by the Oklahoma State Banking Department (OSBD) on January 24, 2014, and the FDIC was appointed Receiver. The estimated loss stemming from BOU's failure as of August 2017 was almost $100 million.

Starting in at least 2009 and continuing through November 2013, the former president falsified customer financial statements, originated nominee loans to cover massive overdrafts, capitalized the principal and interest on past due loans into new loans, and concealed the true financial condition of customers from the bank's Board of Directors, OSBD, and the FDIC. He also executed a scheme to defraud a partial owner and investor in BOU in December 2012. The former president persuaded the investor to wire $40 million to BOU by falsely representing that BOU was growing rapidly and performing well knowing that the bank was on the brink of failure.

Source: *FDIC RMS.*
Responsible Agencies: *This case is being investigated by the FDIC OIG and FBI and is being prosecuted by the U.S. Attorney's Office for the Western District of Oklahoma.*

FDIC OIG Electronic Crimes Unit Assists in Case Involving Bitcoin Cryptocurrency

On July 25, 2017, a joint law enforcement investigation by the FDIC OIG Electronic Crimes Unit, along with DOJ, IRS-CI, FBI, HSI, and U.S. Secret Service, in collaboration with police in Greece, led to the arrest of a Russian National for allegedly running a massive money laundering operation that processed $4 billion in bitcoins through an illegal cryptocurrency exchange, BTC-e. Concurrent with his arrest, the servers and domain of the BTC-e exchange were also seized.

According to the 21-count indictment, which was unsealed by DOJ on July 26, 2017, the Russian National was charged with operating an unlicensed money service business, as well as with money laundering and related crimes. The indictment says numerous transfers from BTC-e administrator accounts went straight to personal bank accounts registered in the Russian National's name.

U.S. authorities have accused BTC-e, founded in 2011, of not only operating as an unlicensed money service business, but also laundering funds for numerous cybercriminal enterprises. "BTC-e facilitated crimes included computer hacking and ransomware, fraud, identity theft, tax refund fraud schemes, public corruption and drug trafficking," according to the indictment. "Since its inception, [the Russian National] and others developed a customer base for BTC-e that was heavily reliant on criminals, including by not requiring users to validate their identity, obscuring and anonymizing transactions and sources of funds, and by lacking any anti-money laundering processes." The indictment also connects BTC-e to the heist of more than $500 million from the Tokyo-based Mt. Gox digital currency exchange.

The value of a bitcoin continues to fluctuate wildly, hitting a record high of more than $4,300 per bitcoin on August 14. From 2011 until the end of 2016, BTC-e processed more than 9.4 million bitcoins, according to court documents. While a bitcoin's fluctuating value makes it difficult to put a dollar value on that quantity of cryptocurrency, at current exchange rates, that quantity of bitcoins would be worth $40.5 billion.

BTC-e's website says that its operations are based in Bulgaria but subject to the laws of Cyprus. "The exchange allegedly maintains a base of operations in the Seychelles Islands and its web domains are registered to shell companies in, among other places, Singapore, the British Virgin Islands, France, and New Zealand," authorities say.

The indictment also alleges that many BTC-e users – as well as the site's operators – also used the notorious Liberty Reserve virtual currency system, based in Costa Rica, which was shuttered by DOJ in 2013.

We will present information on subsequent actions on this case–as they become public—in future semiannual reports.

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 partnerships have evolved from years of hard work in pursuing offenders through parallel criminal and civil remedies resulting in major successes, with harsh sanctions for the offenders. Our collective efforts have served as a deterrent to others contemplating criminal activity and helped maintain the public's confidence in the nation's financial system.

During the reporting period, we partnered with U.S. Attorneys' Offices in the following areas: Alabama, Arkansas, California, District of Columbia, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, 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 the reporting period.

Keeping Current with Criminal Activities Nationwide

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

OIG Headquarters	Financial Fraud Enforcement Task Force, National Bank Fraud Working Group--National Mortgage Fraud Working Sub-group.
New York Region	New York State Mortgage Fraud Working Group; Newark Suspicious Activity Report (SAR) Review Task Force; Philadelphia SAR Review Team; 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; 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.
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	St. Louis Mortgage Fraud Task Force; Kansas City Financial Crimes Task Force; Minnesota Inspector General Council meetings; Kansas City SAR Review Team; Springfield Area 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; Cook County Region Organized Crime Organization; Financial Investigative Team, Milwaukee, Wisconsin; Milwaukee Mortgage Fraud Task Force; 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	FBI Seattle Mortgage Fraud Task Force, 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.
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, Botnet Threat 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, and investigations conducted during the reporting period, our office has emphasized other key initiatives. Specifically, in keeping with our Guiding Principles, we have focused on relations with partners and stakeholders, resource administration, and leadership and teamwork. A brief listing of some of our efforts in these areas follows.

