OIG

OCTOBER 1 2014 • MARCH 31 2015

OFFICE OF INSPECTOR GENERAL | SEMIANNUAL REPORT TO THE CONGRESS

FDIC

FEDERAL DEPOSIT INSURANCE CORPORATION

FDIC

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 6,560 individuals carry out the FDIC mission throughout the country. According to most current FDIC data, the FDIC insured more than $6.2 trillion in deposits in 6,509 institutions, of which the FDIC supervised 4,138. 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 $65.3 billion as of March 31, 2015. Receiverships under FDIC control as of March 31, 2015, totaled 483, with about $7.3 billion in assets.

Office of Inspector General

Semiannual Report to the Congress

October 1, 2014 – March 31, 2015

Federal Deposit Insurance Corporation

Inspector General 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, 2014 through March 31, 2015. Thanks to the dedication of FDIC OIG staff, our work continues to promote economy, efficiency, and effectiveness in FDIC programs and operations, and integrity within the banking industry. Over the past 6-month period, we have dealt with a number of challenging issues and have done our best to approach them vigorously and in creative ways. Several examples from the reporting period follow and are discussed in more detail in our report.

- We completed a comprehensive review of the FDIC's supervisory approach to the ever-increasing risk of cyberattacks and made recommendations to strengthen the manner in which the FDIC ensures that financial institutions and technology service providers are prepared to protect against, detect, respond to, and recover from such events. That work also served as a catalyst for additional OIG work to ensure effective communication between various OIG component offices and other parties both internal and external to the Corporation who have a common interest in protecting FDIC systems and information and the broader financial services industry infrastructure.

- We continued to carry out our independent risk assessment of the FDIC's activities related to the Dodd–Frank Wall Street Reform and Consumer Protection Act (Dodd–Frank Act). This initiative is designed to keep current with the FDIC's efforts associated with implementation of risk management, monitoring, and resolution authorities emanating from the Dodd–Frank Act. We are doing so to more fully understand and analyze operational and political issues and emerging risks impacting the FDIC, the financial community, and internal OIG operations and plans. During the reporting period, we continued to observe the FDIC's Complex Financial Institutions Coordination Group meetings, monitored Dodd–Frank Act issues and media coverage, created a framework through which we can view and communicate Dodd-Frank Act-related risks, and arranged to brief senior-most FDIC leadership to share our perspectives and hear their views on areas where the OIG can add the most value going forward.

- Our Office of Investigations, in partnership with U.S. Attorneys and law enforcement colleagues throughout the country, successfully brought to justice numerous former bank officials and other bank-affiliated parties who had used their positions of trust to undermine the integrity of the banking system. Of special note, in one such case, following a 6-week jury trial, the former Chief Operating Officer of United Commercial Bank, based in San Francisco, California, was found guilty of conspiring with others within the bank to falsify key bank records to conceal millions of dollars in losses and falsely inflate the bank's financial statements. In commenting on the case, the U.S Attorney stated: "UCB is one of the largest criminal prosecutions brought by the United States Department of Justice of wrongdoing by bank officers arising out of the 2008 financial crisis. With actual losses exceeding a half a billion dollars, the prosecution of [the Chief Operating Officer] and other senior officers at UCB is one of the most significant financial fraud cases in the history of the Northern District of California."

- We responded to a number of Congressional requests during the reporting period, including one in which we were asked to review the FDIC's involvement with the Department of Justice program known as Operation Choke Point. We are currently conducting that work in two parts—one investigating the serious allegation that a senior official provided false testimony to the Congress; the other assessing whether the actions and policies of the FDIC were consistent with applicable laws, regulations, and policy, and with the mission of the FDIC. These efforts were ongoing as of the end of the reporting period.

- Recognizing that international financial systems are interconnected and that events affecting one system will automatically impact another, we took steps to broaden our knowledge of global deposit insurance systems and resolution processes. Staff from the OIG met with a delegation from the Deposit Insurance Corporation of Japan (DICJ) to share information on the mission of the FDIC OIG, our investigative function and its coordination with the Department of Justice, and two of our recent investigative cases. Additionally, I recently traveled to Japan at the invitation of the head of the DICJ to speak at its 8th Round Table about the OIG, our role, and the challenges of determining liability in bank resolutions. Representatives from 38 deposit insurance institutions and relevant entities from 15 countries or jurisdictions around the world attended this forum. Earlier in the reporting period I also met with the Chief Internal Auditor of the Deposit Insurance Corporation of Canada to exchange ideas on issues of mutual interest.
- As an independent oversight organization at the FDIC, we continued our planning efforts in the post-crisis environment by taking a fresh look at the Corporation's programs and activities, priorities, systems, and governance structures, with a view toward developing a repeatable and continuous planning process that identifies and helps us address those areas of most risk to the FDIC and the banking industry. In that regard we also came together as an office at an OIG-wide conference at the end of April where our auditors, evaluators, and investigators had opportunities to share with all OIG staff some of their most significant work, insights gained from their efforts, and best practices—all in the interest of informing our thinking about the future and our strategic direction.

Our former Inspector General resigned to become the Department of Defense Inspector General on September 27, 2013. I have been honored to lead our office since that time and appreciate the support we have received from the FDIC Board of Directors and senior management. On behalf of the office, I underscore our commitment to our stakeholders—the FDIC, Congress, other regulatory agencies, OIG colleagues, law enforcement partners, and the public. We rely on the continued strength of positive working relationships with all of them as we strive to help the FDIC accomplish its mission and work in the best interest of the American people.

Fred W. Gibson, Jr.
Acting Inspector General
April 2015

Table of Contents

Inspector General Statement ii

Acronyms and Abbreviations vi

Highlights and Outcomes 1

Strategic Goal Areas

Goal 1: Supervision
Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly 8

Goal 2: Insurance
Help the FDIC Maintain the Viability of the Insurance Fund 33

Goal 3: Consumer Protection
Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy 35

Goal 4: Receivership Management
Help Ensure that the FDIC Efficiently and Effectively Resolves Failing Banks and Manages Receiverships 38

Goal 5: Resources Management
Promote Sound Governance and Effective Stewardship and Security of Human, Financial, Information Technology, and Physical Resources 44

Goal 6: OIG Resources Management
Build and Sustain a High-Quality OIG Staff, Effective Operations, OIG Independence, and Mutually Beneficial Working Relationships 54

Cumulative Results (2-year period) 64

Reporting Requirements 65

Appendix 1
Information Required by the Inspector General Act of 1978, as amended 66

Appendix 2
Information on Failure Review Activity 69

Appendix 3
Peer Review Activity 72

Congratulations and Farewell 74

Acronyms and Abbreviations

ARMS	automated records management system
CCO	chief credit officer
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
COO	chief operating officer
CSIRT	Computer Security Incident Response Team
DIF	Deposit Insurance Fund
Dodd-Frank Act	Dodd–Frank Wall Street Reform and Consumer Protection Act
DRR	Division of Resolutions and Receiverships
ECU	Electronic Crimes Unit
FBI	Federal Bureau of Investigation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FHLBB	Federal Home Loan Bank Board
FI	financial institution
FISMA	Federal Information Security Management Act of 2002
FRB	Board of Governors of the Federal Reserve System
FY	fiscal year
GAO	U.S. Government Accountability Office
GFRS	Governmentwide Financial Report System
GPRA	Government Performance and Results Act of 1993
IP	internet protocol
IRS CID	Internal Revenue Service, Criminal Investigation Division
IT	information technology
IT-RMP	Information Technology-Risk Management Program
MB&T	Montgomery Bank & Trust
NARA	National Archives and Records Administration
NCIJTF	National Cyber Investigative Joint Task Force
NIST	National Institute of Standards and Technology
OCFI	Office of Complex Financial Institutions
OIG	Office of Inspector General
OMB	Office of Management and Budget
ORE	owned real estate
PDBS	Pennsylvania Department of Banking and Securities
PII	personally identifiable information
POA&M	plan of action and milestones
RIMU	Records and Information Management Unit
RMS	Division of Risk Management Supervision
SAR	Suspicious Activity Report
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
TSP	technology service provider
UCB	United Commercial Bank
VA	Department of Veterans Affairs
VPB	Vantage Point Bank

The OIG conducts its work in five strategic goal areas that are linked to the FDIC's mission, programs, and activities, and one that focuses on the OIG's internal business and management processes. A summary of our completed work during the reporting period, along with references to selected ongoing assignments is presented below, by goal area. We are revising our goals and related performance indicators as we plan for fiscal year (FY) 2016. In the interim, for FY 2015, we are highlighting our work within the framework of the goal areas that follow.

Strategic Goal 1: Supervision

Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly

Our work in helping to ensure that the nation's banks operate safely and soundly takes the form of audits, investigations, evaluations, and extensive communication and coordination with FDIC divisions and offices, law enforcement agencies, other financial regulatory OIGs, and banking industry officials. In support of this goal, during the reporting period, we issued a comprehensive report on the FDIC's supervisory approach to cyberattack risks. We made nine recommendations to increase the level of assurance that financial institutions and technology service providers are prepared for cyberattacks. This work prompted additional efforts to better understand cyber risks and coordinate both within the OIG and with external parties to address such risks to FDIC-insured institutions and technology service providers. We also issued an in-depth review of the failure of Vantage Point Bank, Horsham, Pennsylvania, a de novo bank that failed because the bank's Board and management did not effectively manage the risks associated with the bank's rapid expansion of its mortgage operations. We also noted that the FDIC's supervision of the bank could have been improved, and we made three recommendations to improve the effectiveness of the FDIC's supervision of newly insured institutions such as Vantage Point Bank. We completed 10 failure reviews of institutions whose failures caused losses to the Deposit Insurance Fund of less than the threshold of $150 million if failing after January 1, 2012 and under $50 million if failing on or after January 1, 2014, and determined whether unusual circumstances existed that would warrant an in-depth review in those cases. Ongoing OIG audit work includes a material loss review of Doral Bank, San Juan, Puerto Rico, whose failure in February 2015 caused an estimated $749 million loss to the Deposit Insurance Fund. We are also conducting work related to a Congressional request involving the Department of Justice program known as Operation Choke Point.

With respect to investigative work, as a result of cooperative efforts with U.S. Attorneys throughout the country, numerous individuals were prosecuted for financial institution fraud, and we also successfully pursued a number of mortgage fraud schemes. Our efforts in support of bank fraud, mortgage fraud, and other financial services working groups also supported this goal. Particularly noteworthy results from our casework include the pleas and sentencings of a number of former senior bank officials and bank customers involved in fraudulent activities that undermined the institutions and, in some cases, contributed to the institutions' failures. For example, the Chief Operating Officer of United Commercial Bank, based in San Francisco, California, was found guilty of conspiring with others within the bank to falsify key bank records to conceal millions of dollars in losses and falsely inflate the bank's financial statements. In another high-profile case, a former bank director of Montgomery Bank and Trust, Ailey, Georgia, who had earlier faked his own death and later pleaded guilty to bank, wire, and securities fraud, was sentenced to 30 years in prison. He misappropriated and embezzled millions of dollars from the bank. He also duped other investors of more than $51 million and lost most of their funds through speculative trading and other investments. In another case, for their roles in a $49.6 million mortgage fraud scheme, the wife of a former developer and two other co-conspirators were sentenced to 14 years and 20 years in prison each, respectively. The former developer was earlier sentenced to 27 years and 3 months in prison, as mastermind of the scheme.

The Office of Investigations also continued its close coordination and outreach with the Division of Risk Management Supervision (RMS), the Division of Resolutions and Receiverships, and the Legal Division by way of attending quarterly meetings, regional training forums, and regularly scheduled meetings with RMS and the Legal Division to review Suspicious Activity Reports and identify cases of mutual interest. We have coordinated regularly on enforcement action matters with the Legal Division and RMS, an activity that continues to be mutually beneficial. (See pages 8-32.)

Strategic Goal 2: Insurance

Help the FDIC Maintain the Viability of the Insurance Fund

We did not conduct specific assignments to address this goal area during the reporting period. However, our audit and evaluation work in support of goal 1 fully supports this goal, as does the investigative work highlighted above. In both cases, our work can serve to strengthen the FDIC's supervisory program and help prevent or lessen future failures. Further, the deterrent aspect of investigations and the ordered restitution may help to mitigate an institution's losses and losses to the Deposit Insurance Fund. (See pages 33-34.)

Strategic Goal 3: Consumer Protection

Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy

In support of this goal area, we collaborated with OIG counterparts on an evaluation assignment to examine the progress that the prudential regulators and the Consumer Financial Protection Bureau have made in establishing coordination for the consumer protection responsibilities that the various parties carry out. We also researched the FDIC's efforts to serve the unbanked and underbanked to better understand these activities and offer any observations in that regard to FDIC management.

Our Office of Investigations also supports consumer protection through its work. Investigators continue to pursue cases of misrepresentation of FDIC insurance or affiliation where unscrupulous individuals attempt to convince others to invest in financial products allegedly insured by or endorsed by the FDIC. Our Electronic Crimes Unit also responds to instances where fraudulent emails purportedly affiliated with the FDIC are used to entice consumers to divulge personal information and/or make monetary payments. Working with the Corporation's Chief Information Officer Organization, our investigators seek to protect consumers by dismantling such schemes. In further support of consumer protection, the OIG also continued to respond to a number of inquiries from the public, received both through our Hotline and through other channels. We addressed about 150 such inquiries during the past 6-month period. (See pages 35-37.)

Strategic Goal 4: Receivership Management

Help Ensure that the FDIC Efficiently and Effectively Resolves Failing Banks and Manages Receiverships

We completed an assignment involving the FDIC's process for identifying, securing, and disposing of personally identifiable information found in owned real estate properties that the FDIC possesses as receiver of failed institutions. This work raised questions as to the FDIC's responsibilities for handling such information, and we recommended that the Corporation obtain a legal opinion to shed light on how best to handle such personally identifiable information. At the end of the reporting period, we were conducting two assignments involving receivership management activities. In one, we are examining the FDIC's controls over cash flows from receivership-related taxes. In the other, we are reviewing the risks associated with the early terminations of shared loss agreements.

We would also note that in connection with the FDIC's new resolution authority for systemically important financial institutions, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) requires that the FDIC OIG conduct, supervise, and coordinate audits and investigations of the liquidation of any covered financial company by the Corporation as receiver under Title II of the Act. We continued efforts to ensure we are prepared for such an eventuality.

From an investigative standpoint, our Electronic Crimes Unit continued to support investigative activities related to closed banks by providing computer forensic assistance in ongoing fraud investigations. Of note in that regard during the reporting period was the Electronic Crimes Unit's assistance related to the successful case involving the Park Avenue Bank, New York, New York, where forensic support helped bring about during the reporting period guilty pleas of two key parties in a complex fraud scheme—one a former bank executive and the other a former investment firm executive. (See pages 38-43.)

