Office of Inspector General

Semiannual Report to the Congress

OCTOBER 1, 2016 – MARCH 31, 2017

FDIC
Federal Deposit Insurance Corporation

The Federal Deposit Insurance Corporation (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 6,100 individuals carry out the FDIC mission throughout the country. According to most current FDIC data, the FDIC insured more than $6.91 trillion in deposits in 5,913 institutions, of which the FDIC supervised 3,787. As a result of institution failures during the financial crisis, the balance of the Deposit Insurance Fund turned negative during the third quarter of 2009 and hit a low of negative $20.9 billion by the end of that year. The FDIC subsequently adopted a Restoration Plan, and with various assessments imposed over the past few years, along with improved conditions in the industry, the Deposit Insurance Fund balance has steadily increased to a positive $83.2 billion as of December 31, 2016. Receiverships under FDIC control as of December 31, 2016, totaled 378, with about $3.3 billion in assets.

On July 14, 2017, the Office of Inspector General reissued this semiannual report to correct information contained in the original report in Table 1 on pages 53-54. The corrections reflected in this report pertain to significant recommendations from previous semiannual reports on which corrective actions have not been completed.

Office of Inspector General

Semiannual Report to the Congress

October 1, 2016 – March 31, 2017

Federal Deposit Insurance Corporation

Inspector General's Statement

I am pleased to present the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General's (OIG) Semiannual Report for the period October 1, 2016 through March 31, 2017. This is my first such Report since being sworn in as the FDIC Inspector General on January 9, 2017. I am honored to hold this position, and my Office will continue to serve the public and carry out the IG mission with the highest ideals of independent oversight: integrity, fairness, objectivity, thoroughness, and accountability. The work highlighted in this Report reflects these principles and illustrates the importance of our work for the Corporation and the financial sector.

During the reporting period, we issued 7 audit and evaluation reports, made 27 nonmonetary recommendations to strengthen controls in FDIC programs and operations, and identified questioned costs of $126,593. Our work covered diverse topics such as information security; technology service provider contracts with financial institutions; monitoring of Systemically Important Financial Institutions; efforts to ensure shared loss agreement recoveries are remitted; the FDIC's contracts related to managing failed bank data as receiver for failed institutions; and the Work in Place program and related travel expenses.

Our investigations of criminal activity affecting the FDIC and the banking industry resulted in 65 indictments and informations; 54 convictions; 25 arrests; and fines, restitution, and asset forfeitures totaling nearly $75 million. As we discuss in this Semiannual Report, we investigated many former bank officers and directors who misused their positions, and business owners who colluded to obtain funding from financial institutions fraudulently. These individuals are being held accountable through prison sentences and restitution ordered, including one defendant who was sentenced to 3 years in prison and ordered to pay more than $97 million, joint and several with a conspirator, for his role in a complex fraud scheme.

Also of note during the reporting period, on December 16, 2016, the Inspector General Empowerment Act of 2016 was enacted. This legislation amends the IG Act of 1978 to include new provisions designed to support and strengthen IG independence. We are currently implementing certain provisions of the Act, including addressing several new requirements in this Semiannual Report, at Appendix1.

Since joining the OIG, I have identified significant challenges facing the FDIC and the financial sector, particularly with respect to information technology (IT) risks. In addition, our office is seeking to expand our capabilities to conduct robust evaluations of FDIC programs. To address these two factors, I recently announced a reorganization of the OIG's audit and evaluation function. We have created a new Office of IT Audits and Cyber (ITC) and a separate Office of Program Audits and Evaluations (PAE). The ITC office will conduct audits of IT risks and challenges, both internal to the FDIC's own systems and external to banks and the financial sector. The PAE office will conduct program evaluations and performance audits to assess the effectiveness of FDIC operations and perform reviews of failed banks, compliance matters, and other systemic issues. In addition, Stephen Beard will take on a new role as the Deputy IG for Strategy and Performance and will focus on organizational initiatives to enhance efficiency for our Office.

In closing, I would like to acknowledge FDIC OIG personnel, members of the FDIC Board of Directors and management, colleagues in the IG community, law enforcement partners, and Members of Congress and their staff, all of whom have supported the Office and facilitated my transition to the FDIC. Also, I want to express my sincere gratitude to Frederick Gibson for his leadership as the Acting IG for more than 3 years prior to my appointment. With continued and strong support, I look forward to confronting the challenges ahead.

Jay N. Lerner
Inspector General
April 2017

Table of Contents

Acronyms and Abbreviations

AI	assuming institution
BDO	BDO USA, LLP
BFB	Broadway Federal Bank
C&C	Cotton & Company LLP
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISO	Chief Information Security Officer
CO	Counsel's Office
CY-4	Washington Field Office Cyber Squad-4
DATA Act	Digital Accountability and Transparency Act of 2014
DIF	Deposit Insurance Fund
DMS	Data Management Services
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOJ	Department of Justice
DRR	Division of Resolutions and Receiverships
EAR	Equipment Acquisition Resources, Inc.
ECU	Electronic Crimes Unit
FBDS	Failed Bank Data Services
FBI	Federal Bureau of Investigation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FI	financial institution
FISMA	Federal Information Security Modernization Act of 2014

GAO	Government Accountability Office
HBN	Heritage Bank of Nevada
IG	Inspector General
IRS-CI	Internal Revenue Service-Criminal Investigations
IT	information technology
ITC	Office of IT Audits and Cyber
LSB	Lincoln Savings Bank
MTD	Machine Tools Direct, Inc.
NARA	National Archives and Records Administration
NCIJTF	National Cyber Investigative Joint Task Force
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
PAE	Office of Program Audits and Evaluations
PII	personally identifiable information
RMS	Division of Risk Management Supervision
SAR	Suspicious Activity Report
SIFI	systemically important financial institution
SIGTARP	Office of the Special Inspector General for the Troubled Asset Relief Program
SLA	shared loss agreement
TSP	technology service provider
VPB	Vantage Point Bank
WiP	Work in Place

Highlights and Outcomes

The FDIC OIG has conducted its work during the past 6-month period in five goal areas that are linked to the OIG's mission. A summary of our completed work during the reporting period, along with references to selected ongoing assignments, is presented below, by goal area.

Goal 1: Quality Audits and Evaluations

Conduct quality audits, evaluations, and other reviews to ensure economy, efficiency, and effectiveness in FDIC programs and operations

We issued three final audit and four final evaluation reports during the reporting period. Of note, we issued the results of an audit that assessed how clearly FDIC-supervised institutions' contracts with technology service providers (TSP) address the TSP's responsibilities related to business continuity planning and responding to and reporting on cybersecurity incidents. In reviewing a sample of 48 TSP contracts from 19 financial institutions, we did not see evidence in the form of risk assessments or contract due diligence that most FDIC-supervised institutions we reviewed fully considered and assessed the potential impact and risk that TSPs may have on the institution's ability to manage its own business continuity planning and incident response and reporting operations. We made recommendations to address these concerns and FDIC management agreed to take action. We also issued the results of our 2016 review under the Federal Information Security Modernization Act (FISMA) of 2014. We noted in that report that the FDIC had established a number of 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 Science and Technology standards and guidelines. Notwithstanding these actions, we identified security control weaknesses that impaired the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at elevated risk. Management agreed with the six recommendations we made to strengthen information security controls.

In another review of the FDIC's efforts to ensure assuming institutions identify and remit shared loss agreement recoveries to the FDIC, we determined that the FDIC had established controls to mitigate risks and help ensure the assuming institutions appropriately identify and remit recoveries. In fact, we identified several overpayments to the FDIC that were addressed during the audit. Another assignment related to receivership operations involved the FDIC's Failed Bank Data Services (FBDS) project. FBDS is an important system used to maintain records associated with failed institutions when the FDIC becomes the receiver. The FBDS project involved transitioning all legacy data and services from a prior system and contractor to a new contract with CACI-ISS, Inc. We found that the project had not met key milestones and costs exceeded estimates. The transition-related schedule delays caused the FDIC to extend the prior contract several times into 2016—beyond the initially anticipated contract expiration date. As a result of those extensions, and other challenges, the FDIC absorbed about $14.6 million more in transition-related costs than had been estimated. Our office made seven recommendations to strengthen FBDS governance, project management, and contract oversight to reduce FBDS project-related risks going forward.

We also conducted an evaluation in response to two OIG Hotline complaints regarding employee travel. The complainants alleged that certain FDIC employees were traveling excessively and unnecessarily at the FDIC's expense; designated as Work in Place but incurring significant commuting expenses; and traveling frequently enough to invoke tax consequences that were not addressed by the FDIC and the employees involved. We made eight recommendations to strengthen policy and controls surrounding long-term taxable travel, the Work in Place program, and processes for identifying and monitoring unusual or questionable travel patterns. We also recommended that the FDIC disallow and attempt to recover $122,423 in costs associated with an Executive's travel that we found to be unnecessary and unreasonable.

Ongoing assignments in support of this goal are covering such issues as the FDIC's governance of information technology (IT) initiatives, controls for responding to breaches of personally identifiable information (PII), controls for preventing and detecting advanced persistent threats, IT hardware asset management, hiring practices in the Division of Resolutions and Receiverships (DRR), FDIC non-headquarters physical security, progress made in addressing credentialing and multi-factor authentication activities, and a material loss review of a failed FDIC-supervised institution.

Goal 2: Impactful Investigations

Investigate criminal activities affecting financial institutions and conduct other investigative activities to ensure integrity in the banking industry and FDIC internal operations

Our Office of Investigations continued its work addressing criminal activity affecting both open and closed financial institutions. A number of cases we highlight in this report were referred to us by the FDIC's Division of Risk Management Supervision (RMS) and DRR. Cases during the reporting period included those involving former bank directors and officers, employees of the bank, real estate professionals, businessmen, and other bank customers.

To illustrate–the former president and chairman of First State Bank of Altus, Altus, Oklahoma, was sentenced to 48 months in prison after a jury convicted him in July 2016 of bank fraud, conspiracy to commit bank fraud, misapplication of bank funds, making a false bank entry, unauthorized issuance of a bank loan in connection with First State Bank of Altus, and various loan schemes. He was also ordered to pay $10,120,166.58 in restitution to the FDIC.

A former bank branch manager at First Tennessee Bank, N.A., Memphis, Tennessee, was sentenced to serve 36 months in federal prison for embezzlement of funds and tax evasion, to be followed by 5 years of supervised release. He was also ordered to pay restitution in the amounts of $844,254 to First Tennessee Bank, $161,018 to the Internal Revenue Service, and $81,014 to two additional victims of his crimes, for a total of $1,086,286. Of the total amount he embezzled, the former bank manager obtained approximately $967,573 for his personal use. He lost or spent most of this through on-line gambling on various Websites and making payments on various personal consumer debts.

In another case, two developers of the Indian Ridge Resort located in Branson, Missouri, were sentenced in the District of Kansas. They were each sentenced to serve 60 months in prison to be followed by 24 months of supervised release. The wife of one of developers was sentenced to 36 months of supervised release. On May 27, 2015, the three each entered guilty pleas for their role in a real estate construction fraud scheme charging them with bank fraud, conspiracy to commit bank fraud, money laundering, and conspiracy to commit money laundering.

A businessman, the owner and president of Machine Tools Direct, Inc., was sentenced to serve 36 months in prison and was ordered to pay restitution of $97,331,250 for his role in a wire fraud scheme. He and a business partner were indicted on February 27, 2014, and charged with mail fraud, bank fraud, and wire fraud.

In another case, a former vice president and Bank Secrecy Act officer of a Maryland bank pleaded guilty 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. 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 associated with her and her family members. Three of the six victim customers were at least 80 years old, and for two of the accounts, the customers were deceased.

Finally, of note, in one of our employee cases, a former senior capital markets specialist employed by the FDIC was sentenced to serve 2 years of probation in connection with his prior plea of guilty to a misdemeanor charge of intentionally exceeding authorized access to an FDIC computer to obtain information. Between January 2011 and September 2012, he emailed over 900 FDIC documents to his personal email account, including sensitive, confidential, and strictly private information regarding and belonging to systemically important financial institutions.

Office of Investigations special agents continued to partner with U.S. Attorney's Offices throughout the country and participated actively in working groups with law enforcement partners to leverage knowledge and better address issues of mutual concern. Our special agents also offered training in money laundering investigations, and engaged in outreach with groups both internal and external to the FDIC to explain Office of Investigations' role in combatting criminal activity causing harm to the banking system. Overall investigative results for the reporting period attest to the value of solid working relationships with the Corporation, other OIGs, and law enforcement partners. Our investigations during the past 6 months led to 65 indictments; 54 convictions; 25 arrests; and potential fines, restitution, and asset forfeitures totaling nearly $75 million.

Goal 3: Effective Communications
Communicate effectively with internal and external stakeholders

In support of this goal, we continue to reexamine the information needs of the OIG's stakeholders, including the FDIC Board of Directors and FDIC division and office management and their staffs, the Congress, members of the Inspector General (IG) community, the Government Accountability Office (GAO), OMB, the media, and the general public. We do so in the interest of ensuring that our communications are effective and that the messages we convey are transparent, informative, and clearly understood.

We place a high priority on maintaining positive working relationships with the FDIC Chairman, Vice Chairman, other FDIC Board members, and management officials. During the reporting period, the Acting IG, new IG, and other OIG senior executives met regularly with the Chairman and Vice Chairman, attended FDIC Board meetings, and presented the results of completed work at FDIC Audit Committee meetings.

We also maintained positive relationships with the Congress and provided timely responses to a number of congressional inquiries. Congressional interaction during the reporting period included the IG meeting with congressional staff, as well as the Chairman of the Committee on Science, Space, and Technology of the House of Representatives. The IG updated Committee Chairman Lamar Smith on our office's IT-related work. The IG also met with staff from the House Committees on Financial Services and Oversight and Government Reform, and the Senate Committees on Banking and Homeland Security and Governmental Affairs.

The OIG fully supported and participated in IG community activities through the Council of the Inspectors General on Integrity and Efficiency (CIGIE). We coordinated with representatives from the other financial regulatory OIGs and others in the IG community on issues of mutual interest. We answered multiple data calls for information; participated in several CIGIE working groups, including one that addressed new semiannual and other reporting requirements under the IG Empowerment Act; and participated in the Federal Audit Executive Council's DATA Act Working Group. Also, in this regard, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) created the Financial Stability Oversight Council and further established the Council of Inspectors General on Financial Oversight (CIGFO). 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. We attended CIGFO meetings and participated on a CIGFO working group that evaluated and reported on the Financial Stability Oversight Council's efforts to promote market discipline.

We continue to field allegations through our Hotline system and receive inquiries on varied topics from the public through other means, and we make every effort to respond timely to such contacts. During the reporting period, several of the Hotline allegations we received warranted further review, and we pursued those. We also issued a report stemming from an earlier Hotline complaint related to FDIC employee travel, as discussed elsewhere in this report. We completed the Office of Special Counsel's 2302(c) certification program and are now better positioned to inform employees of the rights of Whistleblowers and the remedies available to Whistleblowers under federal law.