Strengthening relations with partners and stakeholders.

- Communicated with the Chairman, Vice Chairman, other FDIC Board Members, the Chief Financial Officer, and other senior FDIC officials through the IG's regularly scheduled meetings with them and through other forums.
- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
- Coordinated with the FDIC Vice Chairman, 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.
- 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 Vice Chairman of such releases.
- Attended FDIC Board Meetings, FDIC Operating Committee meetings, Chief Information Officer Council meetings, corporate planning and budget meetings, and 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; attending or monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the Corporation's Office of Legislative Affairs on issues of mutual interest.
- More specifically, the OIG met with congressional staff to discuss earlier work related to the FDIC's hardware asset management practices, recent and ongoing work in support of our fiscal year 2018 appropriation, and issues regarding OIG email security.
- Maintained the OIG Hotline to field complaints and other inquiries from the public and other stakeholders. The OIG's Whistleblower Protection Ombudsperson 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 Audit Committee, the Professional Development Committee, Legislation Committee, Assistant Inspectors General for Investigations, Council of Counsels to the IGs, and Federal Audit Executive Council; participating in the Federal Audit Executive Council's DATA Act Working Group; participating on an IG Empowerment Act working group related to new semiannual reporting and other requirements; responding to multiple requests for information on IG community issues of common concern; and commenting on various legislative matters through CIGIE's Legislation Committee.
- Participated on the Council of Inspectors General on Financial Oversight (CIGFO), as established by the Dodd-Frank Act, and coordinated with the IGs on that council. This Council facilitates sharing of information among CIGFO member Inspectors General and discusses ongoing work of each member IG as it relates to the broader financial sector and ways to improve financial oversight.
- Provided the Government Accountability Office (GAO) our perspectives on the risk of fraud at the FDIC. We did so in response to GAO's responsibility under Statement of Auditing Standards No. 99, Consideration of Fraud in Financial Statement Audits.
- Coordinated with GAO on ongoing efforts related to the annual financial statement audit of the FDIC and on other GAO work of mutual interest, for example regarding ongoing work on IG vacancies.
- Coordinated with the Office of Management and Budget (OMB) on the OIG's budget submission for FY 2018 and other matters requiring OIG attention.
- Worked closely with representatives of the DOJ, including Main Justice Department, the FBI, and U.S. Attorneys' Offices, to coordinate our criminal investigative work and pursue matters of mutual interest.
- Promoted transparency to keep the American public informed through three main means: redesign of the FDIC OIG Website to include, for example, summaries of completed work, listings of ongoing work, and information on unimplemented recommendations; addition of Twitter capabilities on the FDIC OIG Website for immediately disseminating news of report and press release issuances; and participation in the IG community's oversight.gov Website, which enables users to access, sort, and search more than 5,800 previously-issued IG reports and other oversight areas of interest.

Administering resources prudently, safely, securely, and efficiently.

- Relied on OIG Counsel's Office to ensure the office complied with legal requirements, 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, and management operations of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the office.
- Continued efforts to update the OIG's records and information management program and practices to ensure an efficient and effective means of collecting, storing, and retrieving needed information and documents. Took steps to increase awareness of the importance of records management in the OIG, including through communications to OIG staff in headquarters and field locations.

- Carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. Positions filled during the reporting period included General Counsel, Senior Advisor to the IG, and IT Specialist.
- Hired interns with skills in finance, IT, communications, and management, and planned for their ongoing involvement in OIG activities.
- Prepared a budget justification document for OMB and FDIC OIG Appropriations Committees to support the FDIC Chairman's approval of a fiscal year 2018 budget of $39.1 million to fund 144 authorized positions, up 7 from fiscal year 2017.
- Oversaw contracts to qualified firms to provide audit, evaluation, 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 to complement other OIG functions and closely monitored contractor performance.
- Continued to monitor, track, and control OIG spending, particularly as it relates to OIG travel-related expenses, use of procurement cards, training costs, and other expenditures.
- Explored options for the OIG's email to the Cloud initiative and contracted for business process analysis services to assist us in evaluating requirements for further development of the OIG's Electronic Crimes Unit lab.
- Further developed the OIG's Data Analytics capabilities as a new approach to improve the overall efficiency and effectiveness of the OIG's audit and evaluation assignments; identify and reduce fraud, waste, and abuse; and facilitate OIG decision-making.

Exercising leadership skills and promoting teamwork.