Strategic Goal 5: Resources Management

Promote Sound Governance and Effective Stewardship and Security of Human, Financial, IT, and Physical Resources

In support of this goal area, during the reporting period, we issued the results of a review requested by the Ranking Member and Minority Members of the Committee on Financial Services, U.S. House of Representatives. This review focused on the FDIC's efforts to provide equal opportunity and achieve senior management diversity. We reported that collectively, the FDIC's commitment, initiatives, and process controls promote a workplace that is free of systemic discrimination, and one that provides equal opportunity for women and minorities. Still, more work is needed to increase representation of female employees, and to a larger extent, Hispanic employees throughout the agency and at the executive manager level. We made nine recommendations to address such concerns. In the records management area, we completed work in connection with the FDIC's controls over the destruction of archived paper records, finding that the FDIC lacked adequate controls to ensure that archived paper records are properly destroyed. We identified a need for the FDIC to conduct a program risk assessment, and strengthen its procedures, implement stronger record inventory controls, and enhance controls for reconciling destruction certificates. We issued the results of our Federal Information Security Management Act of 2002 evaluation of the FDIC's information security program for 2014 and made five recommendations to improve the effectiveness of the Corporation's information security program controls and practices. Finally, we completed work involving the FDIC's input to the governmentwide financial report system. At the end of the reporting period we were continuing efforts related to the FDIC's controls over outside counsel costs associated with professional liability claims and a review of controls over its travel card program, the results of which we will include in our next semiannual report.

We promoted integrity in FDIC internal operations through ongoing OIG Hotline and other referrals and coordination with the FDIC's divisions and offices, including corporate labor and employee relations staff and ethics officials, as warranted. (See pages 44-53.)

Strategic Goal 6: OIG Resources Management

Build and Sustain a High-Quality OIG Staff, Effective Operations, OIG Independence, and Mutually Beneficial Working Relationships

To ensure effective and efficient management of OIG resources, we continued to focus on a number of internal initiatives. We closely monitored staffing and, in the interest of succession planning, took steps to ensure that our office is positioned to handle anticipated attrition through a number of hiring efforts. We tracked OIG spending, particularly costs involved in travel, procurements, and petty cash expenditures. We continued to develop a better system to capture data on our investigative cases and took steps to implement enhanced capabilities of TeamMate for our audit and evaluations staff. On an office-wide level, we continued to re-examine and update our policies and procedures and enhance our records management and disposition activities.

We continued to implement our audit/evaluation quality assurance plan to cover the period October 2013–March 2016 to ensure quality in all audit and attestation engagement work and evaluations, in keeping with government auditing standards and *Quality Standards for Inspection and Evaluation*. We also conducted quality reviews of our field office investigative case files. We oversaw contracts with qualified firms to provide audit and evaluation services to the OIG to supplement our efforts and provide additional subject-matter expertise.

We encouraged individual growth through professional development by supporting individuals in our office involved in professional organizations, pursuing professional certifications, or attending graduate schools of banking. We selected four additional OIG staff to attend those banking schools. We launched our mentoring program for 2015 to further develop a strong cadre of OIG resources. We supported OIG staff members taking FDIC leadership training courses. We also employed interns on a part-time basis to promote the interns' professional development and assist us in our work. Our Workplace Excellence Group conducted a review of the OIG awards program in the interest of enhancing that program.

Our office continued to foster positive stakeholder relationships by way of Acting Inspector General and other OIG executive meetings with senior FDIC executives; coordination with the FDIC Audit Committee; congressional interaction; coordination with financial regulatory OIGs, other members of the Inspector General community, other law enforcement officials, and the U.S. Government Accountability Office. We participated in numerous activities involving the Council of the Inspectors General on Integrity and Efficiency, including meetings of its Audit Committee and Council of Counsels to the Inspectors General. Senior OIG executives were speakers at a number of professional organization and government forums, for example those sponsored by FDIC Divisions, the Federal Financial Institutions Examination Council, Department of Justice, and Federal Audit Executive Council. The OIG participated in corporate diversity events and on the Chairman's Diversity Advisory Council. We continued to use our public inquiry intake system to handle communications with the public and maintained and updated the OIG Web site to respond to the public and provide easily accessible information to stakeholders interested in our office and the results of our work.

In the area of risk management, in connection with SAS 99 and the annual audit of the FDIC's financial statements, we provided our perspectives on the risk of fraud at the FDIC to the U.S. Government Accountability Office. We also provided the OIG's annual assurance statement to the FDIC Chairman regarding our efforts to meet internal control requirements. We monitored the Corporation's progress meeting annual performance goals and attended meetings of various corporate committees to further monitor risks at the Corporation and tailor OIG work accordingly. We shared OIG perspectives on risk areas with senior FDIC leadership. In keeping with the Reports Consolidation Act of 2000, we monitored those areas that we had identified as management and performance challenges facing the Corporation for inclusion in its annual report and conducted and planned assignments in a number of those areas. (See pages 54-63.)

Significant Outcomes October 1, 2014 – March 31, 2015	
Audit and Evaluation Reports Issued	**7**
Nonmonetary Recommendations	**35**
Investigations Opened	**41**
Investigations Closed	**40**
OIG Subpoenas Issued	**16**
Judicial Actions:	
Indictments/Informations	**67**
Convictions	**57**
Arrests	**34**
OIG Investigations Resulted in:	
Fines of	**$ 64,500**
Restitution of	**71,686,855**
Asset Forfeitures of	**26,601,365**
Total	**$ 98,352,720**
Cases Referred to the Department of Justice (U.S. Attorney)	**38**
Proposed Legislation and Regulations Reviewed	**8**
Responses to Requests Under the Freedom of Information/Privacy Acts	**7**

The OIG Will Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly

The Corporation's supervision program promotes the safety and soundness of FDIC-supervised insured depository institutions. The FDIC is the primary federal regulator for approximately 4,140 FDIC-insured, state-chartered institutions that are not members of the Board of Governors of the Federal Reserve System (FRB)—generally referred to as "state non-member" institutions. As insurer, the Corporation also has back-up examination authority to protect the interests of the Deposit Insurance Fund (DIF) for 2,370 national banks, state-chartered banks that are members of the FRB, and savings associations regulated by the Office of the Comptroller of the Currency.

The examination of the institutions that it regulates is a core FDIC function. Through this process, the FDIC assesses the adequacy of management and internal control systems to identify, measure, monitor, and control risks, and bank examiners judge the safety and soundness of a bank's operations. The examination program employs risk-focused supervision for banks. According to examination policy, the objective of a risk-focused examination is to effectively evaluate the safety and soundness of the bank, including the assessment of risk management systems, financial condition, and compliance with applicable laws and regulations, while focusing resources on the bank's highest risks. One such risk receiving increased supervisory attention is the risk of cyberattacks that can cause serious harm to financial institutions and their technology service providers. Another important aspect of the FDIC's overall responsibility and authority to examine banks for safety and soundness relates to compliance with the Bank Secrecy Act, which requires financial institutions to keep records and file reports on certain financial transactions. An institution's level of risk for potential terrorist financing and money laundering determines the necessary scope of a Bank Secrecy Act examination.

Prior to passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), in the event of an insured depository institution failure, the Federal Deposit Insurance (FDI) Act required the appropriate regulatory OIG to perform a review when the 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 FRB 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, the OIG will conduct and report on material loss reviews and in-depth reviews of failed FDIC-supervised institutions, as warranted, and continues to review all failures of FDIC-supervised institutions for any unusual circumstances.

The passage of the Dodd-Frank Act brought about significant organizational changes to the FDIC's supervision program. In April 2013, the monitoring (Oversight and Risk Analytics Branches) function for systemically important financial institutions within the Office of Complex Financial Institutions (OCFI) was transferred to the Division of Risk Management Supervision (RMS) and renamed as the Complex Financial Institutions Group (RMS-CFI Group). The institutional knowledge and analysis associated with the RMS-CFI Group is relevant to OCFI's 165(d) plan reviews, orderly liquidation, and international functions, and collaboration across OCFI and the RMS-CFI Group is on-going. The RMS-CFI Group is primarily responsible for monitoring risk within and across large, complex financial companies for back-up supervisory and resolution readiness purposes.

The OIG's audits and evaluations address various aspects of the Corporation's supervision and examination activities, and, through their investigations of financial institution fraud, the OIG's investigators also play a critical role in helping to ensure the nation's banks operate safely and soundly. Because fraud is both purposeful and hard to detect, it can significantly raise the cost of a bank failure, and examiners must be alert to the possibility of fraudulent activity in financial institutions.

The OIG's Office of Investigations works closely with FDIC management in RMS, the Division of Resolutions and Receiverships (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. 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 Anti-Money Laundering Section to address areas of concern, and we communicate regularly with the Department of Justice's Asset Forfeiture and Money Laundering Section. Our current inventory of Bank Secrecy Act/anti-money laundering cases includes four cases.

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 report working groups. Most recently, the OIG has expanded its involvement in several cyber security-related working groups, namely the National Cyber Investigative Joint Task Force and the FBI's Washington Field Office Cyber Task Force. Additionally, when possible, the OIG engages in industry and other professional outreach efforts to keep financial institutions and others informed of fraud-related issues and to educate them on the role of the OIG in combating financial institution fraud.

To assist the FDIC to ensure the nation's banks operate safely and soundly, the OIG's focus is as follows:

- Help ensure the effectiveness and efficiency of the FDIC's supervision program.
- Investigate and assist in prosecuting Bank Secrecy Act violations, money laundering, terrorist financing, fraud, and other financial crimes in FDIC-insured institutions.

OIG Work in Support of Goal 1

In support of this overarching goal of helping ensure the safety and soundness of the nation's banks, we issued the results of a comprehensive review of the FDIC's supervisory approach to cyberattack risks. We also completed an in-depth review during the reporting period—that of the failure of Vantage Point Bank, Horsham, Pennsylvania. As reported in our last semiannual report, we continued conducting our on-going risk assessment of the FDIC's activities related to implementation of the Dodd-Frank Act.

Our office also continued the legislatively mandated review of all failed FDIC-regulated 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. We completed 10 failed bank reviews during the reporting period, and our failed bank review activity is presented in Appendix II.

From an investigative perspective, in support of ensuring the safety and soundness of the nation's banks, we have pursued cases involving fraud in both open and closed institutions. Results of such selected cases are also described below. Importantly, our investigative results would not be possible without the collaboration and assistance of our colleagues at the FDIC and our law enforcement partners throughout the country.

Ongoing Dodd-Frank Act Risk Assessment and Monitoring Effort

The OIG is continuing an ongoing 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 is to understand and analyze operational and political issues and emerging risks impacting the FDIC, the financial community, and internal OIG operations and plans. This continuous and focused risk assessment and monitoring enhances our more traditional, periodic OIG risk assessment and planning efforts and assists with the OIG's internal preparation efforts in the event a systemically important financial institution should fail. The assessment and monitoring is intended to provide an informal, efficient means of making FDIC and OIG management aware of issues and risks warranting attention—it is not being conducted as an audit or evaluation.

During the reporting period, we continued to observe the FDIC's Complex Financial Institutions Coordination Group meetings, monitored Dodd-Frank Act issues and media coverage, created a framework through which we can view and communicate Dodd-Frank Act-related risks, and arranged to brief senior FDIC leadership to share our perspectives and hear their views on areas where the OIG can add the most value going forward.

In the coming weeks, we anticipate communicating to FDIC management periodic summaries of any issues or risks for management consideration. We are also identifying specific areas where the OIG may conduct additional work.

The FDIC's Supervisory Approach to Cyberattack Risks Can Be Strengthened

Information is one of a financial institution's (FI) most important assets. Protection of information is critical to establishing and maintaining trust between the FI and its customers, complying with laws and regulations, and protecting the FI's reputation. Most FIs rely heavily on information technology (IT) systems, external technology service providers (TSPs), and Internet-connected applications to provide or enable key banking functions. The importance of ensuring information security has grown and has become a vital component of operations as FIs and TSPs face growing challenges from cyberattacks.

A cyberattack is a deliberate exploitation of computer systems or networks. Cyberattacks use malicious code to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

In connection with cyber risks, the FDIC conducts IT examinations of FDIC-supervised FIs and TSPs for compliance with provisions in the FDI Act and the 1999 Gramm-Leach-Bliley Act. The federal banking agencies issued implementing *Interagency Guidelines Establishing Information Security Standards* (Interagency Guidelines) in 2001. In 2005, the FDIC developed the Information Technology—Risk Management Program (IT-RMP), based largely on the Interagency Guidelines, as a risk-based approach for conducting IT examinations at FDIC-supervised FIs. The FDIC generally conducts IT examinations of FIs in conjunction with risk management examinations. The FDIC also uses work programs developed by the Federal Financial Institutions Examination Council (FFIEC) to conduct IT examinations of TSPs. The regulators perform comprehensive joint examinations of the largest TSPs and rotate examinations of mid-size TSPs.

In February 2013, President Obama released Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, which established policy to enhance the security and resilience of the nation's critical infrastructure and called for the development of a risk-based cybersecurity framework and a program for its voluntary adoption. The National Institute of Standards and Technology released the *Framework for Improving Critical Infrastructure Cybersecurity* in February 2014 to provide a blueprint that firms of all sizes can use to evaluate, maintain, and improve the resiliency of their computer systems.

Given the risks that cyberattacks pose to FIs and TSPs, we conducted an evaluation to assess the FDIC's efforts to: ensure that FI/TSPs are prepared to protect against, detect, respond to, and recover from cyberattacks; provide sufficient and qualified resources to examine and monitor FIs and TSPs; and promote information sharing about incidents to appropriate authorities.

Our report, issued on March 18, 2015, points out that the FDIC's supervisory approach to cyberattack risks involves conducting IT examinations at FDIC-supervised FIs and their TSPs; staffing IT examinations with sufficient, technically qualified staff; sharing information about incidents and cyber risks with regulators and authorities; and providing guidance to institutions. The FDIC's IT examination program plays an important role in protecting the nation's financial services infrastructure and ensuring that FIs and TSPs are prepared for cyberattacks. We concluded that the FDIC could increase the level of assurance that FIs and TSPs are adequately prepared by taking the following actions:

- Updating and expanding IT examination procedures,
- Providing consistency and transparency to IT examination scope and procedures performed,
- Ensuring that examiners consistently conclude on FI/TSP program level controls and consider the scope of vendors' third-party reviews,
- Completing efforts to estimate examiner resource and competency needs and ensuring those involved in reviewing IT examination reports receive sufficient and current training, and
- Continuing to enhance information sharing associated with cyber risks.

More specifically, our report notes that in 2013, the FDIC conducted 2,323 IT examinations at FIs and TSPs. RMS periodically conducts IT examinations to assess FI/TSPs' information security programs and compliance with the Interagency Guidelines. In that regard, our evaluation showed that:

The OIG's Information Security Manager discusses cyber risks at OIG All-Hands Conference.

- The FDIC and FFIEC IT examination work programs focus on security controls at a broad program level that, if operating effectively, help institutions protect against and respond to cyberattacks. The program level controls include risk assessment, information security, audit, business continuity, and vendor management. However, the work programs do not explicitly address cyberattack risk, could be updated and strengthened, and could better specify desired characteristics for key program-level controls. The FFIEC has an ongoing initiative to update its IT examination guidance to align with changing cybersecurity risks.