We are in the process of updating and refining our Congressional protocols and also developing a more formal and effective means of handling media requests and inquiries. Ongoing efforts to redesign our external Website are intended to provide more useful content and better serve all stakeholders.

Goal 4: Enhanced Understanding of Emerging Issues

Continuously seek to enhance OIG knowledge and understanding of emerging and evolving issues affecting the FDIC, OIG, and insured depository institutions

Our attention to better understanding of emerging issues continued to focus on two matters in particular during the reporting period. First, we continued to expand our involvement and knowledge of cyber security matters in several ways. One of our senior managers serves as a cybersecurity liaison officer to proactively monitor cyber issues and trends from multiple sources and disseminate pertinent information to interested or affected parties both internal and external to the FDIC. He monitors activities of the Corporation's Data Breach Management Team and is a member of the Corporation's Insider Threat and Counterintelligence Program working group. Our information security manager, IT professionals in the former Office of Audits and Evaluations, members of the OIG's Electronic Crimes Unit, and a Special Advisor to the Acting IG play key roles in the cybersecurity arena. Working together, these resources keep current on possible threats to ensure our readiness to address them. We also continued our active participation at the Federal Bureau of Investigation's (FBI) Cyber Task Force in Washington, D.C. and continue to devote an investigative resource to the National Cyber Investigative Joint Task Force. These efforts are paying dividends in terms of increased knowledge and productive networking and information-sharing opportunities. Ongoing audits and evaluations are addressing significant information security topics and those efforts further expand our knowledge base. Additionally, the IG's recent reorganization created an Office of IT Audits and Cyber, and we anticipate this group will further strengthen the OIG's knowledge and understanding of IT issues and emerging cyber threats.

A second priority area of focus for our office is on the implications of the Dodd-Frank Act, and in particular, on the responsibilities that our office would be required to fulfill were a systemically important financial institution to fail. Under current law, these responsibilities would include analyses and reporting on various aspects of the FDIC's liquidation of any covered financial company by the Corporation as receiver under Title II of the Act. We researched the impact of such responsibilities and identified issues relating to scope, frequency, reporting, funding, and coordination efforts that would be needed to successfully meet the mandate of the Dodd-Frank Act. We are continuing to monitor the status of the Dodd-Frank Act requirements, and will respond to those accordingly.

Goal 5: Operational Efficiency and Workforce Excellence

Maximize OIG operational efficiency and workforce excellence

We have devoted ongoing attention to enhancing operational efficiencies and workforce excellence. With an emphasis on our human resources and the talents needed for OIG success, we 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. To that end, we formulated our fiscal year 2018 budget request and received the FDIC Chairman's approval of that request for $39.1 million to fund 144 authorized positions, up 7 from fiscal year 2016. We brought on board a number of new hires during the reporting period—six new audit and evaluation staff, and three criminal investigators. We also 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 and enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities. Finally, OIG senior management announced several new awards to recognize OIG staff: Distinguished Professional Award, Spirit of the OIG Award, and IG Award for Excellence.

During the reporting period, we continued to transition to a new investigative case management system and continued to better track audit and evaluation assignment milestones and costs and to manage audit and evaluation records located in TeamMate or other electronic repositories. In a related vein, we continued efforts to update the OIG's records and information management program and practices to ensure an efficient, effective, and secure means of collecting, storing, and retrieving needed information and documents. In the interest of preserving OIG independence and protecting OIG information, we sought best practices in meetings with other OIGs to discuss their IT environments in relation to their agencies' IT environments. We took additional steps to maintain a secure, effective, and reliable IT environment and educate OIG staff so that we can leverage the tools we use to conduct our work more efficiently.

We undertook strategic planning efforts for each of the OIG's offices, taking into consideration the goals of, and risks to, FDIC corporate programs and operations and those risks more specific to the OIG. We considered resource needs, budgetary constraints, and other challenges to accomplishing our mission. We are incorporating such information in broader discussions as we plan for the future.

Significant Outcomes (October 1, 2016–March 31, 2017)	
Audit and Evaluation Reports Issued	7
Questioned Costs or Funds Put to Better Use	$126,593
Nonmonetary Recommendations	27
Investigations Opened	40
Investigations Closed	57
OIG Subpoenas Issued	10
Judicial Actions:	
Indictments/Informations	65
Convictions	54
Arrests	25
OIG Investigations Resulted in:	
Fines	$342,500.00
Restitution	41,735,550.13
Asset Forfeitures	21,303,719.39
Civil Recoveries	11,525,428.00
Total	$74,907,197.52
Referrals to the Department of Justice (U.S. Attorney)	68
Proposed Regulations and Legislation Reviewed	18
Responses to Requests Under the Freedom of Information/Privacy Act	16

Goal 1: Quality Audits and Evaluations

Conduct quality audits, evaluations, and other reviews to ensure economy, efficiency, and effectiveness in FDIC programs and operations

The OIG's work in support of this goal during the reporting period was largely the responsibility of the OIG's former Office of Audits and Evaluations, which, as noted in the IG's statement, has recently been reorganized. The OIG's Office of Audits provided the FDIC with professional audit and related services covering the full range of its statutory and regulatory responsibility, including major programs and activities. These audits were designed to promote economy, efficiency, and effectiveness and to prevent fraud, waste, and abuse in corporate programs and operations. This office ensured the compliance of all OIG audit work with applicable audit standards, including those established by the Comptroller General of the United States. It also conducted the external peer review of the audit organization of another OIG, according to the cycle established by CIGIE, the results of which we will include in our next semiannual report.

The OIG's former Office of Evaluations was responsible for reviewing and analyzing FDIC programs and activities to provide independent, objective information to facilitate FDIC management decision-making and improve operations. Evaluation projects discussed below were conducted in accordance with the Quality Standards for Inspection and Evaluation. Such evaluation projects are generally more limited in scope than audits are and may be requested by the FDIC Board of Directors, FDIC management, or the Congress.

Prior to passage of the Dodd-Frank Act, in the event of an insured depository institution failure, the Federal Deposit Insurance Act (FDI Act) required the appropriate regulatory OIG to perform a review when the Deposit Insurance Fund (DIF) incurs a material loss. Under the FDI Act, a loss was considered material to the insurance fund if it exceeded $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. These reviews identify what caused the material loss and evaluate the supervision of the federal regulatory agency, including compliance with the Prompt Corrective Action requirements of the FDI Act.

Importantly, under the Dodd-Frank Act, the OIG is now required to review all losses incurred by the DIF under the thresholds to determine (a) the grounds identified by the state or federal banking agency for appointing the Corporation as receiver and (b) whether any unusual circumstances exist that might warrant an in-depth review of the loss. Although the number of failures continues to decline, we conduct and report on material loss reviews and in-depth reviews of failed FDIC-supervised institutions, as warranted, and continue to review all failures of FDIC-supervised institutions for any unusual circumstances.

The assignments discussed below take into account results of the OIG's planning process, which included establishing an inventory of all FDIC programs and activities, evaluating the significance and risk of those programs and activities, and considering management and Congressional interest and statutorily-required reviews. Going forward, as part of the reorganization of the audit and evaluation function, the OIG will continue to ensure that all audits and evaluations are relevant, timely, and assist the Corporation in efficiently and effectively carrying out its mission, programs, and operations. The former Office of Audits and Evaluations also undertook various operational and quality assurance initiatives aimed at improving the consistency and efficiency of its processes and quality of its products; recruiting, developing, and engaging staff; leveraging technology more fully in audits and evaluations; and preparing to address OIG reporting requirements under the Dodd-Frank Act. Of particular importance to the new Office of IT Audits and Cyber will be completion of a multi-year IT coverage framework to help guide our work in this area and ensure systematic, risk-based audits of key operations and activities.

Finally, during the reporting period, in light of increased IG community and Congressional interest in the status of OIG recommendations, we modified our process for closing recommendations that we make to FDIC management. The FDIC Chairman and Vice Chairman agree that an OIG recommendation is not closed until the OIG has reviewed the FDIC's corrective actions and is satisfied that the actions are sufficient to address the recommendation. We plan to review the FDIC's corrective actions in a timely manner, aiming for a target of reviewing the actions within 30 days, and if we are not able to complete our review in this timeframe, we will advise the FDIC's Office of Corporate Management Control and the relevant division(s), so that there is a clear understanding of the status of the recommendation. In addition, we will monitor cases where the Corporation extends the planned completion dates for implementing OIG recommendations. We anticipate continued discussions with the Chairman, Vice Chairman, and FDIC management on open recommendations going forward.

OIG Work in Support of Goal 1

In support of this goal during the reporting period, we issued seven reports. These reports contain 27 nonmonetary recommendations, identify questioned costs of $126,593, and span various FDIC programs and activities, including TSP contracts with FDIC-supervised institutions, FISMA 2016, FDIC efforts to ensure shared loss agreement recoveries are identified and remitted, the FDIC's FBDS project, risk monitoring of systemically important financial institutions, employee travel issues, and contract billings for receivership services. Our office also continued the legislatively mandated review of all failed FDIC-supervised institutions causing losses to the DIF of less than the threshold outlined in the Dodd-Frank Act to determine whether circumstances surrounding the failures would warrant further review. Our failed bank review activity is presented in Appendix II.

At the end of the reporting period, ongoing audit and evaluation assignments were addressing such issues as the FDIC's governance of IT initiatives, controls for responding to breaches of PII, controls for preventing and detecting advanced persistent threats, IT hardware asset management, hiring practices in DRR, FDIC non-headquarters physical security, progress made in addressing credentialing and multi-factor authentication activities, and a material loss review of a failed FDIC-supervised institution. Results of these ongoing assignments will be presented in an upcoming semiannual report.

The results of issued audit and evaluation reports are discussed in the following section.

FDIC-Supervised Institutions' Contracts with Technology Service Providers

Financial institutions (FI) increasingly rely on TSPs to provide or enable key banking functions. Every FI 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 FI 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. As a result, we conducted work to assess how clearly FDIC-supervised institutions' contracts with TSPs address the TSP's responsibilities related to (1) business continuity planning and (2) responding to and reporting on cybersecurity incidents.

By way of background, in 1999, Congress enacted the Gramm-Leach-Bliley Act. Section 501(b) required the federal banking agencies to establish appropriate standards for supervised FIs to protect customer information security and confidentiality. As required by the Gramm-Leach-Bliley Act, in February 2001, the financial regulators issued *Interagency Guidelines Establishing Standards for Safeguarding Customer Information,* requiring development and implementation of administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These Guidelines apply to customer information maintained by or on behalf of FDIC-insured FIs. They state that FIs should:

- exercise appropriate due diligence in selecting service providers;
- contractually require their TSPs to implement appropriate measures to meet the guidelines' objectives related to protecting against unauthorized access to or use of sensitive customer information; and
- monitor contract compliance by the TSPs consistent with the institution's risk assessment, to include reviewing service provider audits, test results summaries, or other equivalent evaluations.

In 2008, the FDIC issued a Financial Institution Letter (FIL) titled, *Guidance for Managing Third-Party Risk*, which emphasized that an institution's board of directors and senior management ultimately are responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships to the same extent as if the activity were handled within the institution. RMS has also reiterated these responsibilities in more recent guidance.

In conducting our work, we reviewed a sample of 48 TSP contracts from 19 financial institutions. We did not see evidence, in the form of risk assessments or contract due diligence, that most of the FDIC-supervised FIs we reviewed fully considered and assessed the potential impact and risk that TSPs may have on the FI's ability to manage its own business continuity planning and incident response and reporting operations. Documentation supported that only 8 of the 19 institutions completed both a risk assessment and contract review to understand the business and legal risks, as recommended by supervisory guidance. Further, when completed, the quality of these assessments varied.

Typically, FI contracts with TSPs did not clearly address TSP responsibilities and lacked specific contract provisions to protect FI interests or preserve FI rights. Contracts also did not sufficiently define key terminology related to business continuity and incident response. As a result, FI contracts with TSPs we reviewed provided FIs with limited information and assurance that TSPs could recover and resume critical systems, services, and operations timely and effectively if disrupted and would take appropriate steps to contain and control incidents and report them timely to appropriate parties.

In the past 2 years, the FDIC independently and the Federal Financial Institutions Examination Council (FFIEC) members collectively took numerous steps to provide institutions comprehensive business continuity, cybersecurity, and vendor management guidance, and to enhance the FDIC and FFIEC's IT examination programs. We concluded that more time is needed to allow FDIC and FFIEC efforts to have a demonstrable and measurable impact on FI and TSP contract language. In that regard, RMS officials noted that often FI contracts with TSPs are dated and do not reflect FDIC and FFIEC efforts to strengthen cybersecurity.

Although RMS does not expect FIs to renegotiate current contracts solely in response to recently issued guidance, it encourages FIs to discuss business continuity and incident response concepts, guidance, and expectations with their service providers. Finally, risks remain that FIs may attempt to transfer their inherent responsibility for FI continuity and information security to TSPs or may not be sufficiently knowledgeable about or engaged in contract management. These risks will require RMS's continued supervisory attention.

Notwithstanding the FDIC's efforts, we recommended that RMS continue to communicate to FIs the importance of (1) fully considering and assessing the risks that TSPs present, (2) ensuring that contracts with TSPs include specific detailed provisions that address FI-identified risks and protect FI interests, and (3) clearly defining key contract terms that would be important in understanding FI and TSP rights and responsibilities. We also recommended that, at an appropriate time, RMS study and assess to what extent FIs have effectively addressed these issues. The FDIC concurred with our recommendations.

Federal Information Security Modernization Act of 2014 — Results for 2016

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. We engaged the professional services firm of Cotton & Company LLP to conduct an audit to evaluate the effectiveness of the FDIC's information security program and practices. The audit included a review of selected security controls related to four general support systems and the FDIC's risk management activities related to an outsourced information service provider supporting asset servicing functions.

Our audit determined that the FDIC had established a number of information security program controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable National Institute of Standards and Technology standards and guidelines. For example, the FDIC had established policies in most of the security control areas that Cotton & Company LLP 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. Among other things, the FDIC:

- restricted (with limited exceptions) the ability of network users to copy information to removable media to reduce the risk of unauthorized exfiltration of sensitive information.
- identified and reported its high value assets to the Department of Homeland Security.
- updated its security control framework to address changes introduced by National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4,* dated April 2013.

Notwithstanding these actions, we identified security control weaknesses that impaired the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at elevated risk. We reported on a total of 17 findings, of which 6 were identified during the current year FISMA audit and the remaining 11 were identified in prior reports issued by the OIG or GAO. Findings from prior reports consisted of control weaknesses that the FDIC was working to address, but had not yet fully remediated, and, therefore, continued to pose risk to the FDIC. Of these, the most notable weaknesses pertained to strategic planning, vulnerability scanning, the FDIC's information security manager program, configuration management, technology obsolescence, third-party software patching, multifactor authentication, contingency planning, and service provider assessments.