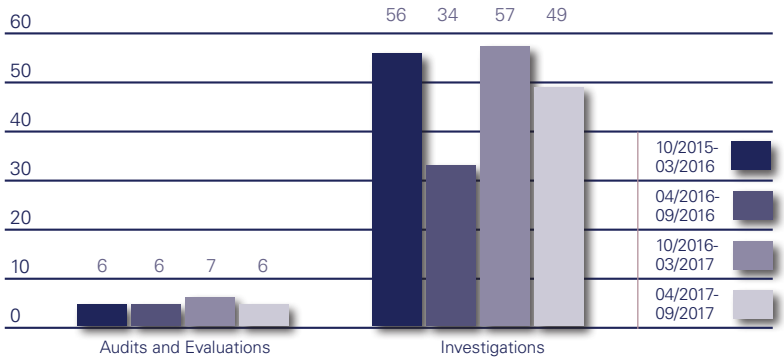
- Held a series of senior leadership meetings to affirm the OIG's unified commitment to the FDIC IG mission and to strengthen working relationships among all FDIC OIG offices.
- Continued to refine strategic plans for individual OIG offices, taking into consideration current resources, skills, accomplishments, challenges, and goals for the future. These individual plans will form the basis for future budget requests, promote further understanding of component offices, and help ensure that office-wide efforts in pursuit of the OIG mission are efficient, effective, and economical.
- Established and selected members to serve on the IG Advisory Council, a cross-cutting group of OIG staff whose mission is to provide leadership toward ONE OIG by promoting collaboration and innovation.
- 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. Held informal meetings and other events and OIG-wide townhall meetings to promote the concept of "One OIG."

- Formed working groups to leverage skills and knowledge in addressing office projects—for example, the interdisciplinary team established to develop management and performance challenges, an audit and evaluation team addressing process improvement and alternative reporting options, and an interdisciplinary team formed to address office-wide IT-related issues and solutions.
- Enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities.
- Instituted 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 further developed a process for administering three new OIG awards to recognize outstanding efforts and to provide staff an opportunity to nominate peers: Distinguished Professional Award, Spirit of the OIG Award, and IG Award for Excellence. Also nominated OIG teams for CIGIE awards.
- 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.

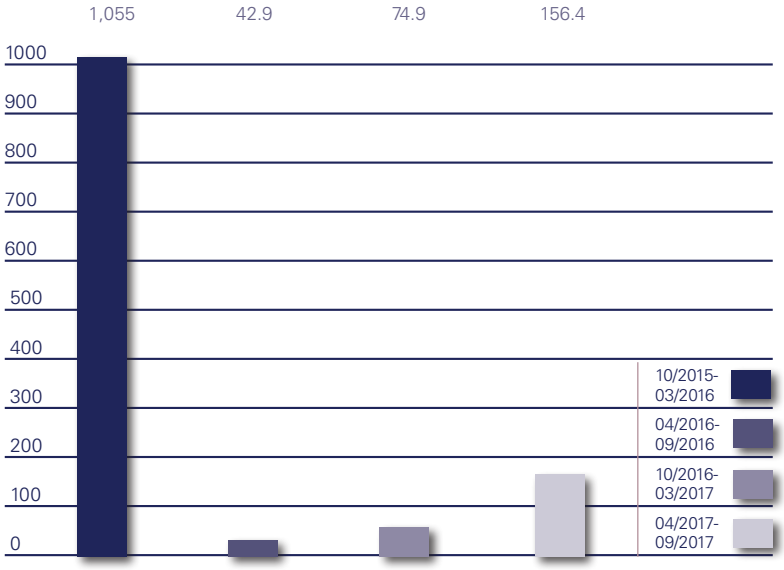
Cumulative Results
(2-year period)

Nonmonetary Recommendations	
October 2015 – March 2016	12
April 2016 – September 2016	16
October 2016 – March 2017	27
April 2017 – September 2017	36

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	30
Section 5(a)(1) Significant problems, abuses, and deficiencies	3-10
Section 5(a)(2) Recommendations with respect to significant problems, abuses, and deficiencies	3-10
Section 5(a)(3) Recommendations described in previous semiannual reports on which corrective action has not been completed	31
Section 5(a)(4) Matters referred to prosecutive authorities	41
Section 5(a)(5) Summary of each report made to the head of the establishment regarding information or assistance refused or not provided	41
Section 5(a)(6) Listing of audit, inspection, and evaluation reports by subject matter with monetary benefits	38
Section 5(a)(7) Summary of particularly significant reports	3-10
Section 5(a)(8): Statistical table showing the total number of audit reports and the total dollar value of questioned costs	39
Section 5(a)(9) Statistical table showing the total number of audit reports and the total dollar value of recommendations that funds be put to better use	39
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	40
• no establishment comment was received within 60 days of providing the report	40
• there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations	32-37
Section 5(a)(11) Significant revised management decisions during the current reporting period	40