  Examiners review prior examination information and consider the technology profile of the FI in planning the scope of the examination. In addition, the IT-RMP is designed for examiners to rely, in part, on FI management attestations regarding the extent to which IT risks are being managed and controlled. Examiners focus their efforts on management-identified weaknesses and may confirm selected safeguards described by management as adequate. Examiners raised concerns about the value of FI management attestations, including whether the design of the attestation questionnaire provides meaningful information for scoping the examination.
- Examination reports routinely included a statement attesting to FI/TSPs' compliance with the Interagency Guidelines and frequently identified concerns or recommended improvements to information security programs. We determined that examiners frequently concluded on the adequacy of risk assessment and audit programs, but examiners were far less likely to have documented their review and/or provided a clear statement of adequacy on intrusion detection programs and incident response plans. Because examiners have wide discretion in conducting and documenting IT examination work and are only required to document examination findings and recommendations, we could not always tell what procedures examiners performed to reach their conclusions.
- Examiner comments and our own review of examination working papers identified program weaknesses at a number of the FIs we sampled. For example, we noted variation in the quality and depth of FI risk assessments and other IT security program elements. With respect to vendor management, although FIs and the IT RMP rely on periodic third-party reviews and audits of vendors' IT controls and risk management practices, we observed that vendors frequently obtained third-party reviews that provided lower levels of assurance. These reviews focused on internal control over financial reporting—versus reviews that address controls relevant to security, availability, processing integrity, confidentiality, and privacy.

As for our objective involving FDIC resources in the IT examination area, the FDIC faces challenges in determining permanent resource needs. The number of IT examination staff has increased, but mostly in non-commissioned, term IT examination analyst positions. The FDIC's future resource needs and competencies will depend largely on how the FDIC/FFIEC changes its IT examination approach.

With respect to training, we reported that opportunities exist to increase regional management IT training. The FDIC has training programs for developing IT examination staff that include mandatory and discretionary courses and on-the-job training experiences. While most IT examination staff have received IT training, many regional supervisors such as Assistant Regional Directors and Case Managers have received limited IT examination training.

We also pointed out that the FDIC could better ensure that examination teams possess necessary qualifications to review complex institutions. For example, non-commissioned IT examination analysts sometimes examined complex FIs under the supervision of a commissioned examiner who was not an IT specialist. Further, IT subject matter experts sometimes served as the examiner-in-charge on complex IT examinations before they had completed required IT on-the-job courses.

Regarding information sharing related to cyberattacks, the FDIC has processes for receiving cyber incident information and various initiatives to help promote information sharing about cyberattack incidents to FIs, the financial sector, and other regulators and authorities. The FDIC receives cybersecurity information through FI security incident reports and Suspicious Activity Reports filed with the Financial Crimes Enforcement Network. We reported that the FDIC participates in a number of interagency and financial sector councils and committees and would soon be approved to begin receiving classified intelligence information on cybersecurity incidents.

The FDIC periodically issues information security-related guidance to FIs on areas such as new regulations and policies. The frequency of FDIC-issued IT guidance increased markedly in 2014, and the FDIC's practice of issuing notices about specific industry cyber threats has evolved. The FDIC has also held webinars, issued technical assistance videos, and discussed cybersecurity issues with banking industry representatives. In our view, the FDIC could enhance information sharing activities by improving the categorization of specific types of cyberattacks in security incident reports and reaching agreements with other regulators to share security incident information.

The FDIC and the FFIEC have ongoing initiatives to update programs for examining FIs and TSPs. Accordingly, we framed the recommendations in our report to complement RMS' efforts associated with updating examination and institution guidance, addressing resource and training challenges, and enhancing information collection and sharing initiatives.

In responding to our report, the Director of RMS concurred with the report's nine recommendations and noted that RMS had started project plans for several of the recommendations. The response outlined corrective actions that were responsive to our recommendations. RMS established planned completion dates for corrective actions throughout 2015 and 2016 and expects to have all actions completed by the end of 2016.

In-Depth Review of the Failure of Vantage Point Bank, Horsham, Pennsylvania, Identifies Opportunities to Enhance Supervision of De Novo Banks

On February 28, 2014, the Pennsylvania Department of Banking and Securities (PDBS) closed Vantage Point Bank (VPB) and the FDIC was appointed receiver. As of September 30, 2014, the estimated loss of VPB's failure was approximately $11 million. Although the loss estimate does not meet the material loss review threshold, the Director of RMS requested that we conduct an in-depth review because VPB's failure involved unusual circumstances. Specifically, the bank engaged in material changes to its business plan during its de novo period without regulatory approval. Our in-depth review determined the causes of VPB's failure and resulting loss to the DIF and evaluated 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. The scope of our work included an emphasis on VPB's deviation from its business plan and the FDIC's supervisory response to the associated risks.

VPB was a state-chartered nonmember bank that opened on December 26, 2007. The bank's revenues consisted of two principal sources: interest revenue from traditional banking services and non-interest revenue from financial services and mortgage banking activities. VPB's traditional banking services involved generating income from the spread between the interest paid on liabilities (e.g., deposits) and collected on earning assets (e.g., loans). The bank's financial services involved selling financial advisory products, non-bank investments, and insurance to generate fee income. VPB's mortgage banking activities initially involved the bank acting as a broker to assist applicants in obtaining residential mortgage loans from other lenders. VPB subsequently expanded its mortgage banking operation in 2011 by establishing a number of limited-purpose loan production offices to originate, book, and sell residential mortgage loans to third-party investors for a fee. With the exception of the mortgage banking operation (which originated loans in various parts of the country), VPB's primary market area was the greater Philadelphia region. At the time of its closure, VPB operated one office in Horsham, Pennsylvania, which is located about 20 miles north of downtown Philadelphia.

We reported that VPB failed primarily because its Board of Directors (Board) and management did not effectively manage the risks associated with the bank's rapid expansion of its mortgage banking operation. After 3 years of operation, VPB had not achieved a pre-tax profit on operations. High overhead expenses and lower-than expected interest revenue from traditional banking services contributed to the bank's recurring pre-tax operating losses. In addition, VPB's capital positon was less than satisfactory, and the bank's management had limited success in raising new capital due to ongoing adverse economic conditions.

In an effort to improve its earnings, VPB embarked on a rapid expansion of its mortgage banking operation beginning in mid-2011. At that time, historically low interest rates were generating considerable demand for mortgage loans and refinancing. The FDIC determined that VPB's expansion of its mortgage banking operation represented a material deviation from the business plan approved in the bank's Order Granting Deposit Insurance (referred to herein as the "original business plan"), which called for developing mortgage banking expertise in a conservative manner. During the second half of 2011, VPB grew from 46 to 158 employees and opened a number of loan production offices. VPB continued to expand its mortgage banking operation throughout 2012, and by the end of that year, the bank had 238 employees and 14 loan production offices in seven states.

Although the expansion of the mortgage banking operation generated significant revenue, VPB continued to generate pre-tax operating losses due in large part to higher-than-projected overhead costs associated with the loan production offices. In addition, VPB did not implement appropriate controls over its expanded mortgage banking operation. In mid-2013, mortgage rates increased, and demand for mortgage loans and refinancing declined precipitously. As a result, VPB closed all of its loan production offices and terminated the majority of its employees. The costs associated with unwinding the mortgage banking operation, together with financial reporting adjustments made in December 2013, contributed to VPB reporting a $3.8 million loss for calendar year 2013. The loss materially impaired VPB's capital position. The PDBS closed VPB on February 28, 2014 because the bank did not have sufficient capital to continue operations and had no viable means of raising additional capital.

With respect to the FDIC's supervision of the bank, in coordination with the PDBS, the FDIC provided ongoing supervisory oversight of VPB through regular on-site examinations, visitations, and various offsite monitoring activities. Examiners identified risks in VPB's operations and brought these risks to the attention of VPB's Board and management through examination reports, letters summarizing visitation results, correspondence, and informal and formal enforcement actions. Such risks included the bank's less than satisfactory earnings and capital, weak business planning practices, and rapid expansion into mortgage banking without adequate risk management controls.

As described in the report, the FDIC's approach to monitoring VPB for compliance with the original business plan was consistent with supervisory guidance for the first 3 years of the bank's operation. However, monitoring in subsequent years was generally not adequate. In addition, the FDIC should have taken stronger supervisory action during the April 2012 examination when examiners confirmed that VPB had materially deviated from its original business plan without obtaining prior FDIC approval to do so. More effective monitoring and stronger supervisory action would have been consistent with supervisory guidance for newly insured banks and may have prompted VPB to better control the expansion of its mortgage banking operation, mitigating the losses incurred by the bank and, to some extent, the DIF. We also noted that enforcement action information related to VPB had not been recorded in the FDIC's automated system of record as prescribed by FDIC policy. With respect to Prompt Corrective Action, we determined that the FDIC implemented supervisory actions that were generally consistent with relevant provisions of Section 38.

Our report also noted that supervisory guidance issued to newly insured banks did not describe the factors to be considered when determining whether a change or deviation in a business plan was major or material. Clarifying existing guidance would help to ensure prompt and full disclosure of major changes and material deviations in bank business plans and better enable the FDIC to address the associated risks. It would also provide the FDIC with a stronger foundation on which to take supervisory action, when needed.

We made three recommendations intended to improve the effectiveness of the FDIC's supervision of newly insured institutions, such as VPB. In responding to our report, the FDIC concurred with the recommendations.

OIG Investigations Address Financial Institution Fraud

As mentioned previously, the OIG's Office of Investigations' work focuses largely on fraud that occurs at or impacts financial institutions. The perpetrators of such crimes can be those very individuals entrusted with governance responsibilities at the institutions—directors and bank officers. In other cases, individuals providing professional services to the banks, others working inside the bank, and customers themselves are principals in fraudulent schemes.

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, embezzlement, and mortgage fraud. Many 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, attorneys, and other individuals involved in residential and commercial lending activities were also implicated in a number of our cases. These cases are 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 contributes to ensuring the continued safety and soundness of the nation's banks.

Former United Commercial Bank/UCBH Holdings, Inc. Chief Operating Officer and Chief Credit Officer Convicted Following a 6-Week Trial

On March 25, 2015, following a 6-week trial, a jury found the former chief operating officer (COO) and chief credit officer (CCO) of United Commercial Bank (UCB) guilty of conspiring with others within the bank to falsify key bank records as part of a scheme to conceal millions of dollars in losses and falsely inflate the bank's financial statements. Among the records falsified were those filed with the Securities and Exchange Commission and the FDIC related to the third and fourth quarters of 2008 describing UCB's allowance for loan losses. Also falsified were documents relating to UCB's quarterly and year-end earnings per share as announced by the bank to the investing public. The former COO/CCO was convicted of one count of conspiracy to commit securities fraud; one count of securities fraud; one count of falsifying corporate books and records; one count of false statements to accountants; one count of circumventing internal accounting controls; one count of conspiracy to commit false bank entries, reports, and transactions; and one count of false bank entries, reports, and transactions.

On November 6, 2009, UCB failed and the FDIC was appointed receiver. With over $10.9 billion in assets, UCB's failure was the ninth largest failure since 2007 of a bank insured by the DIF. Losses to the DIF are estimated at over $677 million.

According to evidence presented at trial, the former COO/CCO conspired with others and deceived UCB's auditors by manipulating the bank's books and records in a manner that misrepresented and concealed the bank's true financial condition and performance and caused the bank to issue materially false and misleading financial statements for the third quarter of 2008 (10Q and Call Report), year-end 2008 (10K and Call Report), and first quarter of 2009 (Call Report). The former COO/CCO was responsible for the quarterly loan loss allowance packages, in which the bank formally calculated the loss reserves it was required to recognize as part of its quarterly and annual financial reporting. At the time, he knew the loan loss allowance package, along with the quarterly call reports, 10Q(s), and 10K(s), for the third quarter 2008 and the year-end 2008 were false and misleading.

In all, the former COO/CCO faces a total overall maximum term of 145 years of imprisonment, up to $16,750,700 in fines and assessments, and up to 27 years of supervised release. His actual term of imprisonment, fines, and assessments and term of supervised release will be imposed by the court at a sentencing hearing currently set for June 30, 2015.

Also during the reporting period, on December 9, 2014, UCB's former Chief Financial Officer pleaded guilty to one count of conspiracy to make a materially false and misleading statement to an accountant. Earlier, on October 7, 2014, the bank's Senior Vice President pleaded guilty to charges of conspiracy to commit false bank entries, reports, and transactions related to his preparation of false and misleading reports.

Source: *In May 2009, UCBH Holdings, Inc., made a public announcement that an internal investigation was initiated and its 2008 year-end financial statements could not be relied on. Once the results of the internal investigation were disclosed to the Board of Directors, the Board of Directors reported the results of the internal investigation to the United States Department of Justice.*
Responsible Agencies: *This is a joint investigation with the FDIC OIG, FBI, FRB and the Consumer Financial Protection Bureau OIG, and Special Inspector General for the Troubled Asset Relief Program (SIGTARP).*

Three Perpetrators of $49.6 Million Mortgage Fraud Scheme Sentenced

The final three individuals involved in a $49.6 million mortgage fraud scheme, which was organized and led by a developer, were sentenced on December 4, 2014. The scheme involved Hampton Springs in Cashiers, North Carolina. The developer's ex-wife was sentenced to 14 years in prison, and the other two individuals who acted as recruiters for the scheme were sentenced to 20 years in prison. As noted in our last semiannual report, the developer himself was sentenced to 27 years and 3 months in prison. All four defendants were convicted by a federal jury in Miami, in July 2014, following an 11-day trial.

According to the indictment and evidence at trial, from 2003 to 2008, the developer and his co-defendants conspired to perpetrate a complex $49.6 million mortgage fraud scheme against various FDIC-insured lenders, including Bank of America, Regions Bank, SunTrust Bank, and Wachovia Bank. The developer and his ex-wife used shell companies to acquire ownership and control of a purported residential property development known as Hampton Springs, located in Cashiers, North Carolina. Then, the developer and the other two conspirators recruited numerous straw borrowers to purchase building lots in the development. Several of the straw borrowers testified at the trial. According to their testimony and other evidence, the developer paid the borrowers to obtain lot purchase loans and construction loans for building lots in Hampton Springs. To obtain the loans, the developer, his ex-wife, the two conspirators, and others submitted fraudulent loan applications and related documents to the lenders and the lenders' closing agents.

Among other things, the loan applications and settlement statements for the lot loans contained fraudulent statements that the borrowers had paid earnest money deposits and cash due at the closing. In fact, the deposits and cash-to-close were paid by the developer and his ex-wife, using proceeds from the fraudulent scheme. Further, the two sent fraudulent correspondence to the closing agents, including letters bearing the forged signatures of borrowers, to create the false impression that the deposits and cash due at closing had been supplied by the borrowers from the borrowers' own funds.

The two other conspirators recruited straw borrowers for the fraud scheme and submitted fraudulent loan applications to the lenders. Further, the two caused their private companies to be disclosed as the employers of straw borrowers whose actual employment was inconsistent with the inflated income stated on their loan applications. Then, when they were contacted by the lenders, the conspirators provided fraudulent verifications of employment for those borrowers.