At the close of the audit, the FDIC was working to strengthen the effectiveness of its information security program controls in a number of other areas. For example, the FDIC was working to:

- improve its incident response capabilities by developing an overarching incident response program guide, updating incident response policies and procedures, hiring an incident response coordinator, and better documenting incident investigative activities;
- enhance the effectiveness of its Data Loss Prevention tool and adopting Digital Rights Management software; and
- hire a permanent Chief Information Security Officer (CISO).

Our FISMA report also discussed a risk related to the FDIC's infrastructure services contract and an observation on recent turnover in the CISO position and whether the CISO's authorities enable the CISO to effectively address the responsibilities defined in FISMA.

We made six new recommendations addressed to the Chief Information Officer to improve the effectiveness of the FDIC's information security program and practices. The Chief Information Officer concurred with all six of the report's recommendations. With respect to the report's observation on the responsibilities, authorities, and recent turnover in the CISO position, the response indicated that management would consider the matter and document whether any changes to the CISO role are warranted.

FDIC Efforts to Ensure Assuming Institutions Remit SLA Recoveries

The FDIC first introduced shared loss agreements (SLA) as a part of selected Purchase and Assumption transactions in 1991 to reduce the FDIC's immediate cash outlays, provide continuity of banking services to failed bank customers, and move assets into the private sector. Under an SLA, the FDIC enters into a Purchase and Assumption Agreement with an assuming institution (AI) to absorb a portion of the loss (typically 80 percent) on a specified pool of assets.

We initiated an evaluation based on the risks associated with AIs identifying and remitting SLA recoveries to the FDIC. An increasing number of Commercial SLAs are becoming 5 years old, resulting in the end of SLA loss coverage but not the end of the 8-year recovery period, during which AIs are required to remit a portion of their recoveries to the FDIC. Our evaluation assessed the FDIC's efforts to ensure that AIs identify and remit SLA recoveries to the FDIC. A recovery typically comprises (1) funds paid by the borrower on assets that the AI previously charged off or experienced a loss on and received reimbursement from the FDIC pursuant to an SLA; or (2) gains from the sale of foreclosed property or SLA assets.

We determined that the FDIC's DRR established controls to mitigate risks and help ensure AIs appropriately identify and remit recoveries to the FDIC. These controls include a process for identifying recovery and non-recovery assets and conducting on-site reviews that focus on recoveries. DRR also issued guidance and provided training to DRR employees, AIs, and third-party contractors that DRR engages to complement its staff. The guidance and training communicate recovery period procedures and expectations.

A contractor that we engaged to test a sample of SLA assets pertaining to five AIs that we selected found several discrepancies. The contractor identified an unreported recovery of $16,423 at one AI as a result of an isolated oversight. The AI agreed with the finding and reimbursed the FDIC for the recovery, following the contractor's review.

At another AI, the contractor found that the institution overpaid the FDIC by $249,937 in recoveries ($257,060 in overpayments minus $7,123 in underpayments). The net over payment was due to internal control weaknesses and accounting software limitations at the AI. The AI stated that improved internal controls, processes, and software changes that have either been implemented or are underway should prevent similar findings from occurring in the future. The contractor also identified an additional SLA asset where the same AI may have overpaid the FDIC in recoveries by $19,526. The FDIC confirmed the contractor's findings during an onsite review of the AI in October 2016 and identified an additional $9,072 in overpayments. The AI planned to process adjustments totaling $278,535 to satisfy all OIG and FDIC questioned claims.

We recommended that the FDIC assess the progress made by the AI that overpaid the FDIC in implementing changes to ensure accurate identification and reporting of SLA recoveries to the FDIC. We also recommended that the FDIC review a sample of the AI's SLA certificates to determine whether errors similar to the ones identified by our review are prevalent with other SLA certificates, and take appropriate action. The FDIC concurred with our recommendations.

The FDIC's Failed Bank Data Services Project

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 FDI 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.

During the financial crisis in 2008, the FDIC entered into a contract with Lockheed Martin to provide a system and services (the Data Management Services or DMS) to collect, store, and search failed financial institution records. Lockheed owned the system and the FDIC owned the records in the system. By the end of 2014, the FDIC had over 500 banks that were in DMS and DMS housed over 900 terabytes of data and 20,000 databases. Also by the end of 2014, the FDIC had spent $450 million on DMS. The FDIC wanted to reduce costs and achieve newer technologies by entering into a new contract with CACI-ISS, Inc. to provide a system and services (the Failed Bank Data Services or FBDS) to replace DMS. The FBDS project included transitioning all legacy data and services from DMS to the new contractor.

We conducted an audit 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.

While the FDIC had a number of significant achievements associated with the FBDS project, we found that the project had not met key milestones and costs exceeded estimates. Specifically, there was a delay in implementing certain system capabilities and transitioning data from the prior contractor's system to the FBDS system. The transition-related schedule delays caused the FDIC to extend the prior contract several times into 2016—beyond the initially anticipated contract expiration date. As a result of those extensions, and other challenges, the FDIC absorbed about $14.6 million more in transition-related costs than estimated. Overall, total transition-related costs remained less than what was originally projected when the FDIC Board of Directors approved the project.

We identified three factors contributing to the project's status. Specifically, FDIC personnel did not fully understand the project's scope and requirements, did not establish clear expectations for the project in contract documents, and did not implement a project management framework to guide and structure project activities. FDIC personnel identified other factors that impacted the project's delays, including technical challenges and the unanticipated failure of a large, complex financial institution.

Our office made seven recommendations to strengthen FBDS governance, project management, and contract oversight to reduce FBDS project-related risks going forward. Specifically, the recommendations included: establishing additional governance over project changes and performance review; completing key project validation and acceptance activities; assessing and revising, as appropriate, FBDS-related contract oversight guidance; implementing an industry best practices project management framework; conducting a feasibility study to assess the desired level of capacity for FBDS; obtaining a process improvement plan, strategy, and guidance; and developing guidance for reviewing and revising contract performance metrics.

FDIC management concurred with our recommendations.

FDIC Monitoring of SIFIs—Risk to Default or Danger of Default

The FDIC is charged under the Dodd-Frank Act with responsibility for liquidating failing financial companies that pose a significant risk to the financial stability of the U.S. These financial companies are commonly known as systemically important financial institutions (SIFIs). We evaluated the progress the FDIC has made in developing criteria and a process for assessing SIFIs' proximity and speed to default or danger of default so that the FDIC is positioned to undertake necessary preparatory actions for a SIFI resolution.

To fulfill its responsibility, the FDIC's RMS-Complex Financial Institutions has undertaken numerous initiatives, including risk monitoring of larger institutions for which FDIC is not the primary federal regulator. This monitoring includes understanding SIFIs':

- structure, business activities, and resolution/recovery capabilities to inform FDIC resolution planning efforts;
- business activities and risk profiles to gauge both proximity to a resolution event and the speed at which an institution's condition could potentially deteriorate to a resolution event; and
- recovery plans, early warning signals and triggers, escalation, and the range of FDIC remedial actions to be taken should a triggering event occur.

As of June 2016, RMS-Complex Financial Institutions was monitoring 16 SIFIs in its financial institution portfolio with assets over $13 trillion.

We determined that the FDIC had made steady progress in developing criteria and a process, namely the Systemic Monitoring System, for assessing the proximity and speed to default for the 16 large and complex SIFIs in the FDIC's portfolio. The Systemic Monitoring System gathers and analyzes SIFI supervisory reports and market information using standardized metrics that are then combined with FDIC onsite institution monitoring teams' perspectives and analyses of the risks shown by those metrics. Ultimately, an FDIC committee assesses the indicated risks from institution monitoring team submissions and other sources to assign a quarterly risk rating for each SIFI on its proximity and speed to default. As the proximity to default increases, the FDIC may take a number of actions, including increased monitoring and a resolution strategy refresh.

We made three recommendations relating to improving Systemic Monitoring System documentation and independently evaluating the Systemic Monitoring System tool's output. Management agreed to take corrective action.

Employee Travel

We initiated an evaluation in response to two 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 involved. We reviewed business travel completed by seven FDIC employees identified in the complaints and developed statistics on business travel completed by all employees identified as WiP by the FDIC.

WiP allows an FDIC employee to work from a location different from the position's normal reporting location. For example, WiP could allow an employee physically located in Dallas to occupy a position normally located in Washington, DC (Washington)—Dallas would be the official duty station and Washington would be the reporting duty station for the WiP employee. The FDIC had not established a formal policy for the WiP program. As of December 2015, the FDIC identified 125 employees in WiP positions.

Importantly, reimbursements for long-term travel to the same location can trigger tax consequences for employees. Factors to consider when determining if travel is taxable include the location of an employee's official duty station and how often an employee travels between two places of business. If an employee travels for work to a single location other than his/her official duty station for the majority of his/her work time for 1 year or more, there is an increased likelihood that the travel expenses are taxable. Ultimately, whether business travel is taxable depends on the facts and circumstances of each travel situation. Travel reimbursements are also generally taxable when an employee travels for reasons of personal convenience instead of business necessity.

We concluded that some of the allegations involving the travel patterns of the seven FDIC employees had merit. Five employees were designated as WiP and traveled frequently to their reporting duty station in Washington in 2015, contrary to the intent of the WiP program. (One of the seven employees was not WiP and did not travel frequently or extensively.) Three of the five WiP employees traveled extensively to Washington under details or promotions exceeding 1 year, which could trigger tax consequences. The FDIC's Division of Finance began withholding taxes for one of those employees when it became apparent that the employee's detail and related travel would exceed 1 year. We reported that the Division of Finance should review the facts and circumstances for the other two WiP employees and determine whether withholding is warranted.

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. WiP is intended for hard-to-fill positions after merit promotion procedures have been unsuccessful and contemplates infrequent travel to the reporting duty station. The FDIC's use of WiP varied and was not always consistent with WiP guidance or a May 2016 draft policy.

The seventh employee named in the allegation was an FDIC executive that the FDIC reimbursed for extensive travel to his original city of residence, which was near an FDIC office (an Alternate Location), over a 14-year period. The Executive had relocated from the Alternate Location to Washington and had operated under an informal work arrangement since 2002 that allowed him to spend a portion of his work time in the Alternate Location, where he continued to maintain a residence. In addition to receiving relocation benefits, the Executive earned a Washington-based salary that was 17-percent higher than what he would have earned in the Alternate Location in 2016.

In our view, the work arrangement created risks and adverse consequences for the Corporation and potentially for the Executive and appeared not to be in the FDIC's best interests. Our report discusses several factors that contributed to this situation, including the Executive's former supervisor's decision to allow the work arrangement and the unique and informal nature of the arrangement. The work arrangement involved unusual provisions and was difficult to monitor, lacked parameters and controls, and created the risk of expenses that outweighed business needs. It would have been prudent for management to periodically review whether the arrangement continued to provide sufficient value to the Corporation.

We also concluded that the Executive took frequent advantage of the work arrangement for his own personal benefit and convenience. FDIC executives are held to a higher standard than other FDIC employees and are expected to practice good stewardship. A number of court cases have concluded that travel expenses paid by an employer should be treated as taxable income by the employee if those expenses are incurred for personal convenience instead of business necessity. We questioned the necessity and reasonableness of $122,423 in costs associated with the Executive's travel to the Alternative Location.

We made eight recommendations to strengthen policy and controls surrounding long-term taxable travel, the WiP program, and processes for identifying and monitoring unusual or questionable travel patterns. We also recommended that the FDIC disallow and attempt to recover $122,423 in costs associated with the Executive's travel to the Alternate Location.

FDIC management concurred with seven recommendations and partially concurred with our recommendation to disallow and attempt to recover costs. The FDIC reviewed the Executive's travel patterns and facts associated with travel to the Alternate Location, recovered $2,658 in charges it concluded were not permitted under the work arrangement, and determined the remaining travel expenses were authorized under the work arrangement.

Invoices Submitted by Lockheed Martin Services, Inc.

As referenced earlier with respect to the FBDS project, to accommodate the enormous data conversion and storage demands associated with the large number of institution failures in recent years, the FDIC entered into a contract with Lockheed Martin Services, Inc. for data management services. Under the contract, Lockheed provided the FDIC with a standard method of maintaining failed institution data, including secure data migration, conversion, cataloging, indexing, storage, security, and retrieval.

We engaged a contractor to audit invoices submitted by Lockheed to determine whether charges the FDIC paid to Lockheed were adequately supported, allowable under the terms and conditions of the contract and task orders, and allocable to their respective task orders. The audit covered selected charges billed on invoices submitted during the period May 2, 2011 through December 31, 2015.

The contractor determined that all but $124 of the $17,478,331 in charges on the 149 firm fixed price and time and materials invoices that it reviewed were adequately supported, allowable under the terms and conditions of the contract and task orders, and properly allocated to their respective task orders. In addition, the contractor determined that Lockheed had allocated the remaining $339,794,230 in firm fixed price and time and materials charges invoiced during the period covered by the audit to the correct task orders.

Further, the charges on all six credit invoices totaling $1,072,632 that the contractor reviewed were adequately supported, allowable under the terms and conditions of the contract and task orders, and properly allocated to their respective task orders. The contractor also confirmed that all of the $1,570,848 in credits due to the FDIC as of June 6, 2012 had been accounted for. Finally, the contractor's analysis of summary invoice data for ten judgmentally selected financial institutions found that the type of services Lockheed invoiced, the associated charges totaling $16,800,860, and the periods during which the services were performed were permissible under the terms of the contract and respective task orders.

The $124 in exceptions that the contractor identified consisted of $103 in duplicate charges, $12 in unallowable travel agent booking fees, and $9 in unallowable hotel expenses. At the contractor's request, Lockheed reviewed its invoices to determine whether additional travel agent booking fees may have been charged to the FDIC on invoices that the firm did not review. Lockheed's review identified an additional $4,046 in unallowable travel agent booking fees. The remaining $112 in duplicate charges and unallowable hotel expenses appeared to be non-recurring errors and, therefore, the contractor did not project these questioned costs to the universe of expenses reviewed. Accordingly, the contractor questioned a total of $4,170 in unallowable travel costs which we are noting in this semiannual report. FDIC management agreed with the recommendation we made as a result of this work.

Goal 2: Impactful Investigations

Investigate criminal activities affecting financial institutions and conduct other investigative activities to ensure integrity in the banking industry and FDIC internal operations

The OIG's Office of Investigations (OI) works closely with FDIC management in RMS, DRR, and the Legal Division to identify and investigate financial institution crime, especially various types of bank fraud. OIG investigative efforts are concentrated on those cases of most significance or potential impact to the FDIC and its programs. The goal, in part, is to bring a halt to the fraudulent conduct under investigation, protect the FDIC and other victims from further harm, and assist the FDIC in recovery of its losses. Pursuing appropriate criminal penalties not only serves to punish the offender but can also deter others from participating in similar crimes. In the case of bank closings where fraud is suspected, our OI may send case agents and computer forensic special agents from the Electronic Crimes Unit to the institution. Electronic Crimes Unit agents use special investigative tools to provide computer forensic support to OIG investigations by obtaining, preserving, and later examining evidence from computers at the bank.