Reporting Requirements (continued)	Page
Section 5(a)(12) Significant management decisions with which the OIG disagreed	41
Section 5(a)(14, 15, 16) An appendix with the results of any peer review conducted by another OIG during the period or if no peer review was conducted, a statement identifying the last peer review conducted by another OIG	43
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	41
Section 5(a)(18) A description of metrics used for Section 5(a)17 information	41
Section 5(a)(19) A report on each OIG investigation involving a senior government employee where allegations of misconduct were substantiated, including • the facts and circumstances of the investigation • the status and disposition of the matter, including if referred to the DOJ, the date of referral, and the date of DOJ declination, if applicable	41
Section 5(a)(20) A detailed description of any instance of Whistleblower retaliation, including information about the official engaging in retaliation and what consequences the establishment imposed to hold the official responsible	41
Section 5(a)(21) A detailed description of any attempt by the establishment to interfere with OIG independence, including with respect to budget constraints, resistance to oversight, or restrictions or delays involving access to information	41
Section 5(a)(22) A detailed description of each OIG inspection, evaluation, and audit that is closed and was not disclosed to the public; and OIG investigation involving a senior government employee that is closed and was not disclosed to the public	41

Appendix 1

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

Review of Legislation and Regulations

The FDIC OIG's review of legislation and regulations during the past 6-month period involved continuing efforts to monitor and/or comment on enacted law and/or proposed Congressional legislation, and other regulatory or guidance documents, as follows:

Legislation, Statutes, and Related Documents

- Public Law 115-42 (regarding stays by Merit Systems Protection Board with no quorum)
- H.R. 2227, *the Modernizing Government Technology Act of 2017*
- S. 1869, *the Whistleblower Coordination Act*
- H.R.1224, the National Institute of Standards and Technology (*NIST) Cybersecurity Framework, Assessment, and Auditing Act of 2017* (draft substitute amendment)
- H.R. 3354, *the Interior and Environment, Agriculture and Rural Development, Commerce, Justice, Science, Financial Services and General Government, Homeland Security, Labor, Health and Human Services, Education, State and Foreign Operations, Transportation, Housing and Urban Development, Defense, Military Construction and Veterans Affairs, Legislative Branch, and Energy and Water Development Appropriations Act, 2018*
- H.R. 3708, *the Cryptocurrency Tax Fairness Act*
- H.R. 378, *the Bonuses for Costcutters Act of 2017*
- H.R. 3312, *the Systemic Risk Designation Improvement Act of 2017*
- H.R. 3243, *the Federal Information Technology Acquisition Reform Act Enhancement Act of 2017*
- *Council of the Inspectors General on Integrity and Efficiency (CIGIE) Legislative Priorities for 2017*

Regulatory or Guidance Documents

OMB Memorandum 17-27, *Assessment and Enforcement of Domestic Preferences In Accordance with Buy American Laws*

FDIC Proposed Rule, *Simplifications to the Capital Rule Pursuant to the Economic Growth and Regulatory Paperwork Reduction Act of 1996*

Office of Personnel Management Proposed Rule, *Administrative Leave, Investigative Leave, Notice Leave, and Weather and Safety Leave*

Q&A Guide to Reporting and Posting Requirements (CIGIE Working Group on Inspector General Empowerment Act, non-Semiannual Report to Congress issues)

Inspectors General Guide to Compliance under the DATA Act (Federal Audit Executive Council DATA Act Working Group)

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. The information in this table is based on (1) information supplied by the FDIC's Risk Management and Internal Control (RMIC) branch, Division of Finance and (2) the OIG's determination of when a recommendation can be closed. RMIC has categorized the status of these recommendations as follows:

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

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

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 Recommended Corrective Actions and Associated Monetary Amounts
Management Action in Process		
AUD-14-002 **Independent Evaluation of FDIC's Information Security Program** November 21, 2013	**10▼**	Coordinate with the Division of Information Technology and FDIC division and office officials, as appropriate, to address potential gaps that may exist between the 12-hour timeframe required to restore mission essential functions following an emergency and the 72-hour recovery time objective for restoring mission-critical applications.
AUD-15-008 **The FDIC's Role in Operation Choke Point and Supervisory Approach to Institutions that Conducted Business with Merchants Associated with High-Risk Activities** September 16, 2015	**2**	Assess the effectiveness of the FDIC's supervisory policy and approach with respect to the issues and risks discussed in this report after a reasonable period of time is allowed for implementation.
AUD-16-004 **The FDIC's Process for Identifying and Reporting Major Information Security Incidents** July 7, 2016	**1***	Revise the FDIC's incident response policies, procedures, and guidelines to address major incidents.
	4*	Establish controls to ensure that future Congressional notifications of major incidents include appropriate context regarding the risks associated with those incidents and that statements of risk are supported by sufficient, appropriate evidence.