Three other defendants involved in this fraud, including the developer's personal assistant, a loan officer at SunTrust Mortgage, and an individual who posed as a tax accountant, had earlier pleaded guilty to the charged conspiracy and agreed to assist the United States. The personal assistant aided the developer and his ex-wife with the misappropriation of loan proceeds and the transmission of fraudulent correspondence to the lenders and the closing agents. The loan officer sponsored fraudulent loan applications for lots in Hampton Springs, including fraudulent applications for $33 million in construction loans. The self-proclaimed accountant furnished fictitious accountant's letters to the loan officer, in support of fraudulent loan applications submitted to SunTrust Mortgage. The three were sentenced earlier in September 2014. The assistant was sentenced to 40 months in prison, the loan officer was sentenced to 64 months in prison, and the individual claiming to be an accountant was sentenced to 30 months in prison.

Source: *U.S. Attorney's Office, Miami Mortgage Fraud Task Force.*
Responsible Agencies: *This is a joint investigation with the FBI. The case is being prosecuted by the U.S. Attorney's Office for the Southern District of Florida.*

OIG Special Agent presents case involving former bank director who faked his own death.

Former Bank Director Who Faked His Own Death Sentenced to 30 Years in Prison

On October 28, 2014, a former director at Montgomery Bank & Trust (MB&T), Ailey, Georgia, which failed on July 6, 2012, was sentenced to 30 years in federal prison for perpetrating a Ponzi scheme that resulted in millions of dollars of losses to dozens of his investors and led to the collapse of the bank.

According to court filings and evidence presented at the guilty plea and sentencing hearings, the former bank director embezzled over $21 million in capital from MB&T, and lost much of it by investing in risky equity securities and options. To cover up his fraud, the former bank director provided MB&T officials with bogus account statements and other false documents which falsely indicated the bank's capital was safely held in an account at a financial services firm, when in truth, most of the money was gone. A further investigation of his activities revealed that between June 2009 and June 2012, the former director also defrauded approximately 115 individual investors who had invested $51 million in two investment funds he managed. He lost almost all of that money through speculative trading, and to cover up his losses, he posted fake account statements on a secure Web site that fraudulently reflected fictitious assets and fabricated investment returns for each investor.

In mid-June 2012, the former director sent acquaintances "suicide letters" in which he admitted he had defrauded MB&T and his individual investors, and that he planned to kill himself by throwing himself off a high-speed ferry boat after it left Key West, Florida. As a result of the suicide claim, the United States Coast Guard searched but to no avail for his body. Shortly after sending the letters, the former director disappeared. After more than a year of searching for him, he was arrested on December 31, 2013, after he presented a false identification during a routine traffic stop in Brunswick, Georgia.

The former director had been in custody since his arrest on December 31, 2013. In addition to being sentenced to 30 years in prison, he was sentenced to serve a term of 5 years of supervised release. As part of his sentence, he will also be ordered to pay restitution to the victims of his crimes in an amount to be determined at a restitution hearing. In addition, he was ordered to forfeit a total of $51 million, representing the proceeds of his crimes.

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

Former Owner of Sacramento Capitals Tennis Team Sentenced to 20 Years in Prison for Fraud Scheme Exceeding $100 Million in Losses

On November 13, 2014, the former owner of the Sacramento Capitals Tennis Team was sentenced to 20 years in prison for a long-running fraud scheme. In addition to the prison term, he was ordered to forfeit multiple properties, vehicles, business interests, and bank accounts to be used to provide restitution to victims. The total value of the properties, vehicles, business interests, and bank accounts is estimated to be at least $3.5 million.

According to court documents, from 2002 to 2014, the former sports team owner convinced nearly 200 victims, including individuals, corporate entities, and financial institutions, to invest in a number of business opportunities by misrepresenting his own financial worth and that of his companies. Those companies, IMG and Relyaid, were involved in the international manufacture, shipment, and distribution of latex gloves. He falsely claimed that these companies did tens of millions of dollars in business with federal agencies every year, most notably the Department of Veterans Affairs (VA). In 2013, he claimed to have more than $125 million in VA contracts alone. In fact, while he did have a contract with the VA, it was only worth up to $25,000 a year.

Ultimately, the sports team owner obtained well over $230 million from his victims. Contrary to his representations, he used much of the money he obtained to pay himself and his family, make lulling payments to participants in his fraudulent investment schemes, and pay outstanding debts unrelated to his false representations. He had purchased properties in Hawaii, Oregon, and California.

In order to establish his financial credibility, he showed investors his personal and corporate tax returns where he actually reported and paid taxes that falsely overstated his annual personal income and the annual gross receipts and sales for IMG. He used investors' money to pay the overstated tax returns.

Source: *FBI.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, Internal Revenue Service Criminal Investigation Division (IRS CID), VA OIG, and the FBI, Sacramento Division. The case is being prosecuted by the U.S. Attorney's Office for the Eastern District of California.*

Reality Television Show Stars Sentenced

On October 2, 2014, two of the stars of the television show "The Real Housewives of New Jersey" were sentenced to prison terms for committing a string of crimes as part of a long-running financial fraud conspiracy. The wife and her husband were sentenced to 15 months and 41 months in prison, respectively. Both defendants had previously pleaded guilty to several counts of the superseding indictment returned against them in July 2013. They each pleaded guilty to one count of conspiracy to commit mail and wire fraud, one count of bankruptcy fraud by concealment of assets, one count of bankruptcy fraud by false oaths, and one count of bankruptcy fraud by false declarations. The husband also pleaded guilty to one count of failure to file a tax return. The wife was ordered to report to the Bureau of Prisons on January 5, 2015, to begin serving her sentence. Her husband will report to serve his sentence after his wife finishes serving her prison term.

According to documents filed in this case and statements made in court, from September 2001 through September 2008, the couple engaged in a mail and wire fraud conspiracy in which they submitted fraudulent applications and supporting documents to lenders in order to obtain mortgages and other loans. They falsely represented on loan applications and supporting documents that they were employed and/or receiving substantial salaries when they were either not employed or not receiving such salaries.

In September 2001, the wife applied for a $121,500 mortgage loan for which she submitted a loan application falsely claiming she was employed as an executive assistant. She also submitted fake W-2 forms and fake pay stubs purportedly issued by her employer. For a $361,250 mortgage loan that the wife obtained in July 2005, she and her husband prepared a loan application which falsely stated she was employed as a realtor and that she made a monthly salary of $15,000. In fact, she was not employed at the time.

On October 29, 2009, they filed a petition for individual Chapter 7 bankruptcy protection in U.S. Bankruptcy Court in Newark. Over the next few months, they filed several amendments to the bankruptcy petition. As part of the bankruptcy filings, they were required to disclose to the United States Trustee their assets, liabilities, income, and any anticipated increase in income. The couple intentionally concealed businesses they owned, income they received from a rental property, and the wife's true income from the television show "The Real Housewives of New Jersey," Web site sales, and personal and magazine appearances. They concealed their anticipated increase in income from the then-upcoming second season of the show. They also testified falsely under oath in bankruptcy proceedings when questioned about their assets and income.

The husband also admitted that during tax years 2004 through 2008, he received income totaling $996,459 but did not file tax returns for those years. In addition to the prison terms, the two were each sentenced to 2 years of supervised release, and ordered to forfeit $414,588. The husband was fined $10,000 and the wife was fined $8,000. The husband was advised by the court that he faces deportation after serving his sentence. That decision will be made by U.S. Immigrations and Customs Enforcement following completion of his prison sentence.

Source: *This investigation was based on a request for assistance from the U.S. Attorney's Office.*
Responsible Agencies: *This is a joint investigation conducted by the FDIC OIG, IRS CID, and the Newark Office of the U.S. Trustee. The case is being prosecuted by the U.S. Attorney's Office for the District of New Jersey.*

Former Loan Officer Sentenced in Multi-Million Dollar Mortgage Fraud Scheme

A former loan officer at George Mason Mortgage, a subsidiary of Cardinal Bank, McLean, Virginia, was sentenced to 42 months in prison, followed by 3 years of supervised release, for conspiracy to commit bank fraud and related charges arising from a multi-million dollar mortgage fraud scheme. More than $1 million in bank accounts belonging to the former loan officer were seized by law enforcement agents when the charges were first filed.

The former loan officer had been found guilty after a 6-day jury trial on May 7, 2014. According to court documents, she and her co-conspirators were responsible for over $15 million in losses to various lending institutions that purchased fraudulent loans that she originated. She and her co-conspirators from the Manassas, Virginia, real estate firm Vilchez & Associates fraudulently inflated the income and assets of their clients to obtain mortgage loans in amounts that the clients were wholly unqualified for. The former loan officer earned hundreds of thousands of dollars in loan commissions from the fraud, while one of the realtors pocketed millions of dollars in real estate commissions. The realtors' conspiracy targeted hundreds of non-English-speaking members of the Northern Virginia Hispanic community who were not able to read the loan applications and closing documents they were asked to sign. Often the amount of the monthly mortgage payments was unknown or even misrepresented to the borrowers. One of the realtors was arrested in Peru where she had been a fugitive. Her brother, who was also a realtor at the firm, was arrested in Peru in December 2012. Both have been fighting extradition to the United States to face charges.

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

Guilty Pleas in Park Avenue Bank Fraud Case

On December 23, 2014, a Kentucky businessman pleaded guilty to his role in tax crimes that caused more than $50 million in losses to the Internal Revenue Service and a massive fraud that involved the bribery of bank officials, the fraudulent purchase of an insurance company, and the defrauding of insurance and bank regulators. The businessman pleaded guilty to a four-count criminal Information in which he was charged with corruptly endeavoring to obstruct and impede the due administration of the internal revenue laws, aiding and assisting with the preparation and presentation of false and fraudulent tax returns, failing and causing the failure to pay taxes to the Internal Revenue Service, and conspiracy to commit bank bribery, commit fraud on bank regulators and the board and shareholders of a publicly-traded company, and fraudulently purchase an Oklahoma insurance company. The total loss on the case was over $129 million.

According to the Information, plea agreement, and statements made during court proceedings, the businessman controlled numerous entities located throughout the United States. Rather than exercise control of these companies openly, he concealed his control by installing other individuals to oversee the companies' day-to-day functions and to serve as the companies' titular owners, directors, or officers. However, it was the businessman who actually controlled the companies and their finances, using them to orchestrate a number of interrelated fraud schemes. Integral to the success of these schemes was his corrupt relationship with Park Avenue Bank and its executives, the former president and chief executive officer, and senior vice president. The executive director of investments at an investment bank and financial services company headquartered in New York was involved in one of the businessman and the former Park Avenue Bank senior vice president's corrupt schemes.

Also during the reporting period, on February 20, 2015, that former investment firm executive pleaded guilty to a criminal Information in which he was charged with conspiracy to commit wire fraud for his role in a massive scheme to defraud his employer and insurance regulators in connection with the fraudulent purchase of an Oklahoma insurance company. The former investment executive admitted that he deceived his employer to enable the illegal purchase of the insurance company. His conspirators—the businessman and the former bank executives—in effect looted the assets of the company, leaving it unable to pay policyholders, and the investment executive pocketed over $200,000 in commissions on a fraudulent $30 million loan. As part of his plea, he agreed to forfeit $200,000 to the United States and to provide restitution of $10 million to the investment firm.

Source: *RMS.*
Responsible Agencies: *This is a joint investigation conducted by the FDIC OIG, FBI, SIGTARP, Department of Homeland Security Investigations, New York State Department of Financial Services, and IRS CID. The case is being prosecuted by the U.S. Attorney's Office for the Southern District of New York.*

Former Bank President Pleads Guilty

On March 13, 2015, the former president of Premier Community Bank (Premier) of the Emerald Coast, Crestview, Florida, entered a guilty plea to a nine-count indictment. The former president was indicted on October 21, 2014, by a federal grand jury for nine felony counts, which included one count of conspiracy to commit bank fraud and/or mail fraud affecting a financial institution, one count of conspiracy to commit money laundering, four counts of false statements to federally insured institutions, and one count of money laundering. Premier was closed on December 16, 2011.

According to the indictment, the former bank president devised a scheme to defraud and fraudulently obtain money and property from Premier; Bank of America; and Beach Community Bank, Fort Walton Beach, Florida. As a part of the scheme, the former president allegedly orchestrated short sales from Bank of America by causing the submission false documents in real estate closings. The indictment also alleged that the former bank president, through his company MSD Investments, received funds from loans he authorized and approved in his capacity as the president of Premier.

Source: *RMS.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, IRS CID, SIGTARP, and the Okaloosa County Sheriff's Office as part of the Northwest Florida Financial Crimes Task Force. The case is being prosecuted by the U.S. Attorney's Office for the Northern District of Florida.*

Former Loan Officer Pleads Guilty to Embezzlement

On January 29, 2015, a former loan officer at United Bank & Trust Company, Versailles, Kentucky, pleaded guilty to a criminal Information charging him with one count of embezzlement. He was suspected of perpetrating a bank fraud scheme using approximately 30 straw loans issued to friends and members of his family. His scheme was carried out over a period lasting from May 2012 until January 2014, and the proceeds were used to pay gambling debts, service the debt on the false loans, and for personal expenses. In order to make the false loans, the former loan officer listed race horses as collateral, knowing that these race horses did not exist. The scheme was disguised using false documents but collapsed when the bank's internal audit function discovered loans to entities outside the former loan officer's lending area. As a result of the scheme, United Bank & Trust Company suffered losses exceeding $983,000.

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

Business Owner/Former Bank Customer Sentenced

On October 6, 2014, the former President of Schmidt Builder's Supply (Schmidt Builders), owner/member of Blue Jay Properties LLC, and owner of RAKD, LLC was sentenced to serve 57 months in prison to be followed by 3 years of supervised release. He was also ordered to pay restitution in the amount of $6,923,622. On September 11, 2013, the former business owner had pleaded guilty to bank fraud, money laundering, and making false statements to an employee benefit plan.

According to court documents, the business owner was alleged to have obtained a $15.2 million construction loan for the purpose of constructing Quinton Pointe Apartments in Junction City, Kansas. He was required to provide $1,225,000 in collateral. He signed a letter to the lender, University National Bank of Lawrence, Kansas, falsely stating that lumber for the construction of the apartment complex, representing collateral for the loan, was prepaid in full and being held by Schmidt Builders, a company for which he was the chief executive officer. He also instructed employees of Schmidt Builders to create a false invoice in an amount of more than $1.3 million to a company he owned called Blue Jay Properties LLC in order to create the false appearance that Blue Jay Properties had prepaid Schmidt Builders for the lumber.

With regard to another count, Schmidt Builders acquired a $12 million line of credit loan from Kaw Valley National Bank of Topeka and agreed to provide the bank with monthly financial reports. The business owner submitted reports to the bank containing false information about the age of certain accounts receivable and the amount of inventory on hand.

Source: *IRS CID.*
Responsible Agencies: *This is a joint investigation conducted by the FDIC OIG, IRS CID, FRB OIG, and U.S. Department of Labor – Employee Benefits Security Administration. The case is being prosecuted by the U.S. Attorney's Office for the District of Kansas.*

Commercial Loan Borrower Pleads Guilty

On January 14, 2015, a plea agreement was unsealed in which a commercial loan borrower pleaded guilty to a five-count Information through which he was charged with wire and bank fraud, conspiracy to commit wire and bank fraud, conspiracy to make false statements to a bank, and conspiracy to commit money laundering in connection with a scheme to defraud Sonoma Valley Bank, Sonoma, California.