Importantly, our criminal investigations can also be of benefit to the FDIC in pursuing enforcement actions to prohibit offenders from continued participation in the banking system. When investigating instances of financial institution fraud, the OIG also defends the vitality of the FDIC's examination program by investigating associated allegations or instances of criminal obstruction of bank examinations and by working with U.S. Attorneys' Offices to bring these cases to justice. The OIG also continues to coordinate with the FDIC's RMS Bank Secrecy Act/Anti-Money Laundering Section to address areas of concern, and we communicate regularly with the Department of Justice's (DOJ) Money Laundering and Asset Recovery Section.

The OIG's investigations of financial institution fraud historically constitute about 90 percent of the OIG's investigation caseload. The OIG is also committed to continuing its involvement in interagency forums addressing fraud. Such groups include national and regional bank fraud, check fraud, mortgage fraud, anti-phishing, and suspicious activity review working groups, as illustrated later in this section. More recently, and as discussed in detail under goal 4 of this report, the OIG, and OI in particular, has expanded its involvement in several cyber security-related working groups, namely the National Cyber Investigative Joint Task Force and the FBI Washington Field Office Cyber Task Force.

Of note during the reporting period, OI staff completed training at the Federal Law Enforcement Training Center in Glynco, Georgia, and held an OI-wide meeting to ensure quality of OI investigative activities and adherence to DOJ investigative requirements. Also during the Fall 2016, an OI special agent and senior investigative advisor participated in a training program in Kiev for the Ukrainian Deposit Guarantee Fund and other Ukrainian agencies, sponsored by the Department of the Treasury's Office of Technical Assistance. The goal of the training was to explain how U.S. authorities investigate bank failure cases and other complex banking investigations, with an emphasis on interagency cooperation on such cases.

OIG Work in Support of Goal 2

The cases discussed below are illustrative of some of the OIG's most important investigative success during the reporting period. These cases reflect the cooperative efforts of OIG investigators, FDIC divisions and offices, U.S. Attorneys' Offices, and others in the law enforcement community throughout the country.

Our cases during the reporting period include those involving bank fraud, wire fraud, obstruction of an examination, embezzlement, and mortgage fraud. Many of our bank fraud cases involve former senior-level officials, other bank employees, and customers at financial institutions who exploited internal control weaknesses and whose fraudulent activities harmed the viability of the institutions and ultimately contributed to losses to the DIF. Real estate developers and agents, and other individuals involved in residential and commercial lending activities were also implicated in a number of our cases. The cases discussed below were conducted by the OIG's special agents in our headquarters and regional offices and reflect nationwide activity and results. The OIG's working partnerships with the Corporation and law enforcement colleagues in all such investigations contribute to ensuring the continued safety and soundness of the nation's banks and help ensure integrity in the FDIC's programs and activities.

Bank Customer Pleads Guilty in Bank Fraud Scheme

On February 7, 2017, the owner and president of Machine Tools Direct, Inc. (MTD), was sentenced to serve 36 months in prison and was ordered to pay restitution of $97,331,250 for his role in a wire fraud scheme. He and a business partner were indicted on February 27, 2014, and charged with mail fraud, bank fraud, and wire fraud.

Between early 2006 and October 2009, the former president of MTD and the former president and co-owner of Equipment Acquisition Resources, Inc. (EAR), engaged in a scheme to fraudulently obtain approximately $190 million from banks and financing companies, eventually causing those lenders to lose at least $100 million. The former MTD president used false representations about his company's business operations, financial status, independence from EAR, and need for financing when applying for loans. The two businessmen falsely represented to lenders that EAR and MTD were separate companies engaged in arms-length sales transactions. In reality, the former MTD president obtained financing for MTD to purchase equipment from EAR, and he and the former EAR president arranged sham sales transactions between the two companies. After MTD received financing from the lenders, the MTD president sent most of the proceeds to the EAR president so that EAR could use the money to make payments on other loans. The former EAR president pleaded guilty on January 7, 2015, and on July 22, 2015, was sentenced to serve 60 months in prison. He too was ordered to pay restitution of more than $97 million, joint and several with the former MTD president.

Source: *Request for assistance from the FBI.*
Responsible Agencies: *The FDIC OIG is conducting the investigation jointly with the FBI. Prosecuted by the U.S Attorney's Office for the Northern District of Illinois.*

Former Loan Officer Sentenced

On October 24, 2016, a former loan officer at Broadway Federal Bank (BFB), FSB, Los Angeles, California, was sentenced to serve 18 months in prison for demanding and accepting kickbacks from borrowers. He was also ordered to pay restitution of $353,925 to the bank.

Between February 2007 and March 2010, the former loan officer processed loan applications submitted on behalf of numerous churches in Los Angeles and the surrounding areas. He worked with brokers and provided them a template for presenting financial information for the churches that ensured the loan applications would be approved. Based on the false information concerning the financial status of the churches, BFB issued loans to the churches.

BFB would pay rebates to loan brokers who brought the loans to the bank. The former loan officer admitted that he corruptly demanded and accepted payments from loan brokers in exchange for procuring loans at BFB. In total, he accepted $353,925 in wrongful payments.

One of the brokers who paid kickbacks was sentenced in February 2016 to one year and one day in federal prison and was ordered to pay $4.2 million in restitution to the bank. He acted as a "consultant" who targeted Los Angeles-area churches with promises of new mortgages to purchase property or refinanced mortgages from the bank. Between 2007 and 2009, he met with representatives of churches and obtained financial information required for the loan applications. Others involved in the scheme then altered the financial information to make it appear the churches were more financially sound than they actually were, and the broker caused these false loan applications to be submitted to the bank.

> ***Source:*** *Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP).*
> ***Responsible Agencies:*** *TThis is a joint investigation by the FDIC OIG, Internal Revenue Service-Criminal Investigations (IRS-CI), FBI, and SIGTARP. Prosecuted by the U.S. Attorney's Office for the Central District of California.*

Former Bank Officer Convicted of Embezzlement and Attempting to Evade Income Tax

On February 6, 2017, a former bank officer was convicted and sentenced for embezzlement and attempting to evade income taxes. She was ordered to serve 30 months in prison to be followed by 5 years of supervised release and to pay restitution to the bank in the amount of $539,485. She further consented to the issuance of an order of prohibition by the FDIC.

The former bank officer was the Central Services Supervisor of Heritage Bank of Nevada (HBN), Reno, Nevada, a position which allowed her access to the bank's electronic processing systems. In November 2014, a change in the bank's chief financial officer triggered a review of HBN's accounts and books. As part of that process, the former bank officer was asked to explain some data associated with HBN's Central Services. She did not respond in a timely manner and her manager was asked to review the matter and provide the new chief financial officer with an explanation.

A review determined that the former supervisor had been using her computer access to HBN's electronic processing systems to alter the processing of debits and credits from her HBN-issued debit card. She was able to alter incoming debits that should have been paid out of her personal account at HBN and caused the debits to be posted to HBN's accounts. She also redirected credits, which should have gone to HBN, to her personal accounts at the bank instead. In addition, the former bank officer caused four restitution checks to HBN from the U.S. District Court to be deposited into her personal accounts. Between 2005 and 2014, she was able to embezzle nearly $539,500.

The former bank officer did not report or pay federal income tax on any of the funds she embezzled. For tax years 2009 through 2014, she failed to completely report income and pay more than $115,000 in federal income taxes.

Source: *FDIC RMS.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, FBI, and IRS-CI. Prosecuted by the U.S. Attorney's Office for the District of Nevada.*

Former Bank Chairman Sentenced

On February 9, 2017, the former president and chairman of First State Bank (FSB) of Altus, Altus, Oklahoma, was sentenced to 48 months in prison after a jury convicted him in July 2016 of bank fraud, conspiracy to commit bank fraud, misapplication of bank funds, making a false bank entry, unauthorized issuance of a bank loan in connection with FSB, and various loan schemes. He was also ordered to pay $10,120,166 in restitution to the FDIC.

On December 2, 2016, a co-conspirator was sentenced to 18 months in federal prison to be followed by 36 months of supervised release after pleading guilty to conspiring with the former bank president to commit bank fraud. He was also ordered to pay $3,250,409 in restitution. He had previously partnered with the former bank president in several businesses headquartered in Altus. In July 2009, state banking regulators closed FSB due to the bank's loan losses, and the FDIC was appointed as the bank's receiver.

Earlier, a federal grand jury had charged the two with fraud related to three loan schemes: (1) a series of FSB loans to finance a real estate development in Routt County, Colorado; (2) a series of "senior life settlement loans" from FSB to support an Altus aerospace company; and (3) a $2 million unauthorized loan from FSB to a company under the former bank president's and the co-conspirator's control. They engaged in these various loan schemes to finance their personal business activities and obtain loan proceeds of over $14 million without proper authorization or approval.

As part of a plea agreement, the government agreed to dismiss at sentencing the charges against the co-conspirator from the indictment. He testified as a witness for the government at the former bank president's trial.

Source: *FDIC RMS.*
Responsible Agencies: *This was a joint investigation with the FBI. Prosecuted by the U.S. Attorney's Office for the Western District of Oklahoma.*

Iowa Businessman Sentenced in Bank Fraud Case

On November 28, 2016, an Iowa businessman was sentenced to serve 3 years in prison to be followed by 4 years of supervised release and ordered to pay restitution of $1,060,022 to Lincoln Savings Bank (LSB), Cedar Falls, Iowa. He previously pleaded guilty to one count of bank fraud after fighting extradition from Brazil on a warrant issued after a November 2012 indictment charging him with four counts of bank fraud and one count of making false statements to a bank.

The businessman and his wife operated a small agricultural business that spread lime and chemicals on farm fields. The company also performed seasonal work, snow removal, and trucking, and refurbished and sold used agricultural equipment. The businessman financed his operations with loans and lines of credit at LSB secured by business assets, equipment, and accounts receivable. The businessman was responsible for the day-to-day operations, and his wife was the bookkeeper. When the fraud was discovered in the spring of 2005, LSB had an aggregate unpaid principal balance of $1,017,533, but the collateral equipment was missing from the yard at the agricultural business, and the businessman's family had relocated to Brazil.

The businessman's scheme to defraud LSB included submitting a false document to the bank which inflated the value of the business's accounts receivable by more than 50 percent and selling equipment and machinery in which LSB had a security interest. In 2003, the businessman asked his parents to serve as officers of a newly formed company, through which used equipment would be bought and sold. Through a series of purchase agreements, bills of sale, and promissory notes, the businessman transferred his company's equipment and machinery to his parents' newly formed company, after which it was shipped to and sold at auction houses in Iowa, Nebraska, Minnesota, and South Dakota. Proceeds from the sales were not used to pay down the debt at LSB but rather were transferred to the businessman for his personal use, including his operations in Brazil.

Source: *FBI.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG and FBI. Prosecuted by the U.S. Attorney's Office for the Northern District of Iowa.*

Indian Ridge Developers Sentenced in Bank Fraud Case

On January 24, 2017, two developers of the Indian Ridge Resort located in Branson, Missouri, were sentenced in the District of Kansas. They were each sentenced to serve 60 months in prison to be followed by 24 months of supervised release. The wife of one of developers was sentenced to 36 months of supervised release. On May 27, 2015, the three each entered guilty pleas for their role in a real estate construction fraud scheme charging them with bank fraud, conspiracy to commit bank fraud, money laundering, and conspiracy to commit money laundering.

Columbian Bank and Trust (CBT) originally loaned a principal of Indian Ridge Resorts LLC, approximately $11.9 million in September 2005 to develop 828 acres of land in Branson, Missouri, for a hotel, golf course, and water park. In February 2007, the remaining 202 acres of land, known as "tract 34," was parceled out and sold to the two developers of Tri-Global Development as the site for the Indian Ridge Town Home Project. The town home lots in tract 34 were sold to various credit-partner investors, and CBT held 28 of the 50 associated notes and underlying collateral. Wells Fargo Bank and Lawrence Bank, Lawrence, Kansas, held the remaining 22 associated notes.

Following the failure of CBT, a review of the 28 notes held by the bank reflected that all 28 notes were between 75 percent and 100 percent drawn, with no supporting performance. By using shell companies and submitting fraudulent loan draw requests to the associated financial institutions, the two developers and one developer's wife falsely obtained the various borrowers' loan proceeds. In her plea, the developer's wife admitted she knew invoices submitted to the bank included overhead and profit in the line item costs, in violation of the terms of the loan agreement.

The developers used these fraudulently obtained loan proceeds for their own expenses as well as for funding other unrelated construction projects in Colorado that were already in default at New Frontier Bank. The FDIC calculated its loss as $8,258,565 on the 28 notes formerly held by CBT.

Source: *FDIC DRR.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG and the IRS-CI. Prosecuted by the U.S. Attorney's Office for the District of Kansas.*

Former President and Bank Director Pleads Guilty

On December 12, 2016, the former president and director of Peoples Savings Bank, Crawfordsville, Iowa, was sentenced to serve 41 months in prison to be followed by 3 years of supervised release and fined $15,000. On April 8, 2016, the former president pleaded guilty to a criminal Information charging him with misapplication of bank funds and obstruction of a bank examination.

According to the Information, from January 2008 until October 2013, the former president misused his position to misappropriate approximately $626,941 from bank customer loans he had originated. He was able to accomplish this by manipulating various banking records and originating loans in the names of unsuspecting bank customers. The money gained from the embezzlement was used to augment his personal lifestyle.

Source: *FDIC RMS.*
Responsible Agencies: *The FDIC OIG is conducting the investigation with assistance from the FBI. Prosecuted by the U.S. Attorney's Office for the Southern District of Iowa.*

Former Trust Officer Sentenced for Bank Fraud

On March 6, 2017 a former trust officer of First State Bank, Mendota, Illinois, was charged with one count of misappropriation of financial institution property. The charging document described how the former trust officer, on more than two occasions and without authorization, took control of money and securities under the custody and control of First State Bank. On March 9, 2017, the former trust officer pleaded guilty to the charges and was sentenced to 4 years in prison followed by 2 years of supervised release.

From January 2009 through July 2016, to carry out her scheme, the former trust officer stole funds from trust accounts and used those funds to cover her personal expenses. The investigation revealed that she misappropriated at least $650,000 from trust accounts, converted the stolen proceeds to bank money orders, and either deposited those money orders into her own accounts or sent them to credit card companies to pay her bills.

Under the plea agreement, the former trust officer will pay restitution of $50,000 to First State Bank, surrender an account maintained at First State Bank in her name containing approximately $130,000, and enter into a stipulation and consent to the issuance of an order of prohibition with the FDIC, and agree to a lifetime ban from banking.

Source: *First State Bank.*
Responsible Agencies*: The case was investigated by the FDIC OIG. Prosecuted by the Illinois Attorney General's Office.*

Former Bank President Sentenced in Bank Fraud Case

On October 13, 2016, the former president of Community State Bank, Brook, Indiana, was sentenced to serve 78 months in prison to be followed by 2 years of supervised release and was ordered to pay restitution of $3,410,233.