▼ The OIG is evaluating management's actions in response to the OIG recommendation.

* The OIG has requested additional information to evaluate management's actions in response to the OIG recommendation.

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-14-002 **Independent Evaluation of the FDIC's Information Security Program – 2013** November 21, 2013	The Federal Information Security Management Act of 2002 (FISMA) states that independent evaluations are to be performed by the agency Inspector General, or an independent external auditor as determined by the Inspector General. The objective of this performance audit was to evaluate the effectiveness of the FDIC's information security program and practices, including the FDIC's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We concluded that the FDIC had established and maintained many information security program controls and practices that were generally consistent with FISMA requirements, Office of Management and Budget (OMB) policy and guidelines, and applicable National Institute of Standards and Technology (NIST) standards and guidelines. The FDIC had established security policies and procedures in almost all of the security control areas we evaluated. The FDIC was also working to develop a formal concept-of-operations document that describes a corporate-wide approach to information security continuous monitoring. Our report contained 15 recommendations intended to improve the effectiveness of the FDIC's information security program controls and practices.	15	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-15-008 **The FDIC's Role in Operation Choke Point and Supervisory Approach to Institutions that Conducted Business with Merchants Associated with High-Risk Activities** September 16, 2015	In a letter dated October 23, 2014, 35 Members of Congress (referred to hereinafter as Members) requested that the FDIC OIG investigate the involvement of the FDIC and its staff in the creation and/or execution of the United States Department of Justice (DOJ or Department) initiative known as Operation Choke Point. In the letter, Members expressed concern that the FDIC was working with DOJ in connection with Operation Choke Point to pressure financial institutions to decline banking services to certain categories of lawfully operating merchants that had been associated with high-risk activities. The letter also indicated that it was the Members' belief that FDIC officials had abused their authority by advancing a political or moral agenda to force certain lawful businesses out of the financial services space. The objectives of the audit were to (1) describe the FDIC's role in the DOJ initiative known as Operation Choke Point and (2) assess the FDIC's supervisory approach to financial institutions that conducted business with merchants associated with high-risk activities for consistency with relevant statutes and regulations. We concluded that the FDIC's involvement in Operation Choke Point had been limited to a few FDIC staff communicating with DOJ employees regarding aspects of the initiative's implementation. These communications with DOJ generally related to the Corporation's responsibility to understand and consider the implications of potential illegal activity involving FDIC-supervised financial institutions. Overall, we consider the FDIC's involvement in Operation Choke Point to have been inconsequential to the overall direction and outcome of the initiative. We found no evidence that the FDIC used the high-risk list to target financial institutions. We also determined that the FDIC's supervisory approach to financial institutions that conducted business with merchants on the high-risk list was within the Corporation's broad authorities granted under the FDI Act and other relevant statutes and regulations. However, the manner in which the supervisory approach was carried out was not always consistent with the FDIC's written policy and guidance. The report contains three recommendations to (1) review and clarify, as appropriate, existing policy and guidance pertaining to the provision and termination of banking services; (2) assess the effectiveness of the FDIC's supervisory policy and approach after a reasonable period of time is allowed for implementation; and (3) coordinate with the FDIC's Legal Division to review and clarify, as appropriate, supervisory policy and guidance to ensure that moral suasion is adequately addressed.	3	1	NA