According to the Information, during the period from March 2009 until approximately September 2012, the borrower, working with others, participated in a material scheme to defraud Sonoma Valley Bank and others and to obtain money from the bank and others by means of materially false and fraudulent pretenses, representations, and promises and by omissions and concealment of material facts. Specifically, the borrower assisted in obtaining a $9.47 million loan for an entity called 101 Houseco, LLC, falsely claiming that he controlled the company, but knowing that he was in reality a straw and that 101 Houseco, LLC, was actually controlled by two other conspirators. Those co-conspirators used the proceeds of the loan to purchase from the FDIC the rights to a prior $31.9 million loan on which one of them had defaulted. This allowed the co-conspirator to gain ownership and control of the Park Lane Villas East, a development in Santa Rosa, California, and ultimately to refinance the property at a favorable interest rate through federal government lender Freddie Mac in September 2012.

Source: *FDIC DRR.*
Responsible Agencies: *This is a joint investigation conducted by FDIC OIG, SIGTARP, and Federal Housing Finance Agency OIG. The case is being prosecuted by the U.S. Attorney's Office for the Northern District of California.*

Countrywide Bank Customer Sentenced to 28 Months in Prison for Making False Statements

On January 8, 2015, a former customer of Countrywide Bank, NA , Alexandria, Virginia, was sentenced to serve 28 months in prison to be followed by 60 months of supervised release and was ordered to pay restitution of $376,468. The former customer's sentence also involved a separate scheme in which he defrauded AIG insurance company.

Between December 2005 and April 2006, the former customer applied for and received six mortgage loans and lines of credit from Countrywide Bank that he used for the purchase and refinance of several real properties all located in Kingsburg, California. In his mortgage loan and line of credit applications for the Kingsburg properties, he knowingly and fraudulently used another person's social security number in an effort to influence the approval and funding of the loans. He ultimately defaulted on his payment obligations, and the Kingsburg properties were foreclosed upon, resulting in losses totaling $376,468. In November 2012, the former customer also filed a petition for bankruptcy in the Northern District of California, using the same fraudulent social security number.

Source: *San Joaquin Financial Crimes and SAR Review Task Force, Fresno, California.*
Responsible Agencies: *This is a joint investigation conducted by the FDIC OIG and Social Security Administration OIG. The case is being prosecuted by the U.S. Attorney's Office for the Southern District of Iowa.*

Former President of First National Bank, Davis, Oklahoma, Sentenced for Bank Fraud

On December 3, 2014, the former president of First National Bank, Davis, Oklahoma, was sentenced to serve 24 months in prison to be followed by 2 years of supervised release, and ordered to pay restitution to the FDIC of $14.7 million. The former president had pleaded guilty on February 24, 2014. On October 20, 2014, a bank customer was found guilty of four counts of bank fraud and one count of conspiracy in connection with the former bank president's actions. The jury also found that the bank customer should forfeit $3.2 million in assets as part of any sentence imposed. The bank customer will be sentenced at a later date.

Testimony at the bank customer's trial established that the bank customer and the former bank president committed bank fraud in an attempt to hide from bank examiners large amounts of loans to the bank customer. During a bank examination on February 7, 2011, the Office of the Comptroller of the Currency discovered the loans in question. Those loans caused the bank to be critically undercapitalized, and on March 11, 2011, First National Bank was closed and the FDIC was named receiver of the bank.

Source: *This investigation was initiated based on a referral from DRR and the Office of the Comptroller of the Currency regarding suspected insider abuse and loan fraud committed by the former bank president.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, FBI, and U.S. Department of Agriculture OIG. The case is being prosecuted by the U.S. Attorney's Office for the Eastern District of Oklahoma.*

Businessman and Office Manager Guilty of Bank Fraud

On August 27, 2014, the owner of Shorts Electric and the office manager of Shorts Electric were charged with bank fraud in connection with a scheme to fraudulently obtain funds from Commercial State Bank, Andrews, Texas.

Between June 2012 and March 2014, the two sold fictitious customer invoices to Commercial State Bank through the Business Manager Program. Through this program, Commercial State Bank would purchase Shorts Electric accounts receivable at a discount and transfer the purchase money into the company's business account, thereby allowing Shorts Electric immediate access to operating funds without having to wait for customer invoices to be paid. Not only did the two purposefully "pad" numerous invoices with expenses and charges not actually incurred by the customers, they created completely fictitious customer invoices and submitted them to Commercial State Bank. Ultimately, those invoices were uncollectible because they did not represent money actually owed to Shorts Electric. Losses to Commercial State Bank were estimated at $398,542.

The business owner and the office manager were arrested on September 3, 2014. On November 24, 2014, the office manager pleaded guilty to bank fraud. On February 24, 2015, she was sentenced to serve 41 months in prison, to be followed by 5 years of supervised release, and ordered to pay a special assessment of $100 and restitution of $371,060 (jointly and severally) to Commercial State Bank, Odessa, Texas.

On December 22, 2014, the business owner pleaded guilty to bank fraud, and he is scheduled to be sentenced on May 14, 2015.

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

Former Bank Executive Vice President Pleads Guilty to Making a False Financial Report to the FDIC in Connection with the Failure of Freedom State Bank, Freedom, Oklahoma

On December 15, 2014, the former executive vice president of Freedom State Bank (FSB), Freedom, Oklahoma, pleaded guilty to submitting a falsified report of the financial condition of FSB to the FDIC. His guilty plea came approximately 6 months after the bank's failure on June 27, 2014.

During his plea hearing, the former executive vice president admitted to preparing and submitting a Consolidated Report of Condition and Income (Call Report) to the FDIC falsely stating that the bank possessed nearly $22 million in assets, when he in fact knew that the true amount was substantially less. The former executive vice president was charged on December 4, 2014, with one count of submitting a false statement to the FDIC. In a written plea agreement, he admitted that he was responsible for causing between $1million and $2.5 million in losses to the bank and agreed that he was subject to a sentencing enhancement for substantially jeopardizing the soundness of a financial institution.

When sentenced, he will face up to 5 years in prison, followed by 3 years of supervised release, and a $250,000 fine. He will also be ordered to pay restitution to the FDIC in an amount to be determined by the court.

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

Businessman Sentenced in Multi-Million Dollar Check Kiting Scheme

In late 2012, a number of financial institutions were the victims of a multi-million dollar check kiting scheme perpetrated by a businessman who owned and operated Richmond Wholesale Company, Inc. (Richmond Wholesale), Staten Island, New York. The businessman, using bank accounts at six financial institutions, including Habib American Bank, M&T Bank, and Capital One Bank, wrote checks to himself and Richmond Wholesale from the accounts at one financial institution and deposited the checks into separate Richmond Wholesale accounts at other financial institutions. At the time he wrote the checks, the businessman knew the initial accounts from which the checks were primarily written lacked sufficient funds to cover the checks. Although the checks had not cleared, the financial institutions immediately credited the deposits. To cover the funds of the checks written from the initial accounts, the businessman transferred funds by wire from the deposit accounts to the initial accounts, artificially inflating the balance of the initial accounts.

During the course of the scheme, the businessman withdrew millions of dollars from the inflated bank accounts. On or about November 13, 2012, the financial institutions began to stop making the deposits available immediately, leaving him unable to transfer money to the initial accounts to cover the checks, and the scheme collapsed. Ultimately, the total check float among all the accounts was approximately $84 million, with losses totaling more than $5.2 million.

On December 13, 2012, the businessman was arrested. On May 21, 2013, he pleaded guilty to eight counts of bank fraud. On November 4, 2014, he was sentenced to 4 years of probation, as well as 500 hours of community service per year. He forfeited $5.2 million and must pay $4.8 million in restitution.

Source: *This investigation was initiated based on a request for assistance from the FBI.*
Responsible Agencies: *This is a joint investigation conducted by the FDIC OIG and the FBI. The case is being prosecuted by the U.S. Attorney's Office for the Eastern District of New York.*

Former Branch Manager Sentenced

On October 29, 2014, a former branch manager of Integrity Bank (Integrity), Camp Hill, Pennsylvania, was sentenced to serve 12 months and one day in prison to be followed by 2 years of supervised release. She was also ordered to pay a $1,000 fine.

The former branch manager stole funds by making four unauthorized withdrawals between May 14, 2012, and March 26, 2013, from the time deposit account of an elderly Integrity Bank customer. The funds were converted into cashier's checks and then used for the branch manager's personal benefit, including the payment of taxes and funding an investment account. The total amount stolen was $125,815. When confronted by bank management, the branch manager admitted to wrongdoing and returned the money to the elderly customer's account.

Source: *This investigation was initiated based on a referral from the FDIC Legal Division.*
Responsible Agencies: *This is a joint investigation conducted by the FDIC OIG, FRB OIG, and the FBI. The case is being prosecuted by the U.S. Attorney's Office for the Middle District of Pennsylvania.*

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 geographic areas: Alabama, Arizona, Arkansas, California, Colorado, District of Columbia, Florida, Georgia, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, 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/New York-New Jersey Health Care Financing Administration Task Force; the Philadelphia Financial Exploitation Prevention Task Force; the Northern Virginia Real Estate Fraud Initiative Working Group, Manassas, Virginia; Maryland Mortgage Fraud Task Force; the New England Mortgage Fraud Working Group; Boston Massachusetts SAR Review Meetings; Philadelphia Mortgage Fraud Working Group.
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; 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.
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 Northern District of Mississippi; SAR Review Team for Southern District of Mississippi; Oklahoma City Financial Crimes SAR Review Working Group; Austin SAR Review Working Group.
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.

The OIG Will Help the FDIC Maintain the Viability of the Insurance Fund

Federal deposit insurance remains a fundamental part of the FDIC's commitment to maintain stability and public confidence in the nation's financial system. The FDIC insures bank and savings association deposits. As insurer, the FDIC continually evaluates and monitors changes in the economy, financial markets, and the banking system, to ensure that the DIF remains viable to protect all insured depositors. To maintain sufficient DIF balances, the FDIC collects risk-based insurance premiums from insured institutions and invests deposit insurance funds.

In the aftermath of the financial crisis, FDIC-insured institutions continue to make gradual but steady progress. Continuing to replenish the DIF in a post-crisis environment is a critical activity for the FDIC. The DIF balance had dropped below negative $20 billion during the worst time of the crisis. During the fourth quarter of 2014, the DIF balance increased by $8.5 billion–from $54.3 billion at September 30, 2014 to an all-time high of $62.8 billion. That quarterly increase was primarily due to $2.0 billion of assessment revenue and a negative $6.8 billion provision for insurance losses, partially offset by $408 million of operating expenses. The DIF balance as of March 31, 2015 was $65.3 billion.

While the fund is considerably stronger than it has been, the FDIC must continue to monitor the emerging risks that can threaten fund solvency in the interest of continuing to provide the insurance coverage that depositors have come to rely upon. In that regard, the FDIC will need to continue to disseminate data and analysis on issues and risks affecting the financial services industry to bankers, supervisors, the public, and other stakeholders on an ongoing basis.

The FDIC, in cooperation with the other primary federal regulators, proactively identifies and evaluates the risk and financial condition of every insured depository institution. The FDIC also identifies broader economic and financial risk factors that affect all insured institutions. The FDIC is committed to providing accurate and timely bank data related to the financial condition of the banking industry. Industry-wide trends and risks are communicated to the financial industry, its supervisors, and policymakers through a variety of regularly produced publications and ad hoc reports. Risk-management activities include approving the entry of new institutions into the deposit insurance system, off-site risk analysis, assessment of risk-based premiums, and special insurance examinations and enforcement actions. In light of increasing globalization and the interdependence of financial and economic systems, the FDIC also supports the development and maintenance of effective deposit insurance and banking systems world-wide.

Over recent years, the consolidation of the banking industry resulted in fewer and fewer financial institutions controlling an ever-expanding percentage of the nation's financial assets. The FDIC has taken a number of measures to strengthen its oversight of the risks to the insurance fund posed by the largest institutions, and its key programs have included the Large Insured Depository Institution Program, Dedicated Examiner Program, Shared National Credit Program, and off-site monitoring systems.

Importantly, with respect to the largest institutions, Title II of the Dodd-Frank Act was intended to help address the notion of "Too Big to Fail." The largest institutions will be subjected to the same type of market discipline facing smaller institutions. Title II provides the FDIC authority to wind down systemically important bank holding companies and non-bank financial companies as a companion to the FDIC's authority to resolve insured depository institutions.

To help the FDIC maintain the viability of the DIF, the OIG's focus in this goal area is as follows:

- Evaluate corporate programs to identify and manage risks in the banking industry that can cause losses to the fund.

OIG Work in Support of Goal 2

We did not complete work specifically related to this goal area during the reporting period. We would note, however, that the OIG's work referenced in goal 1 fully supports the goal of helping the FDIC maintain the viability of the DIF. Even now, for example, although the number of institution failures has declined dramatically, each institution for which we conduct a material loss review, in-depth review, or a failed bank review, by definition, causes a loss to the DIF. The OIG's failed bank work is designed to help prevent such losses in the future. Work that strengthens the FDIC in its supervisory role also helps ensure the viability of the DIF. Similarly, investigative activity described in goal 1 fully supports the strategic goal of helping to maintain the viability of the DIF. The OIG's efforts often lead to successful prosecutions of fraud in financial institutions, with restitution paid back to the FDIC when possible, and/or deterrence of fraud that can cause losses to the fund.

The OIG Will Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy

The FDIC serves a number of key roles in the financial system and among the most important is its work in ensuring that banks serve their communities and treat consumers fairly. The FDIC carries out its role by providing consumers with access to information about their rights and disclosures that are required by federal laws and regulations and examining the banks where the FDIC is the primary federal regulator to determine the institutions' compliance with laws and regulations governing consumer protection, fair lending, and community investment. As a means of remaining responsive to consumers, the FDIC's Consumer Response Center investigates consumer complaints about FDIC-supervised institutions and responds to consumer inquiries about consumer laws and regulations and banking practices.

The FDIC has implemented changes related to the Dodd-Frank Act that have direct bearing on consumer protections. The Dodd-Frank Act established the Consumer Financial Protection Bureau within the FRB and transferred to this bureau the FDIC's examination and enforcement responsibilities over most federal consumer financial laws for insured depository institutions with over $10 billion in assets and their insured depository institution affiliates. Also during early 2011, the FDIC established a new Division of Depositor and Consumer Protection, responsible for the Corporation's compliance examination and enforcement program as well as the depositor protection and consumer and community affairs activities that support that program.

Historically, turmoil in the credit and mortgage markets has presented regulators, policymakers, and the financial services industry with serious challenges. The FDIC has been committed to working with the Congress and others to ensure that the banking system remains sound and that the broader financial system is positioned to meet the credit needs of the economy, especially the needs of creditworthy households that may experience distress. The FDIC has promoted expanded opportunities for the underserved banking population in the United States to enter and better understand the financial mainstream. Economic inclusion continues to be a priority for the FDIC, and a key focus is serving the unbanked and underbanked in our country.