From August 2010 through September 2015, the former president executed a scheme to defraud Community State Bank by causing the bank to issue over $6 million in fraudulent loans. He prepared universal notes and forged the signatures of four bank customers, three of whom were family members, in order to secure the fraudulent loans. After the loans were funded, he used the proceeds to support his lifestyle by purchasing show cattle and vehicles, making property improvements, and repaying earlier fraudulent loans. As president of Community State Bank, he was responsible for preparing the minutes of the Board of Directors meetings and making those minutes available for FDIC examinations. He was aware that any loans to family members would involve increased scrutiny from the bank's Board of Directors and FDIC examiners. To conceal his scheme, and perpetuate his ability to obtain additional fraudulent loans, he prepared one set of minutes for review by the Board of Directors and a second set of minutes for review by the FDIC. The minutes shown to FDIC examiners made it look as though the bank's Board was aware of the loans. The actual Board minutes made no mention of the loans.

Source: *Request for assistance from the FBI.*
Responsible Agencies: *The case was investigated by the FDIC OIG and the FBI. Prosecuted by the U.S. Attorney's Office for the Northern District of Indiana.*

Pennsylvania Man Sentenced to 8 Years in Prison for Fraud Scheme

On February 15, 2017, a Chester, Pennsylvania, man was sentenced to 97 months in prison and 5 years of supervised release, for his multi-year scheme to steal government homes and file false tax forms against various police officers and government officials. Two of his co-conspirators were sentenced in October 2016 to 40 months in prison, and 1 day in prison, respectively, for their crimes. All three were charged in December 2016 with one count of conspiracy to commit offenses against the United States, one count of bank fraud, and one count of corrupt interference with Internal Revenue laws. The Chester man was also charged with three counts of conversion of government property, and one of the co-conspirators was similarly charged with one count of conversion of government property. The Chester man and that same co-conspirator were also charged with one count of creating fictitious obligations.

To further their scheme, the men filed more than 100 false land deeds with the Delaware County Recorder of Deeds Office in an attempt to claim ownership of homes owned by the government or by banks, and then to l ive in the homes, or rent or sell the homes to unsuspecting persons, for their own financial gain. They were self-proclaimed "sovereign citizens," who also filed hundreds of false tax forms against police officers, judges, and other government employees in an attempt to harass and intimidate them in the course of their official duties. In addition to the prison term, the Chester man was also ordered to pay restitution of $190,818.

Source: *U.S. Attorney's Office, Eastern District of Pennsylvania.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, FBI, U.S. Department of Housing and Urban Development OIG, the Treasury Inspector General for Tax Administration, the Federal Housing Finance Agency OIG, the Social Security Administration OIG, and several police departments. Prosecuted by the U.S. Attorney's Office for the Eastern District of Pennsylvania.*

Former Bank Officers and Walton County Man Convicted in Bank Fraud Scheme

On Friday, March 10, 2017, after a 5-day trial, the former president of GulfSouth Private Bank (GulfSouth), Destin, Florida, was convicted of conspiracy to commit bank fraud, four counts of false statements to a federally insured financial institution, bank fraud, and mail fraud affecting a financial institution.

Also on March 10, a co-conspirator from Walton County pleaded guilty to conspiracy to commit bank fraud and one count of making a false statement to a federally insured financial institution. Earlier, on February 27, 2017, a second co-conspirator—the former senior vice president of GulfSouth, pleaded guilty to conspiracy, four counts of false statements to a financial institution, and bank fraud.

In 2007, an individual approached the former president of GulfSouth, and notified him that the individual's company, which had been loaned $3.4 million, was no longer going to be able to make payments on the mortgage loans issued by GulfSouth that had been secured by three condominiums. In an effort to conceal that the loans were going into default, and instead of recognizing that the $3.4 million in loans were losses to the bank, the former bank president devised a scheme to conceal the bad debt.

As a part of the scheme, the former bank president and the former senior vice president solicited four individuals to take out new loans with the bank to purchase the three condominiums. To persuade them to engage in the scheme, the former bank officers told these individuals that the loans would be non-recourse, meaning that, if the men defaulted, GulfSouth would have no recourse against them.

Subsequently, the former bank officers caused new mortgage loans and additional lines of credit to be issued for approximately $3.8 million to the men they had solicited. According to the terms of the fraudulent loans issued during the scheme, the men they solicited were not required to make any payments on the loans until the loans came due months down the road. These new loans were then used to pay off the old loans that were going into default. Issuing these new loans and new lines of credit created the appearance that the debt was "performing," which allowed the former president to avoid having to report the loans associated with the condominiums as bad debt, as required. Further, as a part of the scheme, the two former bank officers caused fraudulent security agreements to be prepared that falsely represented that the four men were obligated to repay their respective new mortgage loans and lines of credit.

In September 2009, GulfSouth received $7.5 million in Troubled Asset Relief Program funds from the U.S. Treasury. Thereafter, the two former officers allowed the condominiums that were collateral for the mortgage loans to be sold in short sales, resulting in a loss to GulfSouth. Further, the former bank president allowed the deficiencies and the lines of credit to be charged off of GulfSouth's books and records.

The sentencing hearings for these individuals were scheduled for May 2017.

Source: *This case was initiated based on information received from SIGTARP.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG and SIGTARP. Prosecuted by the U.S. Attorney's Office for the Northern District of Florida.*

Former First Tennessee Bank Employee Sentenced to Serve 3 Years in Prison for Embezzlement of Funds and Tax Evasion

On March 6, 2017, a former bank branch manager at First Tennessee Bank, N.A., Memphis, Tennessee, was sentenced to serve 36 months in federal prison for embezzlement of funds and tax evasion, to be followed by 5 years of supervised release. He was also ordered to pay restitution in the amounts of $844,254 to First Tennessee Bank, $161,018 to the Internal Revenue Service and $81,014 to two additional victims of his crimes, for a total of $1,086,286.

The former bank manager was an employee of First Tennessee from May 2000 until February 2016. In October 2016, he pleaded guilty to an Information charging him with one count of theft by a bank officer or employee and four counts of attempting to evade or defeat tax. His scheme involved a variety of techniques, including: earning and then abusing the trust of various clients by telling them falsely that he would engage in financial transactions for their benefit, using his position as a manager of the bank to identify clients who he knew did not review their monthly statements, and identifying inactive accounts from which to embezzle money because he knew the owners of such accounts would be unlikely to detect the embezzlement. Upon learning of the embezzlement by the former bank manager, First Tennessee reimbursed most of the losses to its accountholders.

Of the total amount he embezzled, the former bank manager obtained approximately $967,573 for his personal use. He lost or spent most of this through on-line gambling on various Websites and making payments on various personal consumer debts. He did not claim any of these funds as income on his tax returns for years 2012-2015, thus evading paying taxes of approximately $161,000.

Source: *OIG OI-initiated.*
Responsible Agencies: *This is a joint investigation conducted by FDIC OIG, FBI, and IRS-CI. Prosecuted by the U.S. Attorney's Office for the Eastern District of Tennessee.*

Former Lake Cumberland Marina Owner Sentenced to 50 Months in Prison for Bank Fraud

A Kentucky real estate developer, who operated a marina on Lake Cumberland, was sentenced to 50 months in federal prison for nine counts of bank fraud. In addition to his federal prison sentence, he was sentenced to 5 years of supervised release. Restitution will be ordered at a later date.

The former marina owner was convicted last year, after a one-week trial in Lexington, by a jury who found him guilty of defrauding American Founders Bank of over $4 million. According to evidence presented at trial, he bought a marina in south-central Kentucky, using money from nine fraudulent bank loans. He submitted false paperwork in his bank loan applications and claimed that the money would be used to buy boats and homes that did not actually exist. As part of his fraud, he falsified appraisal documents and insurance policies for the nonexistent collateral, and forged signatures of investors and acquaintances, as well as that of his deceased brother. When the scheme collapsed, American Founders Bank suffered a loss of approximately $3,251,897.

Source: *FBI.*
Responsible Agencies: *This case was investigated by the FDIC OIG and the FBI. Prosecuted by the U.S. Attorney's Office for the Eastern District of Kentucky.*

Former Vice President and Bank Secrecy Act Officer Admits to 6-Year Scheme to Steal Over $1.8 Million from Bank Customers

A former vice president and Bank Secrecy Act officer of a Maryland bank 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 Bank Secrecy Act officer, she was responsible for filing Currency Transaction Reports and Suspicious Activity Reports 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 associated with her and her family members. 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.

Sentencing in the case is scheduled for May 2017.

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

Former FDIC Employee Sentenced for Computer Crime

On January 27, 2017, a former senior capital markets specialist employed by the FDIC was sentenced to serve 2 years of probation in connection with his prior plea of guilty to a misdemeanor charge of intentionally exceeding authorized access to an FDIC computer to obtain information.

The former employee was assigned to the FDIC's Schaumburg, Illinois, Temporary Satellite Office. During the course of his employment with the FDIC, he was detailed to the Office of Complex Financial Institutions in Washington, DC. Between January 2011 and September 2012, he emailed over 900 FDIC documents to his personal email account, including sensitive, confidential, and strictly private information regarding and belonging to SIFIs.

Source: *FDIC DRR.*
Responsible Agencies: *This investigation was conducted by the FDIC OIG. Prosecuted by the U.S. Attorney's Office for the Northern District of Illinois.*

Electronic Crimes Unit Responds to Email and Other Schemes

The Electronic Crimes Unit (ECU) continues its work to identify and mitigate the effects of phishing attacks through emails claiming to be from the FDIC. These schemes persist and seek to elicit PII or financial information from their victims. The nature and origin of such schemes vary, and, in many cases, it is difficult to pursue the perpetrators, as they are quick to cover their cyber tracks, often continuing to originate their schemes from other Internet addresses and from locations outside of the U.S.

The ECU has seen an increase in advanced fee schemes, particularly by telephone calls and text messages. Perpetrators vary the schemes used in their attempt to elicit PII in the form of credit card or bank account information, or direct payment from victims. Several attempts were made by perpetrators who represented themselves as representatives of the FDIC, including FDIC law enforcement officials. Those committing these schemes often obtain some public information on the persons they are impersonating in order to lend authenticity to their scheme, and use threatening tactics to persuade victims into providing funds. ECU's investigative efforts have traced several transactions that led to some potential mules, people who serve as intermediaries for criminals by transferring illegally acquired money. As is typical of these schemes, the identities of the mules have proven to be false or stolen. ECU continues to investigate these schemes and coordinate with law enforcement partners to identify the parties involved.

Another type of scheme of interest to the ECU is known as business email compromise. This scam targets businesses that perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

According to the FBI, the business email compromise scam continues to grow and evolve and it targets businesses of all sizes. There has been a 270 percent increase in identified victims and exposed loss since January 2015. The scam has been reported in all 50 states and in 79 countries. Fraudulent transfers have been reported going to 72 countries; however, the majority of the transfers are going to Asian banks located within China and Hong Kong.

There has been an increase in the number of reported computer intrusions linked to business email compromise scams. These intrusions can initially be facilitated through a phishing scam in which a victim receives an email from a seemingly legitimate source that contains a malicious link. The victim clicks on the link, and it downloads malware, allowing the actor(s) unfettered access to the victim's data, including passwords or financial account information.

Another version of this scam involves victims being contacted by fraudsters, who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or email. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of business email compromise scam may occur at the end of the business day or work week or be timed to coincide with the close of business of international financial institutions.

The ECU has investigated several of these schemes targeting either high-level FDIC officials or citizens. There has been no financial loss to the FDIC on these scams. However, some unwitting citizen victims did fall for the scam and one victim in particular has suffered over $90,000 in financial losses to date. ECU continues to investigate these schemes in an effort to identify perpetrators and their networks to prevent further losses.

Strong Partnerships with Law Enforcement Colleagues

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

During the reporting period, we partnered with U.S. Attorneys' Offices in the following areas: Alabama, Arkansas, California, Colorado, District of Columbia, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, 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 HIDTA; Philadelphia Financial Exploitation Prevention Task Force; Maryland Mortgage Fraud Task Force; Philadelphia Mortgage Fraud Working Group; Pittsburgh SAR Review Team.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force; Southern District of Florida Mortgage Fraud Working Group; 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.
Kansas City Region	St. Louis Mortgage Fraud Task Force; Kansas City Financial Crimes Task Force; Minnesota Inspector General Council meetings; Minnesota Financial Crimes Task Force; Kansas City SAR Review Team; Springfield Area Financial Crimes Task Force; Nebraska SAR Review Team; Iowa Mortgage Fraud Working Group.
Chicago Region	Dayton, Ohio, Area Financial Crimes Task Force; Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Detroit SAR Review Team; Financial Investigative Team, Milwaukee, Wisconsin; Milwaukee Mortgage Fraud Task Force; Madison, Wisconsin, SAR Review Team; Indiana Bank Fraud Working Group; FBI Louisville Financial Crime Task Force; U.S. Secret Service Louisville Electronic Crimes Task Force; Western 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; Los Angeles Mortgage Fraud Working Group for the Central District of California; Orange County Financial Crimes Task Force-Central District of California.
Dallas Region	SAR Review Team for the Northern District of Mississippi; SAR Review Team for the Southern District of Mississippi; Oklahoma City Financial Crimes SAR Review Working Group; Austin SAR Review 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.

Goal 3: Effective Communications

Communicate Effectively with Internal and External Stakeholders

Strong working relationships are fundamental to our success. In that regard, effective communications with OIG stakeholders both internal and external to the Corporation are vital. During the reporting period, in addition to focusing on our own staff as a primary stakeholder in our office, we examined the information needs of the OIG's many other stakeholders, including the FDIC Board of Directors and FDIC division and office management and their staffs, the Congress, members of the IG community, GAO, OMB, the media, and the general public.

Importantly, we keep OIG staff informed of office priorities and key activities. We do so through regular meetings among staff and management, bi-weekly updates from senior management meetings, and issuance of OIG newsletters. During the reporting period, the IG also conducted an employee survey, and held informal meetings and two OIG-wide town hall meetings to elicit the views of OIG staff and share his perspectives with them. We also place a high priority on maintaining positive working relationships with the FDIC Chairman, Vice Chairman, other FDIC Board members, and management officials. In that regard, during his first weeks at the FDIC, the IG met with FDIC Board members and senior FDIC management officials to introduce himself and share his perspectives on the role of the IG at the FDIC. The OIG is a regular participant at FDIC Board meetings and at Audit Committee meetings where recently issued audit and evaluation reports are discussed. Other meetings occur throughout the year as OIG officials confer with division and office leaders and attend and participate in internal FDIC conferences and other forums.

Equally, the OIG places a high priority on maintaining positive relationships with the Congress and providing timely, complete, and high-quality responses to congressional inquiries. In most instances, this communication would include semiannual reports to the Congress; issued audit and evaluation reports; responses to other legislative mandates; information related to completed investigations; comments on legislation and regulations; written statements for congressional hearings; contacts with congressional staff; responses to congressional correspondence and Member or Committee requests; and materials related to OIG appropriations.