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

Report Number, Title, and Date	Report Summary	Recommendations Total	Recommendations Outstanding	Potential Cost Savings
AUD-16-001 **FDIC's Information Security Program – 2015** October 28, 2015	The FDIC Office of Inspector General engaged the professional services firm of Cotton & Company LLP (C&C) to conduct a performance audit to satisfy the Federal Information Security Modernization Act of 2014 requirement. The objective of this performance audit was 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. As part of the firm's work, C&C noted several important improvements in the FDIC's information security program over the last year. The report contains six recommendations that are intended to improve the effectiveness of the FDIC's information security program controls and practices.	6	1	NA
EVAL-16-004 **The FDIC's Process for Identifying and Reporting Major Information Security Incidents** July 7, 2016	The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program that includes (among other things) procedures for detecting, reporting, and responding to information security incidents. Such procedures are to include notifying and consulting with, as appropriate, the Congressional Committees referenced in the statute for major incidents. The audit objective was to determine whether the FDIC had established key controls that provide reasonable assurance that major incidents are identified and reported in a timely manner. Although the FDIC had established various incident response policies, procedures, guidelines, and processes, these controls did not provide reasonable assurance that major incidents were identified and reported in a timely manner. The report contains five recommendations addressed to the CIO that are intended to provide the FDIC with greater assurance that major incidents will be identified and reported consistent with FISMA and OMB Memorandum M-16-03.	5	4	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-17-001 **Audit of the FDIC's Information Security Program - 2016** November 2, 2016	The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the FDIC, to perform annual independent evaluations of their information security programs and practices and to report the results to OMB. The FDIC Office of Inspector General (OIG) engaged the professional services firm of Cotton & Company LLP (C&C) to conduct this performance audit. The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. C&C found that the FDIC had established a number of information security program controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. For example, the FDIC had established policies in most of the security control areas that C&C reviewed; engaged an outside firm to test internal network security controls; and provided security awareness training to network users. The FDIC had also taken steps to strengthen its security program controls following the 2015 FISMA audit. The report contains six new recommendations addressed to the Chief Information Officer that are intended to improve the effectiveness of the FDIC's information security program and practices.	6	3	NA
EVAL-17-002 **OIG Hotline Complaints Regarding Employee Travel** December 15, 2016	The FDIC OIG initiated an evaluation in response to two February 2016 OIG Hotline complaints regarding employee travel. The complainants alleged that certain FDIC employees were (1) traveling excessively and unnecessarily at the FDIC's expense; (2) designated as Work in Place (WiP), but incurring significant commuting expenses; and (3) traveling frequently enough to invoke tax consequences that were not addressed by the FDIC and the employees. The objective of the evaluation was to assess the merits of the complaints. We concluded that some of the allegations involving the travel patterns of the FDIC employees had merit. We also found that the FDIC lacks a formal policy for the WiP program that defines the program objective and establishes parameters for its use and there were differing views among divisions on when it was appropriate to offer such arrangements to employees. We also questioned the necessity and reasonableness of costs associated with a former FDIC executive's travel, over an extended period of time. The report contains eight recommendations to address observations identified in the report and strengthen policy and controls surrounding long-term taxable travel, the WiP program, and processes for identifying and monitoring unusual or questionable travel patterns. The report also contains a recommendation to disallow and attempt to recover $122,423 in costs associated with the executive's travel.	8	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-17-004 **Technology Service Provider Contracts with FDIC-Supervised Institutions** February 14, 2017	Financial institutions increasingly rely on technology service providers (TSPs) to provide or enable key banking functions. Every financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information, including when such financial institution customer information is maintained, processed, or accessed by a TSP. Based on results from two prior evaluations, we determined that greater scrutiny of the sufficiency of TSP contracts with FDIC-supervised institutions was warranted. Our evaluation objective was to assess how clearly FDIC-supervised institutions' contracts with TSPs address the TSPs' responsibilities related to (1) business continuity planning and (2) responding to and reporting on cybersecurity incidents. We did not see evidence that most of the FDIC-supervised institutions we reviewed fully considered and assessed the potential impact and risk that TSPs may have on the financial institutions' ability to manage their own business continuity planning and incident response and reporting operations. Institutions' contracts with TSPs typically did not clearly address TSP responsibilities and lacked specific contract provisions to protect financial institutions' interests. While the FDIC independently and the Federal Financial Institutions Examination Council members collectively took numerous steps to provide institutions comprehensive business continuity, cybersecurity, and vendor management guidance, as well as enhance examination programs, we concluded that more time is needed to allow those efforts to have an impact. The report contains two recommendations for the FDIC to continue communication efforts; and, at an appropriate time, to conduct a follow-on study to assess the extent that financial institutions have effectively addressed key issues.	2	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-17-003 **The FDIC's Failed Bank Data Services Project** March 27, 2017	The FDIC, as receiver for a failed financial institution, acquires control of the institution's records and generally must maintain them in accordance with the Federal Deposit Insurance Act for at least 6 years. Maintaining these records is critically important as they are used by various internal and external stakeholders, including outside counsel, to support such activities as investigations, litigation, customer service, tax administration, research, and asset sales. The FDIC's Failed Bank Data Services (FBDS) project established a new contract and system to facilitate this important task. The objective of this performance audit was to determine (1) the status of the project, including progress and costs in relation to goals, budgets, and milestones; (2) factors contributing to the project's progress; and (3) significant issues or risks that must be addressed to achieve project success. The FDIC had a number of significant achievements associated with the FBDS project, but the project did not meet key milestones and costs exceeded estimates. We found that FDIC personnel did not fully understand the project's scope and requirements at the outset, establish clear expectations for all aspects of the project in contract documents, and implement a formal project management framework to guide and structure project activities. FDIC personnel identified other factors that impacted the project's status, including technical challenges and the unanticipated failure of a large, complex financial institution. The report contains seven recommendations to strengthen FBDS governance, project management, and contract oversight to reduce FBDS project-related risks going forward.	7	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				
AUD-17-005 August 15, 2017	*Material Loss Review of Seaway Bank and Trust Company, Chicago, Illinois*			
Receivership Management				
EVAL-17-006 July 13, 2017	*FDIC's Process for Filling Certain DRR Time-Limited Positions*			
Resources Management				
AUD-17-004 June 8, 2017	*Follow-on Audit of the FDIC's Identity, Credential, and Access Management (ICAM) Program*			
EVAL-17-005 June 8, 2017	*The FDIC's Controls over the Information Technology Hardware Asset Management Program*			
EVAL-17-007 September 18, 2017	*Controls over Separating Personnel's Access to Sensitive Information*			
AUD-17-006 September 29, 2017	*The FDIC's Processes for Responding to Breaches of Personally Identifiable Information*			
Totals for the Period		**$0**	**$0**	**$0**