Consumers today are also concerned about data security and financial privacy. Banks are increasingly using third-party servicers to provide support for core information and transaction processing functions. The FDIC seeks to ensure that financial institutions protect the privacy and security of information about customers under applicable U.S. laws and regulations.

Every year fraud schemers attempt to rob consumers and financial institutions of millions of dollars. The OIG's Office of Investigations can identify, target, disrupt, and dismantle criminal organizations and individual operations engaged in fraud schemes that target our financial institutions or that prey on the banking public. OIG investigations have identified multiple schemes that defraud consumers, and the OIG continues efforts to halt such activity.

The misuse of the FDIC's name or logo has been identified as a common scheme to defraud consumers. Such misrepresentations have led unsuspecting individuals to invest on the strength of FDIC insurance while misleading them as to the true nature of the investment products being offered. These consumers have lost millions of dollars in the schemes. Investigative work related to such fraudulent schemes is ongoing and will continue. With the help of sophisticated technology, the OIG continues to work with FDIC divisions and other federal agencies to help with the detection of new fraud patterns and combat existing fraud. Coordinating closely with the Corporation and the various U.S. Attorneys' Offices, the OIG helps to sustain public confidence in federal deposit insurance and goodwill within financial institutions.

To assist the FDIC to protect consumer rights and ensure customer data security and privacy, the OIG's focus in this goal area is as follows:

- Contribute to the effectiveness of the Corporation's efforts to ensure compliance with consumer protections at FDIC-supervised institutions.
- Support corporate efforts to promote fairness and inclusion in the delivery of products and services to consumers and communities.
- Conduct investigations of fraudulent representations of FDIC affiliation or insurance that negatively impact public confidence in the banking system.

OIG Work in Support of Goal 3

During the reporting period, we conducted research on the FDIC's activities related to unbanked and underbanked households and intend to communicate our observations to the Division of Depositor and Consumer Protection. We continued to coordinate with financial regulatory OIG counterparts in an assignment to examine the progress that the prudential regulators and the Consumer Financial Protection Bureau have made in establishing coordination for the consumer protection responsibilities that the various parties carry out. We also continued efforts to protect consumers by way of our Electronic Crimes Unit's involvement in investigating email schemes that prey on the public.

Further, in response to consumer inquiries received through our public inquiry system, the OIG has referred a number of matters either to the FDIC's Consumer Response Center or to other entities offering consumer assistance on banking-related topics. Our efforts in some of these areas are discussed below.

Electronic Crimes Unit Responds to Email and Other Schemes

The Electronic Crimes Unit (ECU) continues to work with agency personnel and an FDIC contractor to identify and mitigate the effects of phishing attacks through emails claiming to be from the FDIC. These schemes persist and seek to elicit personally identifiable and/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.

In prior semiannual reports, we noted that the ECU learned that over 20 individuals in foreign countries were contacted by individuals claiming to be from the FDIC's DRR. The foreign individuals were fraudulently informed that the FDIC was going to reimburse them for stock losses after they paid fees to release the funds. The ECU informed the foreign individuals that these types of contacts are fraudulent. We noted that other government agencies may have been victimized by the same group of scammers. During the reporting period, the ECU continued to coordinate with the FBI, Treasury Inspector General for Tax Administration, and the Internal Revenue Service on this multi-agency case.

OIG's Inquiry Intake System Responds to Public Concerns and Questions

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 makes every effort to acknowledge each inquiry and be responsive to the concerns raised. We coordinate closely with others in the Corporation through the FDIC's Public Service Provider working group and appreciate their assistance. We handle those matters within the OIG's jurisdiction and refer inquiries, as appropriate, to other FDIC offices and units or to external organizations. During the past 6-month period, we addressed approximately 150 such matters.

We have responded to a continuing stream of inquiries from individuals who have received phishing emails asking us to confirm their authenticity. In these cases, we inform the recipients that the emails are fraudulent and advise them not to reply in any way.

The OIG Will Help Ensure that the FDIC Efficiently and Effectively Resolves Failing Banks and Manages Receiverships

One of the FDIC's most important roles is acting as the receiver or liquidating agent for failed FDIC-insured institutions. The FDIC's responsibilities include planning and efficiently handling the resolutions of failing FDIC-insured institutions and providing prompt, responsive, and efficient administration of failing and failed financial institutions in order to maintain confidence and stability in our financial system.

As part of the resolution process, the FDIC values a failing federally insured depository institution, markets it, solicits and accepts bids for the sale of the institution, considers the least costly resolution method, determines which bid to accept, and works with the acquiring institution through the closing process. The receivership process involves performing the closing function at the failed bank; liquidating any remaining assets; and distributing any proceeds to the FDIC, the bank customers, general creditors, and those with approved claims.

The FDIC's resolution and receivership activities have presented a substantial and challenging workload for the Corporation in recent years. Banks over the past years have become more complex, and the industry has consolidated into larger organizations. During the recent financial crisis, in particular, the FDIC was called upon to handle failing institutions with significantly larger numbers of insured deposits than it has dealt with in the past.

Adding to the FDIC's workload, under the Dodd-Frank Act, the FDIC was given new resolution authority for large bank holding companies and systemically important non-bank financial companies. As noted above, the FDIC has historically carried out a prompt and orderly resolution process under its receivership authority for insured banks and thrifts. The Dodd-Frank Act gave the FDIC a similar set of receivership powers to liquidate failed systemically important financial firms. The FDIC's Office of Complex Financial Institutions works in concert with RMS, DRR, and the Legal Division in carrying out systemic resolution activities.

In a number of instances, through purchase and assumption agreements with acquiring institutions, the Corporation has entered into shared loss agreements. In fact, since loss sharing began during the most recent crisis in November 2008, the Corporation resolved 304 failures with accompanying shared loss agreements; the initial covered balance was $216.5 billion. As of March 31, 2015, 272 receiverships still had active shared loss agreements, with a covered asset balance at that time of $44.1 billion.

Under these agreements, the FDIC agrees to absorb a portion of the loss—generally 80-95 percent—which may be experienced by the acquiring institution with regard to those assets, for a period of up to 10 years. As another resolution strategy, the FDIC entered into 35 structured sales transactions involving 43,315 assets with a total unpaid principal balance of $26.2 billion. Under these arrangements, the FDIC retains a participation interest in future net positive cash flows derived from third-party management of these assets.

Other post-closing asset management activities continue to require FDIC attention. FDIC receiverships manage assets from failed institutions, mostly those that are not purchased by acquiring institutions through purchase and assumption agreements or involved in structured sales. As of March 31, 2015, DRR was managing 483 active receiverships with assets in liquidation totaling about $7.3 billion. As receiver, the FDIC seeks to expeditiously wind up the affairs of the receiverships. Once the assets of a failed institution have been sold and the final distribution of any proceeds is made, the FDIC terminates the receivership.

As recovery from the crisis continues, some of these risk sharing agreements will be winding down and certain currently active receiverships will be terminated. Given the substantial dollar value and risks associated with the risk sharing activities and other receivership operations, the FDIC needs to ensure continuous monitoring and effective oversight to protect the FDIC's financial interests.

Looking back to the recent banking crisis, the FDIC increased its permanent resolution and receivership staffing and significantly increased its reliance on contractor and term employees to fulfill the critical resolution and receivership responsibilities associated with the ongoing FDIC interest in the assets of failed financial institutions. Now, as the number of financial institution failures continues to decline, the Corporation is reshaping its workforce and adjusting its budget and resources accordingly. Between January 2012 and April 2014, the FDIC closed three of the temporary offices it had established to handle the high volume of bank failures. In this connection, authorized staffing for DRR, in particular, fell from a peak of 2,460 in 2010 to 1,463 proposed for 2013, which reflected a reduction of 393 positions from 2012 and 997 positions over 3 years. DRR authorized staff for 2014 was 916. Authorized staffing for 2015 is 756. Of note, DRR will continue to substantially reduce its non-permanent staff each year, based on declining workload.

While OIG audits and evaluations address various aspects of controls in resolution and receivership activities, OIG investigations benefit the Corporation in other ways. For example, in the case of bank closings where fraud is suspected, our Office of Investigations may send case agents and computer forensic special agents from the ECU to the institution. ECU 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.

The OIG also coordinates with DRR on concealment of assets cases that may arise. In many instances, the FDIC debtors do not have the means to pay fines or restitution owed to the Corporation. However, some individuals do have the means to pay but hide their assets and/or lie about their ability to pay. In such instances, the Office of Investigations would work with both DRR and the Legal Division in pursuing criminal investigations of these individuals.

To help ensure the FDIC efficiently and effectively resolves failing banks and manages receiverships, the OIG's focus is as follows:

- Evaluate the FDIC's plans and systems for managing bank resolutions.
- Investigate crimes involved in or contributing to the failure of financial institutions or which lessen or otherwise affect recoveries by the DIF, involving restitution or otherwise.

OIG Work in Support of Goal 4

During the reporting period, and as discussed further below, we completed work related to the FDIC's controls for identifying securing, and disposing of personally identifiable information (PII) in owned real estate (ORE) properties that the FDIC inherits as receiver. We also continued an assignment to examine the FDIC's controls over cash flows from receivership-related taxes and another involving the risks associated with the early termination of shared loss agreements. Ongoing efforts of our ECU as they relate to bank closings support this goal and are described below.

The FDIC Can Enhance Controls for Identifying, Securing, and Disposing of Personally Identifiable Information in Owned Real Estate Properties

As the receiver of failed FDIC-insured financial institutions, the FDIC acquires ORE properties that are located throughout the United States and its territories. These properties include single-family homes, condominiums, office buildings, retail establishments, hotels, and undeveloped land (among other types of property). In some cases, ORE properties are found to contain personal property, including PII, that was left behind by the previous owners or occupants of the properties. Establishing controls to properly handle PII found at ORE properties is critical to mitigating the risk of an unauthorized disclosure that could lead to identity theft, consumer fraud, and potential legal liability or reputational damage to the Corporation. Given such risks, we conducted an audit to determine whether the FDIC has established internal controls to properly identify, secure, and dispose of PII in ORE properties. As part of our work, we reviewed the FDIC's handling of PII found at 10 non-statistically sampled ORE properties.

By way of background, when an insured financial institution fails, the FDIC establishes a receivership to liquidate the institution's assets. In many cases, these assets include ORE properties. Within the FDIC, DRR has primary responsibility for liquidating assets in receivership. According to DRR records, the FDIC acquired and liquidated approximately 14,000 ORE properties between February 2007 (when the most recent financial crisis began) and December 31, 2014.

DRR typically identifies PII at ORE properties through physical site inspections. DRR has engaged two national asset management firms (ORE contractors) to manage, market, and dispose of ORE properties. As part of their responsibilities, the ORE contractors are required to conduct site inspections of properties assigned to them. Site inspections address such things as the condition and appearance of the property, security risks, health and safety issues, and signage. In May 2014, DRR issued formal guidance requiring the ORE contractors to identify, report, safeguard, and destroy hardcopy information and electronic equipment that may contain PII. DRR Resolutions and Receiverships Specialists (Account Officers) oversee the management, marketing, and sale of ORE properties. As part of their responsibilities, Account Officers review site inspection reports prepared by the ORE contractors and ensure that liability issues, including those related to PII, are identified and properly addressed. Account Officers also perform site inspections of ORE properties to ensure they are being properly maintained and marketed for sale.

When PII is identified in an ORE property, DRR's general approach is to secure the information and arrange for its immediate destruction. In doing so, DRR coordinates with other organizations within the FDIC. These principally include the Computer Security Incident Response Team (CSIRT), a group within the Chief Information Officer Organization that is responsible for providing technical assistance in investigating, reporting, resolving, and closing incidents; the Privacy Program staff, which reviews FDIC-prepared incident risk analyses/impact assessments and makes the final determination regarding whether an incident constitutes a breach of PII; and the Legal Division which may, on a case by-case basis, provide advice on legal issues pertaining to PII found in ORE properties.

We reported that the FDIC strengthened a number of internal controls during the course of our audit that were designed to properly identify, secure, and dispose of PII at ORE properties. Among other things, DRR held a training conference and issued formal guidance to its ORE contractors and Account Officers in May 2014 that addressed procedures for identifying, reporting, securing, and disposing of PII. DRR also modified its ORE contracts in October 2014 to specifically require that the contractors search for PII during every property site inspection. Although these control improvements are positive, they do not fully address the findings of our audit.

Specifically, our review of 10 non-statistically sampled ORE properties found that PII was often not identified in a timely manner and that practices for handling and disposing of the information were inconsistent in certain key respects. For example, we found that DRR contacted some, but not all, of the owners of the PII to allow them an opportunity to remove the information before it was destroyed. We also found that CSIRT was not always contacted when PII was discovered and that CSIRT did not always conduct formal investigations when PII was discovered. Further, the type of documentation that DRR retained as evidence of the destruction of PII varied considerably, and in some instances, PII that had been authorized to be destroyed was erroneously sent to an off-site storage facility.

The nature of PII found in ORE properties raises important questions regarding the FDIC's responsibilities and obligations for handling the information. Unlike PII that DRR acquires in support of its mission (e.g., bank customer, depositor, and employee information that are considered records of failed institutions), PII acquired from ORE properties is typically left behind by businesses and individuals that may have no business relationship with the failed institution or the FDIC. We determined that a legal opinion is needed to clarify whether the PII:

- should be treated as a record of the failed institution, the personal property of the previous owner or occupant of the ORE property, or abandoned property;
- falls within the scope of federal, state, and local statutes and regulations and government-wide policy and guidance that address the handling and disposal of PII, and the extent to which the FDIC may, as a matter of policy, voluntarily comply with such criteria;
- is subject to any retention requirements; and
- should be reviewed to determine whether it is needed in connection with a criminal or civil investigation before the PII is destroyed.

In our view, obtaining a legal opinion would reduce the risk of inconsistent handling and disposal practices, which can expose the FDIC to potential criticism. After obtaining a legal opinion, it would be prudent for the FDIC to review its existing policies, procedures, guidance, and training related to the handling and disposal of PII at ORE properties to determine whether changes are warranted. In addition, the FDIC should determine an appropriate disposition for certain PII that was identified in the ORE properties that were in our sample and sent to off-site storage.

We made three recommendations intended to improve the FDIC's handling of PII found in ORE properties. The Director, DRR, concurred with the recommendations and described actions that were responsive to the recommendations.

In addition, we identified a potential control enhancement related to the FDIC's automated tools that were used to track and report information pertaining to ORE property site inspections. We reported this matter separately because it was not considered significant in the context of our audit results.

Electronic Crimes Unit Supports Closed Bank Investigations

The ECU continues to support the OIG's Office of Investigations by providing computer forensic assistance in ongoing fraud investigations, as illustrated in the following example.

ECU Provides Forensic Analysis for Case Involving Former Executives of Park Avenue Bank, New York, New York

The ECU played a key role in a successful case that resulted in two individuals pleading guilty for their roles in a complex fraud scheme during the current reporting period. (See write-up on Guilty Pleas in Park Avenue Bank case earlier in this report.) Through forensic analysis, the ECU provided assistance in establishing the involvement of the various defendants in this complex case.