The OIG fully supports and participates in IG community activities through CIGIE. We coordinate closely with representatives from the other financial regulatory OIGs. In this regard, the Dodd-Frank Act created the Financial Stability Oversight Council and further established CIGFO. 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. CIGFO may also convene working groups to evaluate the effectiveness of internal operations of the Financial Stability Oversight Council.

Additionally, the OIG meets with representatives of the GAO to coordinate work, provide OIG perspectives on risk and minimize duplication of effort. Similarly we coordinate with the OMB on budgeting and other matters requiring OIG attention. As noted earlier in this report, we also work closely with representatives of the DOJ, including the FBI and U.S. Attorneys' Offices, to coordinate our criminal investigative work and pursue matters of mutual interest.

With respect to public stakeholders interested in our office and/or who contact the OIG for information or assistance, the OIG's inquiry intake system supplements the OIG Hotline function. The Hotline continues to address allegations of fraud, waste, abuse, and possible criminal misconduct. However, over the past several years, our office has continued to receive a large number of public inquiries ranging from media inquiries to requests for additional information on failed institutions to pleas for assistance with mortgage foreclosures to questions regarding credit card companies and banking practices. These inquiries come by way of phone calls, emails, faxes, and other correspondence. The OIG captures and tracks all inquiries in a system known as QUEST and makes every effort to acknowledge each inquiry and be responsive to the concerns raised. We coordinate closely with others in the Corporation who field inquiries and concerns from the public and appreciate their assistance in responding to those who contact our office. We handle those matters within the OIG's jurisdiction and refer inquiries, as appropriate, to other FDIC offices and units or to external organizations.

Importantly, during the reporting period, in recognition of the important role that whistleblowers play in reporting waste, fraud, and abuse and in saving taxpayer dollars and serving the public interest, the OIG took steps to strengthen our whistleblower protection understanding and capabilities to ensure that whistleblowers understand the appropriate channels for reporting their concerns.

Whistleblowers can approach the OIG in a number of ways. Perhaps the most common vehicle for whistleblowers to contact us is through our Hotline. Alternatively, whistleblowers can contact OIG staff directly to inform them of concerns. The OIG's Whistleblower Protection Ombudsman's role is to educate FDIC employees about prohibitions on retaliation for protected disclosures, and educate FDIC employees who have made or are contemplating making a protected disclosure about the rights and remedies against retaliation for protected disclosures.

Our office considers whistleblower protection to be a key priority. On March 31, 2017, we completed the Office of Special Counsel's 2302(c) Certification Program, which allows federal agencies to meet the statutory obligation to inform employees about the rights and remedies available to them for making protected disclosures. The FDIC OIG completed the 2302(c) certification requirements through a series of actions, including: placing informational posters at OIG facilities; providing information about prohibited personnel practices and retaliation to new OIG employees as part of the orientation process; providing current employees information about prohibited personnel practices and retaliation; training supervisors on prohibited personnel practices and retaliation; and establishing a link from OIG's Website to the Office of Special Counsel's Website.

The OIG's completion of the Office of Special Counsel's 2302(c) certification program demonstrates its commitment to instructing OIG employees about the rights of whistleblowers and the remedies available to whistleblowers under federal law. Additionally, the OIG is committed to working with the FDIC to reinforce through education the protections available for whistleblowers.

OIG Work in Support of Goal 3

During the reporting period, we maintained open communication channels with stakeholders, as follows:

FDIC Board, Management, and Staff:

- Communicated with the Chairman, Vice Chairman, other FDIC Board Members, the Chief Financial Officer, and other senior FDIC officials through the Acting IG's and 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.

- Kept RMS, DRR, the Legal Division, and other FDIC program offices informed of the status and results of our investigative work impacting their respective offices. This was accomplished by notifying FDIC program offices in headquarters and the regional offices of recent actions in OIG cases and providing OI's quarterly reports to RMS, DRR, and the Legal Division outlining activity and results in our cases involving closed and open banks. Coordinated closely with the Legal Division on matters pertaining to enforcement actions and professional liability cases.

- 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, IT/Cyber Security Oversight Group 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.

- Reviewed five draft FDIC directives on such matters as workplace violence prevention, measuring user activity on FDIC external Websites, and assigning and safeguarding IT assets. We provided substantive comments on proposed policy related to reporting information security incidents.

- Provided the OIG's view of the management and performance challenge areas that we identified at the FDIC, in accordance with the Reports Consolidation Act of 2000 for inclusion in the Corporation's annual report: Maintaining Strong Information Security and Governance Practices, Carrying Out Dodd-Frank Act Responsibilities, Maintaining Effective Supervision and Preserving Community Banking, Carrying Out Current and Future Resolution and Receivership Responsibilities, Ensuring the Continued Strength of the DIF, Promoting Consumer Protections and Economic Inclusion, Implementing Workforce Changes and Budget Reductions, and Ensuring Effective Enterprise Risk Management Practices.

The Congress:

- 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 IG met with congressional staff, as well as the Chairman of the Committee on Science, Space, and Technology of the House of Representatives. The IG updated Committee Chairman Lamar Smith on our office's IT-related work. The IG also met with staff from the House Committees on Financial Services and Oversight and Government Reform, and the Senate Committees on Banking and Homeland Security and Governmental Affairs.

The IG Community:

- Supported the IG community by attending monthly CIGIE meetings; participating on the CIGIE Audit Committee and the Professional Development Committee (and leading its Human Resources Roundtable); attending Legislative Committee, Assistant Inspectors General for Investigations, Council of Counsels to the IGs, Federal Audit Executive Council and other meetings; 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, such as significant open OIG recommendations and related monetary benefits, key agency datasets, OIG Website and Hotline practices, CIGIE Training Institute planning, OIG work resulting in legislative changes; and various legislative matters raised by CIGIE's Legislation Committee.

- Communicated with representatives of the OIGs of the federal banking regulators and others to discuss audit, evaluation, and investigative matters of mutual interest and leverage knowledge and resources.

- Participated on CIGFO, as established by the Dodd-Frank Act, and coordinated with the IGs on that council. Joined others on a CIGFO audit team in issuing a final report regarding the Financial Stability Oversight Council's efforts to promote market discipline.

The Government Accountability Office:

- Provided 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.

- Attended the annual CIGIE-GAO Coordination Meeting, discussing such issues as Data Act implementation, the IG Empowerment Act's implications for computer matching and survey administration, fraud risks, and handling of open recommendations.

- 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.

The Public:

- Continued using our QUEST inquiry intake system to capture and manage inquiries from the public, media, Congress, and the Corporation, in the interest of prompt and effective handling of such inquiries. Coordinated with other FDIC divisions and offices to share information on inquiries and complaints received, identify common trends, and determine how best to respond to public concerns. Responded to 203 such inquiries during the past 6-month period.
- Participated in numerous outreach efforts and professional forums including teaching a section of the DOJ's Money Laundering and Asset Recovery Section's Financial Investigations Seminar, which takes participants through a money laundering and asset forfeiture case study; presenting an investigative case and additional information on FDIC OIG coordination with the Corporation on investigations at a Federal Reserve Board OIG investigators' all-hands meeting; attending the Association of IGs meeting in Boston, Massachusetts; sharing perspectives on succession planning at the International Public Management Association for Human Resources conference; and speaking to graduate students at Northern Illinois University about law enforcement and the OIG's work investigating various white-collar crimes.
- Participated in a training program in Kiev for the Ukrainian Deposit Guarantee Fund and other Ukrainian agencies, sponsored by the Department of the Treasury's Office of Technical Assistance. The goal of the training was to explain how U.S. authorities investigate bank failure cases and other complex banking investigations, with an emphasis on interagency cooperation on such cases.

Ongoing work at the end of the reporting period in support of this goal included revision of OIG Congressional protocols to update procedures for Congressional activities, participation in the IG community's Public Affairs interest group, research on the use of social media as a tool for communicating OIG work, development of new and more relevant content for the OIG's external Website, and formulation of a more formal media relations function.

Goal 4: Enhanced Understanding of Emerging Issues

Continuously seek to enhance OIG knowledge and understanding of emerging and evolving issues affecting the FDIC, OIG, and insured depository institutions

The FDIC OIG keeps current on emerging issues and threats to the FDIC, our own office, and insured depository institutions. A priority area of focus for the OIG is the evolving issue of cyber security. To enhance the OIG's knowledge and understanding of current and emerging cyber threats to our office, the FDIC, the financial services industry at-large, and other federal entities and operations, we have increased our participation in government-wide task forces and law enforcement working groups, and actively expanded our monitoring and awareness of cyber-related matters. The OIG's Cyber Event Group is designed to identify key resources to ensure the OIG's continuous coverage and readiness to address potentially urgent cyber events affecting the FDIC or other federal entities. Importantly, and as noted earlier, as part of a reorganization announced during the reporting period, the IG created the Office of IT Audits and Cyber, and this group will further strengthen the OIG's knowledge and understanding of IT and cyber risks posing threats to the FDIC and the financial sector. Further discussion of our efforts in the cyber security realm is presented below.

A second area of high importance facing our office relates to the Dodd-Frank Act and the risk of failure of a SIFI. As noted in past semiannual reports, we undertook a risk assessment of the Act in the interest of better understanding its impact on the FDIC and our office. From that assessment, we have completed several reviews and continue to open others. Additionally, a provision in the Dodd-Frank Act could have a substantial bearing on our workload and resources, as along with the failure of a SIFI would come a set of responsibilities for the FDIC OIG as well. Specifically, in the event of a Title II Orderly Liquidation, the OIG would be required to conduct work to address various issues and meet certain reporting requirements based on that work. This area is also discussed below.

OIG Work in Support of Goal 4

FDIC OIG Increases Efforts to Address Cyber Threats

The OIG is tackling threats to the FDIC's IT environment on multiple fronts. One of our senior managers continues to serve as the OIG's Senior Cyber Security Liaison Officer. In that role, he is monitoring cyber-related activities and potential threats both internal and external to the FDIC and disseminating information to mitigate potential risk or harm to the FDIC, the OIG, and insured depository institutions. This same individual represents the OIG at meetings of the Data Breach Management Team for awareness purposes. He is also a member of the Insider Threat and Counterintelligence Program working group. Our interest is to proactively prevent any release by FDIC insiders—accidental or deliberate—of sensitive information beyond the walls of the FDIC's secure environment—through electronic means such as emailing sensitive information to personal email accounts or otherwise allowing such information to be disclosed without authorization. Others in the OIG play key roles in the IT and cybersecurity arena, to include our information security manager, IT professionals throughout the office, members of our ECU, and a Special Advisor to the IG. Our OIG Cyber Event Group, comprised of many of these individuals, continues to ensure OIG readiness to address cyber threats to the FDIC and share information with interested parties internal and external to the FDIC. Finally, the OIG's auditors, evaluators, and investigators involved in IT and cyber issues have begun regular coordination meetings to identify areas where collaboration can occur and ensure we are leveraging the skills, knowledge, and technical tools that exist in the OIG as we confront IT and cyber-related challenges.

Over the past reporting period, the OIG has also continued its participation in two key cyber-related task forces, in the interest of enhancing our understanding and awareness of current and emerging cyber issues and sharing our own expertise with others seeking to combat cyber threats. These task forces and our involvement are described below. Finally, we also participate in training activities sponsored by the 1st Information Operations Command of the U.S. Army to better understand the authorities, roles, and responsibilities of the defense and intelligence communities to identify, analyze, and respond to potential cyber threats.

FBI Cyber Task Force

The FBI has established a nationwide network of field office Cyber Task Forces to focus on cybersecurity threats. In addition to key law enforcement and homeland security agencies at the state and local level, each Cyber Task Force partners with many of the federal agencies at the headquarters level. This promotes effective collaboration and de-confliction of efforts at both the local and national level.

In support of the national effort to counter threats posed by terrorist, nation-state, and criminal cyber actors, each Cyber Task Force synchronizes domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions. Each Cyber Task Force leverages the authorities and capabilities of the participating agencies to accomplish the mission.

The FDIC OIG ECU continued its participation in the Washington Field Office Cyber Squad-4 (CY-4) during the reporting period. There are 30 federal, state, and local law enforcement agencies participating in CY-4, which has a total of more than 75 members. Through participation in CY-4, the ECU assists with new and ongoing FBI and partner cyber investigations by conducting interviews, victim notifications, forensic evidence review, and search warrants. The ECU agents also have access to many FBI informational systems and cyber notifications, allowing them to search for relevant data on subjects and entities already under investigation or intrusions at FDIC- insured banks. In connection with the task force, agents from financial regulatory agencies have formed a sub-group to avoid stove-piped approaches; enhance coordination; and share access to agency databases, systems, and resources, when possible.

Our involvement with the Cyber Task Force has increased our awareness of current threats. As a result of our access to the FBI's systems and other notifications received as a member of the task force, we have opened several investigative inquiries that are currently underway.

National Cyber Investigative Joint Task Force

The National Cyber Investigative Joint Task Force (NCIJTF) is a multi-agency cyber center that serves as the national focal point for coordinating, integrating, and sharing information related to cyber threat investigations. The task force performs its role through the cooperation and collaboration of its co-located partner agencies, its affiliate member agencies, and its on-site representatives from both international partners and state and local law enforcement organizations. Members have access to a unique, comprehensive view of the nation's cyber threats while working together in a collaborative environment in which they maintain the authorities and responsibilities of their home agencies.

The NCIJTF was established in 2008 by National Security Presidential Directive 54/HSPD-23. The responsibility for the task force's development and operation was given to the U.S. Attorney General who entrusted this mission to the FBI. In 2013, the NCIJTF separated from the FBI's cyber operational organization and increased the leadership and participation from its member agencies. Key functions of the NCIJTF include:

- Integrating domestic cyber data
- Coordinating whole-of-government cyber campaigns
- Analyzing and sharing domestic cyber information
- Exploiting financial data to generate new leads and to discover new threats
- Coordinating 24/7 cyber incident threat responses
- Identifying adversaries, compromises, exploit tools, and vulnerabilities
- Informing cyber policy and legislation decision-making

The NCIJTF is led by a Director assigned from the FBI and a Principal Deputy Director assigned from the National Security Agency. Assisting them in the operational direction and tempo of the task force is the NCIJTF Mission Council, comprised of representatives from the National Security Agency, Central Intelligence Agency, U.S. Secret Service, Department of Homeland Security, CYBERCOM, Air Force Office of Special Investigations, and FBI who serve in the roles of NCIJTF Deputy Directors. This leadership team helps identify cross-agency gaps and redundancies that might otherwise hinder the NCIJTF's ability to develop, aggregate, integrate, and appropriately share information relating to the nation's most critical adversary-based cyber threats.