Table IV: Audit and Evaluation Reports Issued with Questioned Costs

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

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

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

Table VI: Status of OIG Recommendations Without Management Decisions

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

Table VII: Status of OIG Reports Without Comments

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

Table VIII: Significant Revised Management Decisions

In our November 2013 audit report, entitled *Independent Evaluation of the FDIC's Information Security Program—2013* (Report Number AUD-14-002), we noted that Homeland Security Presidential Directive-20, National Continuity Policy, (HSPD-20) and the Federal Emergency Management Agency's (FEMA) Federal Continuity Directives 1 and 2 (FCDs) required the FDIC to continuously perform its mission essential functions (MEFs) that support the FDIC's primary mission essential function (PMEF), or resume them within 12 hours of an emergency event. However, the FDIC had established a recovery time objective for all of its mission-critical IT systems and applications of 72 hours after an emergency declaration or business disruption. Accordingly, we recommended that the FDIC address potential gaps that may exist between the 12-hour minimum timeframe required to restore MEFs following an emergency and the 72-hour recovery time objective for restoring mission-critical IT systems and applications.

FDIC management concurred with the recommendation and indicated that it would establish a working group to assess the Corporation's Continuity of Operations Plan and identify potential gaps in support service recovery capabilities (including IT systems and applications). At the conclusion of this effort, a set of options and recommendations would be presented to FDIC executive management to either accept identified risks or authorize resources to close identified gaps. All of these actions were to be completed by December 31, 2014.

Our office held several meetings with FDIC management during 2017 to discuss the status of corrective actions to address the recommendation. Management noted that, subsequent to the issuance of our recommendation, HPSD-20 had been replaced by Presidential Policy Directive-40, National Continuity Policy, and FEMA had updated its FCDs to clarify continuity requirements imposed on federal agencies. In light of these changes, FDIC management notified our office on September 27, 2017 that it had taken alternative corrective action to address the recommendation. Specifically, management provided us with a written plan and other materials describing the actions the Corporation had taken to address the recommendation and management's approach for addressing federal continuity policy requirements going forward. These materials indicate that the FDIC is updating its Business Process Analysis and Business Impact Analysis for the purpose of validating its PMEF and supporting MEFs. The materials reference various planned and ongoing initiatives aimed at strengthening the resiliency and availability of the FDIC's mission-critical IT systems and applications. As of the end of the reporting period, we were reviewing these materials to determine whether they are responsive to the recommendation.

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: **49**

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: **None**

Number of indictments and criminal Informations: **57**

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 41 individuals, 9 business entities, and 3 instances where the case was referred but the subjects are unknown at this time. Our total indictments and criminal Informations includes indictments, Informations, and superseding indictments.

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

During this reporting period, there were no such allegations or referrals to DOJ.

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 the reporting period, there were no evaluations or audits closed. There were no investigations involving senior government employees that were closed.

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, 2017 through September 30, 2017
(for failures that occur on or after January 1, 2014 causing losses to the DIF of less than $50 million)

Institution Name	Closing Date	Estimated Loss to the DIF (Dollars in Millions)	Grounds Identified by the State Bank Supervisor for Appointing the FDIC as Receiver	Unusual Circumstances Warranting In-depth Review?
Reviews Ongoing				
Proficio Bank (Cottonwood Heights, Utah)	3/3/17	$11.0		

Peer Review Activity

Federal Inspectors General are required to engage in peer review processes related to both their audit and investigative operations. The FDIC OIG is reporting the following information related to its peer review activities. These activities cover our most recent roles as both the reviewed and the reviewing OIG and relate to both audit and investigative peer reviews.

Audit Peer Reviews

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

- The 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.

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.

FDIC OIG Peer Review of the Tennessee Valley Authority OIG

The FDIC OIG completed a peer review of the system of quality control for the audit organization of the Tennessee Valley Authority (TVA) OIG, and we issued our final report to that OIG on May 16, 2017. We reported that in our opinion, the system of quality control for the audit organization of the TVA OIG, in effect for the 12 months ended September 30, 2016, had been suitably designed and complied with to provide the TVA OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. The TVA OIG received a peer review rating of pass.