Park Avenue Bank was closed on March 12, 2010, and at the time of failure, the estimated loss to the DIF was $50.7 million. Because there was evidence of potential fraud by current and former bank employees at that time, ECU assistance was requested for review of emails and other document files. The OIG's ECU agent attended the closing and coordinated with both the bank's IT staff and forensic contractors on site at the closing.

The OIG's ECU agent received over 3 terabytes of electronic evidence from the forensic contractors. The agent also received approximately 300 gigabytes of data from the bank's former IT manager. This data was processed in a computer forensics software, and keyword searches were conducted for the FDIC lead agent and the Assistant U.S. Attorney prosecuting the case. The ECU agent also searched through this data for 123 emails that were archived on the bank's email exchange server. The agent successfully recovered needed evidence through extensive searches for archive identifiers. Doing so helped the investigative team and prosecutor establish the nature of the fraud scheme and the parties involved.

The OIG Will Promote Sound Governance and Effective Stewardship and Security of Human, Financial, IT, and Physical Resources

The FDIC must effectively and economically manage and utilize a number of critical strategic resources in order to carry out its mission successfully, particularly its human, financial, information technology (IT), and physical resources. As the number of financial institution failures continues to decline, the Corporation is reshaping its workforce and adjusting its budget and resources accordingly. Efforts to promote sound governance, effective security, and vigilant stewardship of its core business processes and the IT systems supporting those processes, along with attention to human and physical resources, will continue to be keys to the Corporation's success as it operates in a post-crisis environment.

During the 2015 planning and budget process, the Corporation reassessed its current and projected workload along with trends within the banking industry and the broader economy. Based on that review, the FDIC expects a continuation of steady improvements in the global economy, a small number of insured institution failures, gradual reductions in post-failure receivership management workload, and significant further reductions in the number of 3-, 4-, and 5-rated institutions. While the FDIC will continue to need some temporary and term employees over the next several years to complete the residual workload from the financial crisis, industry trends confirm that there will be a steadily decreasing need for non-permanent employees going forward several years.

Given those circumstances, the FDIC Board of Directors approved a $2.32 billion Corporate Operating Budget for 2015, 3.0 percent lower than the 2014 budget. In conjunction with its approval of the 2015 budget, the Board also approved an authorized 2015 staffing level of 6,875 positions, down from 7,200 previously authorized, a net reduction of 325 positions. This is the fifth consecutive reduction in the FDIC's annual operating budget.

As conditions improve throughout the industry and the economy, the FDIC will continue its efforts to achieve the appropriate level of resources but at the same time, it needs to remain mindful of ever-present risks and other uncertainties in the economy that may prompt the need for additional resources and new skill sets and expertise that may be challenging to obtain. In that regard, the FDIC is continuing to work towards integrated workforce development processes as it seeks to bring on the best people to meet the FDIC's changing needs and priorities, and do so in a timely manner.

The FDIC has long promoted diversity and inclusion initiatives in the workplace. Section 342 of the Dodd-Frank Act reiterates the importance of standards for assessing diversity policies and practices and developing procedures to ensure the fair inclusion and utilization of women and minorities in the FDIC's contractor workforce. The Dodd-Frank Act also points to the Office of Minority and Women Inclusion as being instrumental in diversity and inclusion initiatives within the FDIC working environment. This office will need to ensure it has the proper staff, expertise, and organizational structure to successfully carry out its advisory responsibilities to ensure diversity and inclusion.

From an IT perspective, with heightened activity in the financial services industry and economy, the FDIC has engaged in in massive amounts of information sharing, both internally and with external partners. The FDIC may also be in a position to share highly sensitive information with other members of the Financial Services Oversight Council formed pursuant to the Dodd-Frank Act. FDIC systems contain voluminous amounts of critical data. The Corporation needs to maintain a strong and effective information security management program to protect against cyber threats to its internal systems and infrastructure, and ensure the integrity, availability, and appropriate confidentiality of bank data, personally identifiable information, and other sensitive information in an environment of increasingly sophisticated security threats and global connectivity.

In a related vein, continued attention to ensuring the physical security of all FDIC resources is also a priority. The FDIC needs to be sure that its emergency response plans provide for the safety and physical security of its personnel and ensure that its business continuity planning and disaster recovery capability keep critical business functions operational during any emergency.

Overall, enterprise risk management is a critical aspect of governance at the FDIC. Notwithstanding a stronger economy and financial services industry, the FDIC's enterprise risk management framework and related activities need to be attuned to emerging risks, both internal and external to the FDIC that can threaten corporate success. Certain issues and risk areas may fall within the purview of a single division or office, while others are cross-cutting within the FDIC, and still others involve coordination with the other financial regulators and other external parties. The Corporation needs to adopt controls, mechanisms, and risk models that can address a wide range of concerns—from specific, everyday risks such as those posed by personnel security practices and records management activities, for example, to the far broader concerns of the ramifications of an unwanted and harmful cyberattack or the failure of a large bank or systemically important financial institution.

The Corporation's stakeholders—including the Congress, American people, media, and others— expect effective governance, sound risk management practices, and vigilant regulatory oversight of the financial services industry to avoid future crises. Leaders and individuals at every working level throughout the FDIC need to understand current and emerging risks to the FDIC mission and be prepared to take necessary steps to mitigate those risks as changes occur and challenging scenarios that can undermine the FDIC's short- and long-term success present themselves.

To promote sound governance and effective stewardship and security of human, financial, IT, and physical resources, the OIG's focus in this goal area is as follows:

- Evaluate corporate efforts to manage human resources and operations efficiently, effectively, and economically.
- Promote integrity in FDIC internal operations.
- Promote alignment of IT with the FDIC's business goals and objectives.
- Promote IT security measures that ensure the confidentiality, integrity, and availability of corporate information.
- Promote personnel and physical security.
- Promote sound corporate governance and effective risk management and internal control efforts.

OIG Work in Support of Goal 5

During the reporting period, we completed four assignments in support of this goal area. We conducted a review the FDIC's efforts to provide equal opportunity and achieve senior management diversity. In the records management area, we completed work in connection with the FDIC's controls over the destruction of archived paper records. We completed our Federal Information Security Management Act of 2002 evaluation of the FDIC's information security program for 2014. Finally, we completed work involving the FDIC's input to the governmentwide financial report system. At the end of the reporting period, among other assignments, we were conducting work related to travel card controls and controls over outside counsel costs associated with professional liability claims. Completed reviews and investigative work are summarized below.

The FDIC Seeks to Provide Equal Opportunity and Achieve Senior Management Diversity

In March 2014, the Ranking Member and Minority Members of the U.S. House of Representatives Committee on Financial Services requested that we perform work related to the FDIC's efforts to increase senior management diversity. The members referenced a 2013 Government Accountability Office report that concluded, among other things, that management-level representation of minorities and women among the federal financial agencies had not changed substantially from 2007 through 2011 despite senior management diversity provisions in the Dodd-Frank Act. The members requested that we determine whether agency internal operations and personnel practices were systematically disadvantaging minorities and women from obtaining senior management positions.

The Committee members sent similar requests to the OIGs of the other federal financial regulators. We coordinated with the other OIGs and agreed to follow a common objective and approach to conducting the evaluation work. We also met and discussed our planned objective and approach with the Committee staff. Accordingly, our overall objective was to assess agency personnel operations and other efforts to increase agency diversity, create a workplace free of systematic discrimination, and provide equal opportunity for minorities and women to obtain senior management positions. The scope of this evaluation generally pertained to information and activities for the 3-year period 2011 through 2013.

Our report notes that a commitment to equal opportunity, diversity, and inclusion is critical for the federal government as an employer. Title 5 of the United States Code, section 2301(b)(1) provides that federal recruitment should be from qualified individuals from appropriate sources in an endeavor to achieve a workforce from all segments of society, and selection and advancement should be determined solely on the basis of relative ability, knowledge, and skills, after fair and open competition which assures that all receive equal opportunity. As the nation's largest employer, the federal government has an obligation to lead by example. Seeking to attain a diverse, qualified workforce is a cornerstone of the merit-based civil service.

Section 342 of the Dodd-Frank Act required the federal financial regulators to establish an Office of Minority and Women Inclusion to be responsible for all matters of the agency relating to diversity in management, employment, and business activities. Further, in August 2011, the President issued Executive Order 13583, *Establishing a Coordinated Government-Wide Initiative to Promote Diversity and Inclusion in the Federal Workforce*, to promote the federal workplace as a model of equal opportunity, diversity, and inclusion.

We reported that collectively, the FDIC's commitment, initiatives, and process controls promote a workplace that is free of systematic discrimination, and one that provides equal opportunity for women and minorities to obtain senior management positions. Despite these efforts, the FDIC's workforce statistics indicate that more work is needed to increase representation of female employees, and to a larger extent, Hispanic employees throughout the agency and at the executive manager level. We also noted that female and minority representation has remained relatively the same since 2008. Our report discusses various factors that present challenges to the FDIC's progress in this regard, such as low turnover and limited representation of women and minorities in job occupations that are prevalent at the FDIC. The Corporation established an Office of Minority and Women Inclusion as required by the Dodd-Frank Act and has implemented numerous councils, groups, and initiatives to promote diversity, inclusion, and fairness. Further, FDIC human resources processes and operations include controls intended to achieve fair and equitable outcomes. There are opportunities, however, for the FDIC to improve operations associated with its diversity and inclusion efforts.

While the FDIC has programs with controls in place to ensure fairness, we identified several areas for improvement and made nine recommendations related to recruiting, leadership training and expressions of interest programs, further analysis of employee performance results, the reliability of diversity data, and updating relevant policies.

The Deputy to the Chairman and Chief Operating Officer, Chief of Staff, responded to our report on behalf of the Corporation. The FDIC concurred with the report's nine recommendations and noted its commitment to narrowing representational gaps and promoting fair and equitable workplace outcomes. The FDIC established planned completion dates for the corrective actions throughout 2015, and expects to have them all accomplished by December 31, 2015.

Controls Over Destruction of Archived Paper Records Need Improvement

Effective records management is critical for ensuring that sufficient documentation is created; that agencies can efficiently locate and retrieve records needed in the daily performance of their missions; and that records of historical significance are identified, preserved, and made available to the public. Therefore, it is fundamental that the FDIC properly maintain and protect from damage, misuse, or improper disposition all business records created or collected in the course of conducting business, including those acquired from failed insured depository institutions. Internal control is a major part of managing an organization. It comprises the plans, methods, and procedures used to meet missions, goals, and objectives, and serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. Internal control should provide reasonable assurance that the objectives of the agency are being achieved through effective and efficient operations, reliable reporting, and compliance with applicable laws and regulations.

We conducted an evaluation to determine the extent to which controls in the FDIC's Records and Information Management program provided reasonable assurance that paper records stored off-site are being properly destroyed. We performed work to determine whether controls exist and are working as intended to ensure that record destruction decisions are properly authorized and communicated to the FDIC's records management contractor, Iron Mountain, Inc.; the FDIC's records management databases are updated and properly reflect destruction dates as supported by destruction certificates; and Iron Mountain's destruction process works as described.

Most federal agencies are required by the Federal Records Act (44 U.S.C. § 3101) to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the government and of persons directly affected by the agency's activities. The FDIC has determined that the Corporation is not covered, but FDIC policy reflects the spirit of the Act.

The FDIC contracts with Iron Mountain, Inc., for a range of records management and storage services, including records destruction. Iron Mountain uses Iron Mountain Connect™ to support its records management and billing under the FDIC's contract. The FDIC's Records and Information Management Unit (RIMU) and other FDIC staff access Iron Mountain Connect, which Iron Mountain provides as a gateway for control of customers' off-site records.

We concluded that the FDIC lacks adequate controls to ensure that archived paper records are properly destroyed. Because of control weaknesses with the records management process and the automated records management system (ARMS) that the FDIC uses to account for and manage the location of paper records, we could not confirm that record destruction decisions were properly authorized, and we observed significant FDIC records inventory discrepancies. We concluded that Iron Mountain has a robust control structure for records destruction that mitigates the risk that records could be destroyed without FDIC authorization. As discussed in more detail below, we identified a need for the FDIC to conduct a program risk assessment, and strengthen its procedures, implement stronger record inventory controls, and enhance controls for reconciling destruction certificates.

Risk Assessment and Procedures. FDIC management needs to conduct a comprehensive risk assessment and improve procedures to establish effective controls over archived paper records. While the Records and Information Management Policy Manual established recordkeeping policy, RIMU lacked sufficient implementing procedures for identifying, managing, and destroying paper records. We identified a need for greater management attention in this regard. For instance, it appears that operational events such as bank failures and FDIC office closings led to records being sent to Iron Mountain without first being entered into ARMS, creating inventory discrepancies. A comprehensive risk assessment should identify operational risks to effective records management and then the Division of Administration should develop procedures and controls to address those risks.

Inventory Controls. The FDIC needs to inventory and accurately account for its archived paper records. We identified significant inventory discrepancies during our evaluation. As of June 30, 2014, ARMS recorded 431,372 fewer boxes of archived records than Iron Mountain Connect, or nearly 33 percent of the total FDIC boxes recorded in Iron Mountain Connect. Only 249,750 ARMS box identifiers (28 percent) directly matched Iron Mountain Connect records and at least 501,640 Iron Mountain Connect box identifiers (38 percent) did not match ARMS records. Following our field work, the Division of Administration identified about 58 percent of the unmatched boxes, though further work was needed to verify box contents and enter information into ARMS. These discrepancies occurred, in part, because RIMU does not have adequate procedures to establish and maintain its records inventory. The inventory discrepancies impair the FDIC's ability to adhere to its records retention schedule, identify records subject to legal holds and legal demands, and effectively review contractor costs for records storage. In addition, the FDIC risks records being misplaced or lost.

Reconciling Destruction Requests. RIMU should strengthen procedures and controls to help ensure the FDIC can account for archived paper records that are destroyed. We were not always able to reconcile the FDIC's requests to destroy records with Iron Mountain's documentation certifying destruction. We concluded that RIMU's records destruction procedures needed improvement, contributed to inventory discrepancies, and created risk that records could become misplaced or lost. RIMU updated its SOP during our field work in November 2014. The update includes steps for reconciling Iron Mountain destruction certificates with FDIC record destruction requests and updating ARMS.

The Division of Administration began further corrective actions immediately following our field work, before we issued our report. In responding to the six recommendations we made in the report, the FDIC concurred and committed to completing corrective actions by December 31, 2015.

Federal Information Security Management Act Report Notes Progress and Areas Warranting Management's Attention

In accordance with the Federal Information Security Management Act of 2002 (FISMA), we conducted an audit to evaluate the effectiveness of the FDIC's information security program controls and practices, including the FDIC's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We evaluated the effectiveness of security controls by performing audit procedures to assess consistency between the FDIC's security controls and FISMA requirements, Office of Management and Budget (OMB) policy and guidelines, and National Institute of Standards and Technology (NIST) standards and guidelines.

Our audit scope covered the 11 security control areas outlined in the Department of Homeland Security's (DHS) December 2, 2013, document entitled, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics.* Our work included an analysis of selected controls for three of the FDIC's general support systems and a review of the Corporation's oversight of an outsourced information service provider that supports the FDIC's marketing of failing financial institutions.