Central to its mission, the NCIJTF provides a means for multi-agency teams to address both standing and emerging issues related to cyber threat investigations across the federal, state, local, and international law enforcement, intelligence, counterintelligence, and military communities. For example, the NCIJTF develops and coordinates whole-of-government cyber campaigns, acting as the integrating mechanism among stakeholders and ensuring all pertinent community members are leveraged for maximum results.

The NCIJTF collaborates closely with other Federal Cyber Centers, and as new cyber incidents arise, helps to ensure that the right U.S. government resources are brought to bear. The task force also provides guidance on financial investigative tools and techniques, generates new leads, and uncovers new cyber threats by exploiting financial data.

The OIG has assigned one of its special agents to the NCIJTF. Within the task force, the agent works within the Office of Threat Pursuit. This office supports U.S. government criminal and national security cyber operations and intelligence matters through case coordination, virtual currency consultation, and cyber financial analysis. Specifically, the Office of Threat Pursuit enhances cyber investigations through the application of financial investigative techniques, procedures and business acumen, in order to identify evidence of criminal and national security threats, identify co-conspirators and benefactors, establish an enterprise's hierarchy, and identify and seize assets.

As an independent federal regulator, the FDIC does not have direct access to the federal cyber centers. However, as a member of the NCIJTF, the FDIC OIG does have access and is also able to provide insight into the financial industry by acting as a subject matter expert. In addition, the FDIC OIG has been able to coordinate with other federal regulators within the financial industry, including the Securities and Exchange Commission OIG, Office of the Comptroller of Currency, and others. The OIG has used information obtained, both classified and unclassified, to brief the IG and other appropriate FDIC senior staff and to conduct additional research on current trends and threats affecting the financial and banking sectors.

Dodd-Frank Act Risk Assessment and Related Work

Some months ago, the OIG undertook an initiative to keep current with the FDIC's efforts associated with implementation of risk management, monitoring, and resolution authorities emanating from the Dodd–Frank Act. Our purpose in doing so was to understand and analyze operational issues and emerging risks impacting the FDIC, the financial community, and internal OIG operations and plans. This continuous and focused risk assessment and monitoring enhanced our more traditional, periodic OIG risk assessment and planning efforts and assisted with the OIG's internal preparation efforts in the event a SIFI should fail. The assessment and monitoring provided an informal, efficient means of making FDIC and OIG management aware of issues and risks warranting attention.

We subsequently identified areas where we believed we could add value. To name a few, and as discussed in other semiannual reports, we audited the FDIC's controls for safeguarding sensitive information in resolution plans, and we evaluated the FDIC's resolution plan review process. During the reporting period, as discussed earlier, we issued a report on the FDIC's risk monitoring of SIFIs' proximity and speed to default or danger of default.

In addition, currently under the Dodd-Frank Act--Title II Orderly Liquidation Authority, Section 211, the FDIC IG shall conduct, supervise, and coordinate audits and investigations of the liquidation of any covered financial company by the Corporation as receiver under the title, including collecting and summarizing:

- a description of actions taken by the FDIC as receiver;
- a description of material sales, transfers, mergers, obligations, purchases, and other material transactions by the FDIC;
- an evaluation of the adequacy of the policies and procedures of the Corporation under section 203(d) and orderly liquidation plan under section 210(n)(14);
- an evaluation of the utilization by the FDIC of the private sector in carrying out its function, including the adequacy of any conflict-of-interest reviews; and
- an evaluation of overall performance of the FDIC in liquidating the covered financial company, including administrative costs, timeliness of the liquidation process, and impact on the financial system.

The timing of such work would be not later than 6 months after the date the Corporation is appointed receiver and every 6 months thereafter. Findings and evaluations are to be included in the IG's semiannual reports and the IG would appear before appropriate committees of the Congress, if requested.

The OIG views the above requirements to be highly significant to our office and the Corporation. We have planned for such an eventuality by researching issues relating to scope, frequency, reporting, funding, and needed resources. We have considered an audit approach to such work, corresponding reporting mechanisms in line with Title II of the Dodd-Frank Act, and how best to capture and track any expenses we incur if we are statutorily required to audit or investigate any covered financial company by the Corporation as receiver. We will continue to monitor any change in the requirements of Title II and respond accordingly.

Goal 5: Operational Efficiency and Workforce Excellence

Maximize OIG operational efficiency and workforce excellence

While the OIG's audit, evaluation, and investigation work is focused principally on the FDIC's programs and operations, we also hold ourselves to high standards of performance and conduct. We seek to recruit and retain a high-quality staff, and promote employee engagement at all levels of the organization. A major challenge for the OIG over the past few years was ensuring that we had the resources needed to effectively and efficiently carry out the OIG mission at the FDIC, given a sharp increase in the OIG's statutorily mandated work brought about by numerous financial institution failures, the FDIC's substantial resolution and receivership responsibilities, and its resolution authorities under the Dodd-Frank Act. We now have a bit more discretion in planning our work and have been able to focus attention on certain corporate activities that we have not reviewed for some time. Still, however, we are facing future attrition in our OIG workforce and are currently operating below our authorized staffing level for fiscal year 2017. We are closely monitoring our staffing and taking steps to ensure we are positioned to sustain quality work to address risk areas and replenish our human resources as OIG staff leave.

To ensure a high-quality staff, we must continuously invest in keeping staff knowledge and skills at a level equal to the work that needs to be done, and we emphasize and support training and development opportunities for all OIG staff. We also seek to ensure effective and efficient use of human, financial, IT, and procurement resources in conducting OIG audits, evaluations, investigations, and other support activities, and have a disciplined budget process to see to that end. In all of our operations, we want to leverage the capabilities of the technological tools at our disposal. That said, we are acutely aware of information security vulnerabilities and continue to take steps to secure and safeguard the information that we possess.

Our office continues efforts to better manage the voluminous records in our possession—both in electronic and hard copy form. Records management activities are ongoing and designed to ensure the OIG maintains information needed to carry out its mission and respond to litigation needs or Congressional requests for documents. Similarly, we are seeking to more clearly capture and outline our policies and procedures for the numerous operational activities that we undertake on a daily basis to ensure that these activities occur efficiently and effectively.

To achieve excellence, the OIG must be professional, objective, fact-based, nonpartisan, fair, and balanced in all its work. Also, the IG and OIG staff must be free both in fact and in appearance from personal, external, and organizational impairments to their independence. As a member of CIGIE, the OIG is mindful of the Quality Standards for Federal Offices of Inspector General. Further, the OIG conducts its audit work in accordance with generally accepted government auditing standards; its evaluations in accordance with *Quality Standards for Inspection and Evaluation*; and its investigations, which often involve allegations of serious wrongdoing that may involve potential violations of criminal law, in accordance with Quality Standards for Investigations and procedures established by DOJ.

The OIG supports the Government Performance and Results Modernization Act of 2010, signed into law on January 4, 2011, and is committed to applying its principles of strategic planning and performance measurement and reporting to our operations. Importantly, the OIG has re-examined the strategic and performance goals and related activities that have guided our past efforts and continues strategic planning efforts to provide the best framework within which to carry out our mission and achieve goals in the current FDIC and OIG operating environment.

OIG Work in Support of Goal 5

The following activities from the reporting period reflect our commitment to maximizing operational efficiency and ensuring workforce excellence:

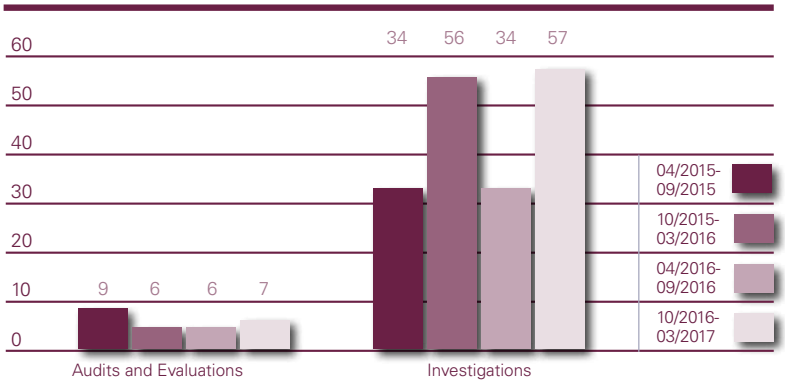
- Carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. Positions filled during the reporting period included six new audit and evaluation staff members and three criminal investigators.
- Recruited interns with skills in finance, IT, law, communications, and management, and planned for their involvement in ongoing OIG activities.
- 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. Selected OIG staff to enroll in the American Bankers Association Commercial Lending School, Southwestern Methodist University, Dallas, Texas; and Colorado Graduate School of Banking, University of Colorado, Boulder, Colorado.
- Researched options for a new training and development system to enable better tracking of professional development of OIG staff.
- Enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities.
- Provided one of the members of the OIG's Counsel's Office to serve as a Special Assistant U.S. Attorney for multiple cases and trials involving bank fraud. This opportunity allows the Associate Counsel to apply legal skills as part of the prosecutorial teams in advance of and during the trials.
- Announced three new OIG awards to acknowledge outstanding efforts and to provide staff an opportunity to nominate peers: Distinguished Professional Award, Spirit of the OIG Award, and IG Award for Excellence.
- Continued to implement a new investigative case management system and worked to migrate audit and evaluation data and upgrade TeamMate.
- 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.
- Undertook a number of initiatives to ensure security of the OIG's IT infrastructure and internal operations, including researching other OIGs' IT environments to identify possible best practices to adopt, and disseminating IT security-related notifications to OIG staff.
- Addressed independence concerns regarding OIG to OIG internal emails residing in the FDIC's email vault and continued to coordinate with the Division of Information Technology as it remediates the problem of email comingling. Also worked with a consultant to assist our office in independently reviewing how the problem was identified and is being remediated.

- Coordinated with a contractor to refine the technical and security requirements for redesign of the OIG's external Website.
- Reviewed and updated 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 and made substantial progress converting and transferring such policies to a new automated policies and procedures repository for use by all OIG staff.
- 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.
- Prepared a budget justification document 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.
- Continued to monitor, track, and control OIG spending, particularly as it relates to OIG travel-related expenses, use of procurement cards, and petty cash expenditures.
- Relied on OIG Counsel's Office to provide legal advice and counsel to teams conducting audits and evaluations, and to support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.
- Coordinated with the Railroad Retirement Board OIG as it conducted the peer review of the system of quality control for our audit organization, and received a rating of "pass" as a result of the Railroad Retirement Board OIG's review.
- Undertook strategic OIG planning efforts for all 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 and will help ensure office-wide efforts in pursuit of the OIG mission are efficient, effective, and economical.

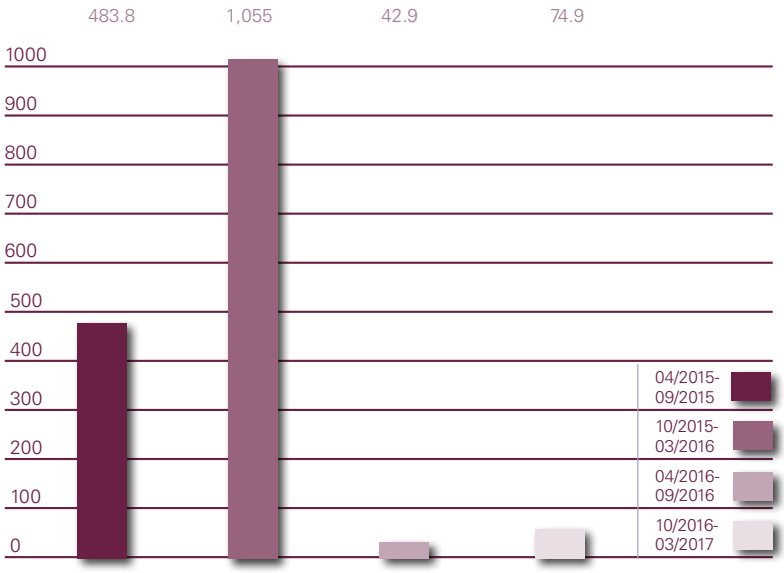
Cumulative Results (2-year period)

Nonmonetary Recommendations	
April 2015 – September 2015	20
October 2015 – March 2016	12
April 2016 – September 2016	16
October 2016 – March 2017	27

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	52
Section 5(a)(1) Significant problems, abuses, and deficiencies	11-21
Section 5(a)(2) Recommendations with respect to significant problems, abuses, and deficiencies	11-21
Section 5(a)(3) Recommendations described in previous semiannual reports on which corrective action has not been completed	53
Section 5(a)(4) Matters referred to prosecutive authorities	62
Section 5(a)(5) Summary of each report made to the head of the establishment regarding information or assistance refused or not provided	62
Section 5(a)(6) Listing of audit, inspection and evaluation reports by subject matter with monetary benefits	60
Section 5(a)(7) Summary of particularly significant reports	11-21
Section 5(a)(8): Statistical table showing the total number of audit reports and the total dollar value of questioned costs	61
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	61
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	62
• no establishment comment was received within 60 days of providing the report	62
• there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations	55
Section 5(a)(11) Significant revised management decisions during the current reporting period	62

Reporting Requirements (continued)	Page
Section 5(a)(12) Significant management decisions with which the OIG disagreed	62
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	65
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	62
Section 5(a)(18) A description of metrics used for Section 5(a)17 information	62
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	63
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	63
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	63
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	63

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, including the following:

Public Law No. 114-317, the Inspector General Empowerment Act: Counsel's Office (CO) reviewed and analyzed the Act and participated in a CIGIE Working Group regarding the Act's potential impacts on IG semiannual reporting requirements under the Inspector General Act, Website reporting requirements, and actions to take when an OIG document contains recommendations for corrective action.

Public Law No. 114-328, the National Defense Authorization Act of 2017: CO reviewed section 1138 of the Public Law, namely, the Administrative Leave Act of 2016, and will await implementing regulations and/or guidance from Office of Personnel Management and CIGIE regarding the Act.

Draft legislation: CO reviewed the Every Dollar Counts Act, which would expand IG coverage to agencies that do not currently have an IG and which would address IG pay issues. We did not provide comments.

Draft CIGIE Legislative Priorities: CO provided comments to CIGIE regarding a draft version of the Whistleblower Right to Know Act, which would amend IG Act of 1978 provisions regarding Whistleblower Protection Ombudsmen.

Draft legislation: The Federal Records Modernization Act: CO provided comments on provisions of the bill affecting IG semiannual reporting requirements regarding federal records management practices.

OMB Memoranda 17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements, and 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information: CO sought to clarify with OMB the requirements under FISMA for congressional reporting of information security breaches and/or incidents.

Various pieces of legislation introduced in Congress or OMB memoranda: CO reviewed and prepared a digest for internal OIG purposes describing the following:

- H.R. 69, the Thoroughly Investigating Retaliation Act
- H.R. 71, the Taxpayers Right to Know Act
- H.R. 26 and S. 21, the Regulations from the Executive in Need of Scrutiny Act of 2017
- H.R. 5, the Regulatory Accountability Act of 2017
- S. 790, the Return to Prudent Banking Act
- S. 585, the Dr. Chris Kirkpatrick Whistleblower Protection Act
- S. 582, the Office of Special Counsel Reauthorization Act of 2016
- OMB Memorandum 17-21, Implementing Executive Order 13771

OMB Circulars A-130, Managing Information as a Strategic Resource, and A-123, Management's Responsibility for Risk Management and Internal Controls, each as revised in 2016: CO coordinated with the FDIC Legal Division in determining the legal applicability of those Circulars to the FDIC, which could impact future OIG work.