We also issued a letter of comment to the TVA OIG that set forth findings and recommendations that were not considered to be of sufficient significance to affect our overall opinion.

TVA OIG posted the peer review report on its Website at http://oig.tva.gov/peer_reports.html.

Investigative Peer Reviews

Quality assessment peer reviews of investigative operations are conducted on a 3-year cycle as well. 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. For our office, applicable Attorney General Guidelines include the Attorney General Guidelines for Offices of Inspectors General with Statutory Law Enforcement Authority (2003), Attorney General Guidelines for Domestic Federal Bureau of Investigation Operations (2008), and Attorney General Guidelines Regarding the Use of Confidential Informants (2002).

- The Department of the Treasury OIG conducted the most recent 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 February 1, 2016. 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 December 31, 2015, was in compliance with quality standards established by CIGIE and applicable Attorney General guidelines. These safeguards and procedures provided reasonable assurance of conforming with professional standards in the planning, execution, and reporting of FDIC OIG investigations.
- The FDIC OIG conducted a peer review of the investigative function of the Environmental Protection Agency (EPA) OIG. We issued our final report to EPA OIG on December 2, 2014. We reported that, in our opinion, the system of internal safeguards and management procedures for the investigative function of the EPA OIG in effect for the period October 1, 2012 through September 30, 2013 was in compliance with the quality standards established by CIGIE and Attorney General Guidelines.

At the end of the reporting period, our office was completing its peer review of the investigative operations of the Small Business Administration OIG. We will include those results in our next semiannual report.

Congratulations and Farewell

Congratulations to FDIC OIG CIGIE Award Winners, whose work was recognized at the annual Awards Ceremony on October 19, 2017:

Awards for Excellence

Jill Benham, Audit Specialist, and Laura Benton, Audit Manager
In recognition of Completing an Audit of the FDIC's Process for Identifying and Reporting Major Information Security Incidents.

Esteban Santana, Special Agent, Dallas
In recognition of Uncovering a Multi-Million Dollar Fraud Scheme at First State Bank of Altus.

Frank Coppola, Special Agent, New York
In Recognition of the Team's Outstanding Efforts and Contributions Related to the Successful Multi-Agency Criminal Investigation and Prosecution of Multiple Defendants in the Steven Hameed et al. Criminal Case.

Luke Itnyre, Auditor in Charge, and Andrew Godfrey, Auditor
For their team effort on an audit conducted while at the Small Business Administration OIG in identifying improvement opportunities for the oversight of 7(a) loans that will promote efficiency and reduce risk to taxpayers.

Fran Mace, Deputy Assistant Inspector General for Investigations
For his work conducted while at the Department of Defense on the Southwest Asia Procurement Fraud Investigative Team.

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

Jay Chappell retired after 28 years of federal service. He began his career at the Federal Home Loan Bank Board, which merged with the FDIC in October 1989. Jay served as a criminal investigator in the FDIC OIG and became a supervisory criminal investigator charged with leading the OIG's Electronic Crimes Unit in February 2006.

Dan Bergan retired from the OIG after almost 29 years of federal service. His career included service at the Department of the Army, Department of Housing and Urban Development, and Internal Revenue Service. He joined the FDIC OIG's Chicago Office as a criminal investigator in January 2004.

Townhall Meetings

April 5, 2017

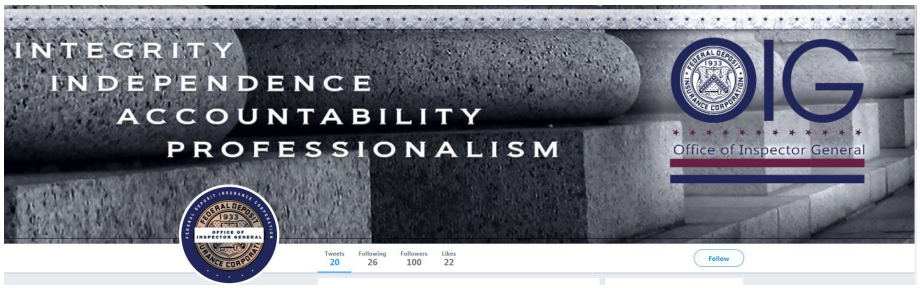
FDIC OIG management and staff from the OIG's headquarters and field locations join to discuss the OIG's audits, evaluations, investigations, and other office priorities.

FDIC Chairman Martin J. Gruenberg (above left) and FDIC Vice Chairman Thomas M. Hoenig (right) shared their perspectives on issues facing the FDIC with OIG senior management and staff.

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 New 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

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

Whistleblowers can contact the OIG's Whistleblower Ombudsperson through the Hotline by indicating: Attention: Whistleblower Ombudsperson.

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