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

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

Management Action in Process: (seven 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 Planned 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.*

*The FDIC is considering new requirements in Presidential Policy Directive PPD 40, National Continuity Policy (July 15, 2016) and updates to the Department of Homeland Security's Federal Continuity Directives as it works to address this recommendation.

Management Action in Process (continued)		
AUD-15-008 **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	**1**[a]	Review and clarify, as appropriate, existing policy and guidance pertaining to the provision and termination of banking services to ensure it adequately addresses banking products other than deposit accounts, such as credit products.
	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.
	3	Review and clarify, as appropriate, existing supervisory policy and guidance to ensure it adequately defines moral suasion in terms of the types and circumstances under which it is used to address supervisory concerns, whether it is subject to sufficient scrutiny and oversight, and whether meaningful remedies exist should moral suasion be misused.
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.
	3	Ensure that the revisions to the FDIC's incident response policies and procedures addressed in Recommendation 1 of this report include criteria for determining whether an incident is major consistent with FISMA and OMB Memorandum M-16-03.
	4[a]	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.

[a]The OIG is evaluating 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 Modernization Act of 2014 (FISMA) states that the 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, OMB policy and guidelines, and applicable National Institute of Standards and Technology 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
AUD-15-003 **In-Depth Review of the Failure of Vantage Point Bank, Horsham, Pennsylvania** March 30, 2015	FDIC's Division of Risk Management Supervision requested that we conduct an in-depth review because Vantage Point Bank's (VPB) failure involved unusual circumstances. Specifically, the bank engaged in material changes to its business plan during its de novo period without regulatory approval. The objectives of the in-depth review were to (1) determine the causes of VPB's failure and resulting loss to the DIF and (2) evaluate the FDIC's supervision of the institution, including the FDIC's implementation of the Prompt Corrective Action provisions of Section 38 of the FDI Act. VPB failed primarily because its Board of Directors and management did not effectively manage the risks associated with the bank's rapid expansion of its mortgage banking operation. Our report contained three recommendations intended to improve the effectiveness of the FDIC's supervision of newly insured institutions, such as VPB.	3	1	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-15-007 **Material Loss Review of Doral Bank, San Juan, Puerto Rico** September 3, 2015	The FDIC OIG conducted a material loss review of the failure of Doral. The objectives were to (1) determine the causes of Doral's failure and the resulting material loss to the DIF and (2) evaluate the FDIC's supervision of Doral, including the FDIC's implementation of the Prompt Corrective Action provisions of section 38 of the FDI Act. Poor asset quality was the underlying cause of Doral's failure. Puerto Rico's severe and prolonged economic decline coupled with weak underwriting and risk management practices were significant factors in the deterioration of Doral's loan portfolio. The report included two recommendations. The first one was intended to enhance the effectiveness of supervisory controls for ensuring the FDIC's compliance with the FDI Act examination frequency requirements when a bank is on a targeted examination schedule. The second recommendation involved issuing or revising policy guidance to document the requirements and responsibilities of Regional Accountants related to conducting analysis for complex and/or unique accounting transactions, including when such matters should be escalated within the Division.	2	1	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
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 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) 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 our 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 was 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 considered 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 contained 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	3	NA

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-16-001 **FDIC's Information Security Program – 2015** October 28, 2015	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct the 2015 FISMA audit. The objective of the 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 contained six recommendations that were intended to improve the effectiveness of the FDIC's information security program controls and practices.	6	2	NA
EVAL-16-005 **The FDIC's Controls Over Receivership Asset Securitizations** June 30, 2016	The FDIC OIG evaluated select key controls over the FDIC receivership asset securitizations following their origination, to ensure those controls are performing as intended. We contracted with the independent professional services firm BDO USA, LLP to perform the evaluation. Overall, BDO did not discover any significant deficiencies in DRR processes and controls associated with monitoring receivership asset securitizations and structured sales of guarantee notes following their originations. However, BDO concluded that opportunities exist for DRR to better document processes performed in procedures and job aids, and to address key personnel dependencies within the Capital Markets Group and closing/post-closing support contractor. We made six recommendations to better document processes within DRR policies, procedures, and/or job aids, enhance certain controls, and address key personnel dependencies.	6	1	$55,000

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

Report Number, Title, and Date	Report Summary	Recommendations		Potential Cost Savings
		Total	Outstanding	
AUD-16-003 **The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans** July 6, 2016	The resolution plans required by the Dodd-Frank Act contain some of the most sensitive information that the FDIC maintains. Accordingly, safeguarding the plans from unauthorized access or disclosure is critically important to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system. In September 2015, an employee working in the FDIC's Office of Complex Financial Institutions abruptly resigned from the Corporation and took sensitive components of resolution plans without authorization. The objectives of the audit were to (a) determine the factors that contributed to this security incident involving sensitive resolution plans and (b) assess the adequacy of mitigating controls established subsequent to the incident. We identified a number of factors that contributed to the security incident involving sensitive resolution plans. Most notably, an insider threat program would have better enabled the FDIC to deter, detect, and mitigate the risks posed by the employee. In addition, a key security control designed to prevent employees with access to sensitive resolution plans from copying electronic information to removable media failed to operate as intended. Our report described additional control improvements that the FDIC should implement to better safeguard sensitive resolution plans. The report contained six recommendations. One recommendation was to establish a corporate-wide insider threat program. The remaining five recommendations were to strengthen the FDIC's information security controls, particularly with respect to safeguarding sensitive resolution plans submitted to the Corporation under the Dodd-Frank Act.	6	2	NA
AUD-16-004 **The FDIC's Process for Identifying and Reporting Major Information Security Incidents** July 7, 2016	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 provided reasonable assurance that major incidents would be 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 contained five recommendations addressed to the Chief Information Officer that were 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	5	NA

Table III: Audit and Evaluation Reports Issued by Subject Area

Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	**Title**	**Total**	**Unsupported**	
Supervision				
EVAL-17-003 January 26, 2017	*The FDIC's Risk Monitoring of Systemically Important Financial Institutions' Proximity and Speed to Default or Danger of Default*			
EVAL-17-004 February 14, 2017	*Technology Service Provider Contracts with FDIC-Supervised Institutions*			
Receivership Management				
EVAL-17-001 December 6, 2016	*The FDIC's Efforts to Ensure SLA Recoveries Are Identified and Remitted*			
AUD-17-003 March 27, 2017	*The FDIC's Failed Bank Data Services Project*			
Resources Management				
AUD-17-001 November 2, 2016	*Audit of the FDIC's Information Security Program - 2016*			
EVAL-17-002 December 15, 2016	*OIG Hotline Complaints Regarding Employee Travel*	$122,423		
AUD-17-002 December 20, 2016	*Invoices Submitted by Lockheed Martin Services, Inc. under FDIC Contract No. CORHQ-08-G-0120*	$4,170		
Totals for the Period		**$126,593**	**$0**	**$0**

Table IV: Audit and Evaluation Reports Issued with Questioned Costs

		Questioned Costs	
	Number	Total	Unsupported
A. For which no management decision has been made by the commencement of the reporting period.	0	$0	$0
B. Which were issued during the reporting period.	2	$126,593	$0
Subtotals of A & B	**2**	**$126,593**	**$0**
C. For which a management decision was made during the reporting period.	2	$126,593	$0
(i) dollar value of disallowed costs.	1	$4,170	$0
(ii) dollar value of costs not disallowed.	1	$122,423	$0
D. For which no management decision has been made by the end of the reporting period.	0	$0	$0
Reports for which no management decision was made within 6 months of issuance.	0	$0	$0

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

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

Table VI: Status of OIG Recommendations Without Management Decisions

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

Table VII: Status of OIG Reports Without Comments

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

Table VIII: Significant Revised Management Decisions

During this reporting period, there were no significant revised management decisions.

Table IX: Significant Management Decisions with Which the OIG Disagreed

During this reporting period, there were no significant management decisions with which the OIG disagreed.

Table X: Instances Where Information Was Refused

During this reporting period, there were no instances where information was refused.

Table XI: Investigative Statistical Information

Number of investigative reports issued: **57**

Number of persons referred to the Department of Justice for criminal prosecution: **68**

Number of persons referred to state and local prosecuting authorities for criminal prosecution: **2**

Number of indictments and criminal Informations: **65**

Description of the metrics used for the above information: Reports issued reflects case closing memorandums issued to FDIC management. With respect to the 68 referrals to the Department of Justice, the total represents 58 individuals, 8 business entities, and 2 instances where the case was referred but the subjects are unknown at this time. Two individuals were referred to state and local prosecutors. Our total indictments and criminal Informations statistic 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

We terminated one evaluation assignment and issued a memorandum to management that was not disclosed to the public, as discussed briefly below:

November 30, 2016 Memorandum Regarding FDIC OIG Evaluation of the FDIC's Efforts to Address Risks from an Identified Router Software Vulnerability: In mid-August 2016, Cisco Systems, Inc., confirmed that leaked malware exploited a high-severity vulnerability that had gone undetected for years. Importantly, the malware could be used to attack Cisco router software designed to protect and manage information networks and data centers. As Cisco products are commonly used in IT networks, we initiated an assignment to evaluate the FDIC's susceptibility to the vulnerability, including how the systems of the FDIC's outsourced IT service providers and those of FDIC-supervised banks and their service providers might be affected. As part our review, we also gained an understanding of the FDIC's actions to assess and address internal and external risks associated with the reported vulnerability.

We determined that the FDIC had evaluated the risks to its own systems as well as those associated with service providers and the industry. The FDIC took steps it believed were appropriate to remediate those risks.

We discussed the results of our work with FDIC officials at the completion of our review. In a memorandum to management, we communicated suggestions related to (1) vendor notification guidelines to ensure effective communication and (2) coordination between the Chief Information Officer and the FDIC's RMS with respect to known and previously unknown malware and other security threats.

Having conveyed those points to the responsible officials, we terminated the evaluation and plan to leverage the results of this work as we plan and perform future work in the information security area.

We did not close any investigations involving senior government employees that were not disclosed to the public.

Appendix 2

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

FDIC OIG Review Activity for the Period October 1, 2016 through March 31, 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 Completed				
The Woodbury Banking Company (Woodbury, Georgia)	8/19/16	$5.2	The bank was unable to meet requirements of a 2011 Consent Order and a 2015 Modification to that Order, including requirements for minimum levels of capitalization. Further, the bank's capital level represented a significant safety and soundness concern.	No
First CornerStone Bank (King of Prussia, Pennsylvania)	5/6/16	$10.8	The bank was unable to meet certain requirements of a May 2010 Consent Order and August 2014 Amendment to that Order, and operated in an unsafe and unsound manner.	No
Trust Company Bank (Memphis, Tennessee)	4/29/16	$7.2	The bank was conducting its business in an unsafe and unsound manner.	No
Harvest Community Bank (Pennsville, New Jersey)	1/13/17	$22.3	The bank was unable to meet requirements of a 2015 Consent Order and operated in an unsafe and unsound manner.	No
Reviews Ongoing				
Proficio Bank (Cottonwood Heights, Utah)	3/3/17	$11.0		

Appendix 3

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 *Guide for Conducting Peer Reviews of Audit Organizations of Federal Offices of Inspector General*, based on requirements in the *Government Auditing Standards* (Yellow Book). Federal audit organizations can receive a rating of pass, pass with deficiencies, or fail.

- The 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.

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 National Archives and Records Administration OIG

The FDIC OIG completed a peer review of the audit operations of the National Archives and Records Administration (NARA) OIG, and we issued our final report to that OIG on April 30, 2014. We reported that in our opinion, the system of quality control for the audit organization of the NARA OIG, in effect for the 12 months ended September 30, 2013, had been suitably designed and complied with to provide the NARA OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. The NARA OIG received a peer review rating of pass.

NARA OIG posted the peer review report on its Website at www.archives.gov/oig/

We are completing a peer review of the audit organization of the Tennessee Valley Authority OIG and will include those results in our next semiannual report.

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, as applicable. 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.

We plan to begin our peer review of the investigative operations of the Small Business Administration OIG in August 2017.

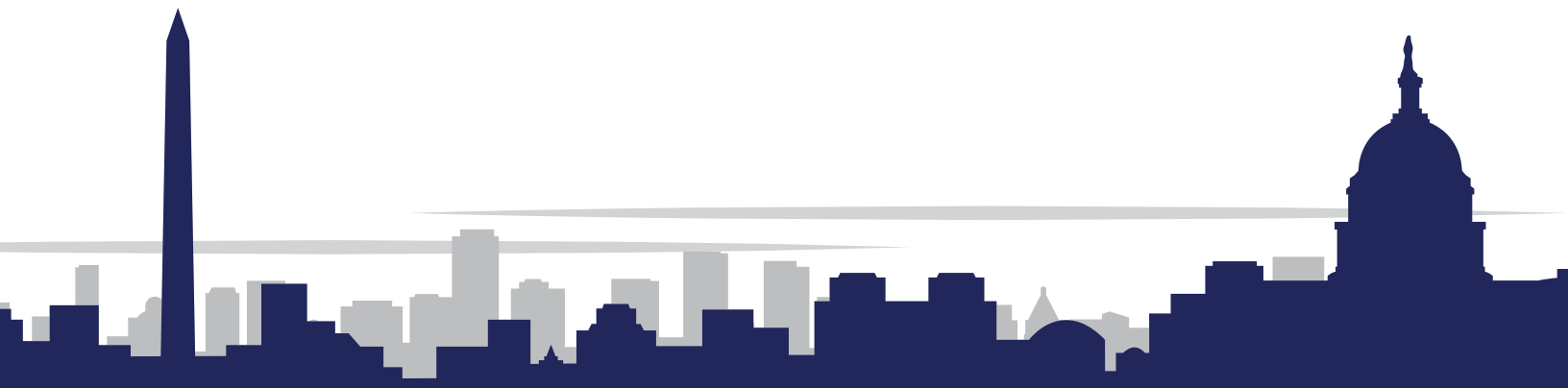
Congratulations and Farewell

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.

Anitra Hawkins

Ann Lewis

Michael Stevens



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

To learn more about the FDIC OIG and for more information on matters discussed in this Semiannual Report, visit our Website:
http://www.fdicig.gov

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. The OIG maintains a toll-free, nationwide Hotline **(1-800-964-FDIC)**, electronic mail address **(IGhotline@FDIC.gov)**, and postal mailing address. The Hotline is designed to make it easy for employees and contractors to join with the OIG in its efforts to prevent fraud, waste, abuse, and mismanagement that could threaten the success of FDIC programs or operations.

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