We concluded that, except as described below, 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 NIST standards and guidelines. The FDIC had also taken action subsequent to our prior-year security evaluation to strengthen controls in a number of the areas that we evaluated, including:

- *Incident Response and Reporting*—by strengthening procedures and guidance for addressing computer security incidents and communicating those incidents to senior FDIC management;
- *Risk Management*—by issuing a formal policy that subjects all application development efforts—including those managed by the FDIC's business divisions or offices—to appropriate information security risk management and IT governance; and
- *Outsourced Information Systems and Services*—by establishing more meaningful metrics pertaining to oversight activities, making progress in completing those oversight activities, and beginning to require stronger security and privacy clauses for newly-awarded service agreements administered by the FDIC's Legal Division.

In addition, the FDIC had implemented 17 of 19 recommendations from our 2012 and 2013 security evaluation reports that were unaddressed as of November 21, 2013, and was working to address the remaining two recommendations at the close of our audit.

Notwithstanding these accomplishments, we reported that management attention was warranted in the security control areas of:

- *Risk Management.* The FDIC was revising its IT security risk management program policy to align with OMB policy and NIST guidelines. The FDIC can further its efforts in this area by adopting new or modified security controls, as appropriate, consistent with NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, dated April 2013.
- *Continuous Monitoring.* The FDIC was performing a number of continuous monitoring activities and had developed an assessment methodology for monitoring at the information systems level. However, the FDIC had not developed a written, corporate-wide information security continuous monitoring strategy as required by OMB policy.
- *Configuration Management.* The FDIC was working on a multi-year effort to develop baseline configurations for its information systems and strengthen its vulnerability and patch management program. As part of that effort, the Corporation needs to develop written procedures to ensure that newly-released operating system patches are tested in a consistent manner and that test results are adequately documented.
- *Plan of Action and Milestones (POA&M).* The FDIC had several initiatives underway to improve its POA&M process. The FDIC can further these efforts by (a) reviewing and enhancing (where appropriate) existing controls designed to ensure that security vulnerabilities are recorded on POA&Ms in a timely manner and (b) conducting an internal assessment of the effectiveness of the POA&M process after a reasonable period of time is allowed for the implementation of planned and ongoing improvement initiatives.
- *Contingency Planning.* The FDIC made meaningful progress in addressing our prior-year recommendations in this area. At the time of our audit, the FDIC was working to complete ongoing analysis to confirm the appropriateness of established recovery time objectives for systems supporting mission-essential functions.

Our report notes that addressing the issues described above will better align the FDIC's security program controls with FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines. It will also facilitate the identification, evaluation, and mitigation of risk to the FDIC's information and information systems.

We made five recommendations intended to improve the effectiveness of the FDIC's information security program controls and practices. The FDIC's then-Acting Chief Information Officer concurred with those recommendations.

The FDIC's General Ledger Information Agrees with Summary Information in the Governmentwide Financial Report System

Many federal agencies, including the FDIC, were required to provide financial information for the FY ended September 30, 2014, to the Department of the Treasury for inclusion in the annual Financial Report of the United States Government. The Treasury Financial Manual describes the roles of agency Chief Financial Officers and Inspectors General in processing such information through the Department of the Treasury's automated financial reporting tool – the Governmentwide Financial Report System (GFRS). We conducted an audit to verify that the FDIC's summary general ledger information agreed with summary information entered into the GFRS for the FY ended September 30, 2014.

Section 405 of the Government Management Reform Act of 1994 (31 United States Code 331(e)(1)) requires the Secretary of the Treasury to annually prepare and submit to the President and the Congress an audited financial statement for the preceding FY. The Treasury Financial Manual describes, among other things, how agencies are to provide data for inclusion in the annual Financial Report of the United States Government using the GFRS. Further, the IGs are required to submit certain documents, such as agency legal and management representation letters, to the Department of the Treasury, the U.S. Government Accountability Office (GAO), OMB, and/or Department of Justice.

We verified that the FDIC's summary general ledger information agreed with summary information entered into the GFRS for the FY ended September 30, 2014. As part of our work, we verified that the FDIC's data submissions in the GFRS for the year ended December 31, 2013 agreed with the Corporation's audited financial statements for that year. In that regard, the GAO expressed an unmodified opinion on the financial statements of the funds administered by the FDIC in its March 2014 report entitled, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2013 and 2012 Financial Statements* (Report No. GAO-14-303). In addition, we submitted copies of requisite reports and representation letters to the Department of the Treasury, GAO, OMB, and the Department of Justice in accordance with the Treasury Financial Manual.

Our report did not contain recommendations, and the Corporation elected not to provide a written response.

The OIG's Electronic Crimes Unit Recovers Stolen Laptops

During the reporting period, the FDIC CSIRT notified the OIG that an FDIC laptop was missing from inventory and believed to be stolen. Specifically, a Lenovo X-201 had been returned to inventory when a former employee separated from the FDIC in April 2013. Later, however, between October 2013 and March 2014, the FDIC had received a McAfee ePolicy Orchestrator alert from a machine named "Jesussaves". While the machine was apparently renamed, the machine serial number and other identifying information matched the Lenovo X-201 formerly assigned to the separated FDIC employee. CSIRT was able to determine that the machine was no longer in the FDIC's inventory. The internet protocol (IP) address associated with the machine name "Jesussaves" was a Verizon Fios IP address.

A subpoena was sent to Verizon for the registered owner of the IP address. Verizon records showed that the IP address was registered to the wife of an FDIC contractor. The ECU went to the residence and spoke with the wife of the FDIC contractor. While in the residence, the contractor's wife returned the missing X-201 and the ECU special agent identified a second FDIC laptop that was also missing from the FDIC's inventory. The ECU later interviewed the contractor, who admitted to taking both laptops without permission. The contractor accepted a plea agreement for one count of theft over $1,000 and under $10,000. He was sentenced to 2 years in prison, all suspended, and 18 months of probation.

Responsible Parties: *The case was prosecuted by the Prince George's County, Maryland, State's Attorney's Office.*

FDIC OIG's Electronic Crimes Unit Addresses Threats to FDIC Information Security

The Electronic Crimes Unit is tackling threats to the FDIC's IT environment on several fronts. During the reporting period, we continued our coordination with the Division of Information Technology and the Chief Information Officer Organization with respect to detecting and preventing insider threats to the abundance of sensitive information and personally identifiable information held by the Corporation. Together we are seeking to proactively prevent any release by FDIC insiders—accidental or deliberate—of such 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.

Additionally, and on a broader scale, the OIG is a member of the National Cyber Investigative Joint Task Force (NCIJTF). In 2008, the President mandated the NCIJTF to be the focal point for all government agencies to coordinate, integrate, and share information related to all domestic cyber threat investigations. The FBI is responsible for developing and supporting the joint task force, which includes 19 intelligence agencies and law enforcement, working together to identify key players and schemes. Its goal is to predict and prevent what is on the horizon and to pursue the enterprises behind cyber attacks. The NCIJTF focuses on making the Internet safer by pursuing the terrorists, spies, and criminals who seek to exploit our systems. Because they act globally across many jurisdictions, the collaboration offered through the NCIJTF is critical to ensure all legal means and resources available are used to track, attribute, and take action against these cyber threats.

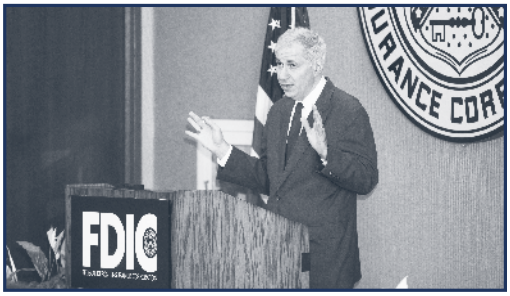
Finally, during the reporting period, the OIG became a member of the FBI's Washington Field Office Cyber Task Force. With the FDIC headquarters and primary information technology infrastructure located within the Washington Field Office territory, the OIG is well situated to be part of any cyber investigation involving the FDIC. Additionally, as part of this task force, we are in contact with other FBI cyber task forces around the country, thus enabling coordination and communication on issues affecting FDIC field locations as well.

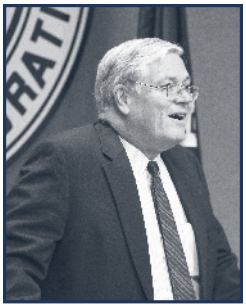
OIG Resources Management: Build and Sustain a High-Quality Staff, Effective Operations, OIG Independence, and Mutually Beneficial Working Relationships

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 develop and retain a high-quality staff, effective operations, OIG independence, and mutually beneficial working relationships with all stakeholders. 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 new resolution authorities under the Dodd-Frank Act. All of these activities required vigilant, independent oversight. Now that the crisis has eased and economic conditions are improving, we 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. As a result, we are closely monitoring our staffing and taking steps to ensure we are positioned to sustain quality work even 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 strive to keep communication channels open throughout the office. We are mindful of ensuring 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.

To carry out our responsibilities, the OIG must be professional, independent, objective, fact-based, nonpartisan, fair, and balanced in all its work. Also, the Inspector General 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 the Council of the Inspectors General on Integrity and Efficiency (CIGIE), the OIG is mindful of the Q*uality 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 the Department of Justice.





Senior leaders share perspectives with OIG staff at All-Hands Conference. (Pictured above: FDIC Chairman Martin Gruenberg, Acting IG Fred Gibson, and FDIC Vice Chairman Tom Hoenig.)

Strong working relationships are fundamental to our success. We place a high priority on maintaining positive working relationships with the FDIC Chairman, Vice Chairman, other FDIC Board members, and management officials. 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 meet with division and office leaders and attend and participate in internal FDIC conferences and other forums.

The OIG also 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 CIGIE activities. 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 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 Inspector General 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 Government Accountability Office to coordinate work, provide OIG perspectives on risk, and minimize duplication of effort. We also work closely with representatives of the Department of Justice, including the FBI and U.S. Attorneys' Offices, to coordinate our criminal investigative work and pursue matters of mutual interest.

The FDIC OIG has its own strategic and annual planning processes independent of the Corporation's planning process, in keeping with the independent nature of the OIG's core mission. The Government Performance and Results Act of 1993 (GPRA) was enacted to improve the management, effectiveness, and accountability of federal programs. GPRA requires most federal agencies, including the FDIC, to develop a strategic plan that broadly defines the agency's mission and vision, an annual performance plan that translates the vision and goals of the strategic plan into measurable objectives, and an annual performance report that compares actual results against planned goals. The GPRA Modernization Act of 2010 was signed into law on January 4, 2011.

The OIG supports GPRA and is committed to applying its principles of strategic planning and performance measurement and reporting to our operations. The OIG's Business Plan has historically laid out a basic foundation for establishing goals, measuring performance, and reporting accomplishments consistent with the principles and concepts of GPRA. We continuously seek to integrate risk management considerations in all aspects of OIG planning—both with respect to external and internal work. Importantly, the OIG is continuing to re-examine the strategic and performance goals and related activities that have guided our past efforts to determine whether they continue to provide the best framework within which to carry out our mission in the current FDIC and OIG operating environment.

To build and sustain a high-quality staff, effective operations, OIG independence, and mutually beneficial working relationships, the OIG's focus is as follows:

- Effectively and efficiently manage OIG human, financial, IT, and physical resources.
- Ensure quality and efficiency of OIG audits, evaluations, investigations, and other projects and operations.
- Encourage individual growth and strengthen human capital management and leadership through professional development and training.
- Foster good client, stakeholder, and staff relationships.
- Enhance OIG risk management activities.

A brief listing of OIG activities in support of these areas of focus follows.

Acting IG Fred Gibson with participants at DICJ's 8th Round Table in Tokyo, Japan.

Ideas Exchanged in Tokyo

Acting Inspector General Fred W. Gibson was invited to attend and make presentations at the Deposit Insurance Corporation of Japan's 8th Round Table on March 25-26, 2015, in Tokyo, Japan. This international conference included 38 representatives of deposit insurance institutions and relevant entities from 15 countries/jurisdictions around the world. Attendees came from Korea, Malaysia, Vietnam, the Philippines, Taiwan, Thailand, and Europe, to name a few. The theme of the roundtable was "Legal Issues on Bank Resolution." Emphasis was on the following matters: legal powers and role-sharing among resolution authorities, legal issues regarding the resolution of systemically important financial institutions, and pursuit of liability in bank resolutions.

Effectively and Efficiently Manage OIG Human, Financial, IT, and Physical Resources

1	Provided the OIG's FY 2016 budget proposal to our House Appropriations Subcommittee on Financial Services and General Government, and Senate Appropriations Subcommittee on Financial Services and General Government, proposing a budget of $34.6 million, to fund 130 authorized positions, which reflects no change from our FY 2015, FY 2014, and FY 2013 budgets.
2	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.
3	Continued efforts to develop a new investigative case management system and worked to better track audit and evaluation assignment milestones and costs and to manage audit and evaluation records located in TeamMate or on shared drives or SharePoint sites.
4	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.
5	Continued using our 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. Participated with the FDIC's group of Public Service Providers to share information on inquiries and complaints received, identify common trends, and determine how best to respond to public concerns.
6	Continued to refine our redesigned OIG Intranet site to provide a more useful, efficient work tool for all OIG staff.
7	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 three entry–level investigators and an IT specialist.

Ensure Quality and Efficiency of OIG Audits, Evaluations, Investigations, and Other Projects and Operations

1	Continued to implement the OIG's Quality Assurance Plan for October 2013–March 2016 to ensure quality in all audit and attestation engagement work and evaluations, in keeping with government auditing standards and *Quality Standards for Inspection and Evaluation*. As part of those efforts, held auditor and evaluator training to reinforce policies, procedures, and adherence to standards.
2	Oversaw contracts to qualified firms to provide audit and evaluation services to the OIG to enhance the quality of our work and the breadth of our expertise as we conduct audits and evaluations, and closely monitored contractor performance.
3	Participated in planning and attended the FDIC's Annual Accounting and Auditing Conference to offer OIG staff and others continuing professional education in matters relating to the current economic environment, emerging risk areas, and changes to accounting and auditing standards and practices, in the interest of enhancing the quality of the audit and evaluation function and knowledge of current trends and approaches to auditing and accounting issues.
4	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.
5	Issued the results of a peer review of the system of internal safeguards and management procedures for the investigative function of the Environmental Protection Agency to ensure compliance with quality standards established by CIGIE and applicable Attorney General guidelines. Determined that EPA OIG was in compliance with quality standards established by CIGIE and relevant Attorney General Guidelines.
6	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 all such policies to a new automated policies and procedures repository for use by all OIG staff.
7	Monitored and participated in the Corporation's Plain Writing Act initiative to ensure quality products and OIG compliance with the intent of the Act, particularly with respect to the OIG's interface with the public on the OIG Web site.

Encourage Individual Growth and Strengthen Human Capital Management and Leadership Through Professional Development and Training

1	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 four OIG staff for enrollment in the next session of the banking schools at Southwestern Graduate School of Banking, Southern Methodist University, Dallas; Graduate School of Banking, University of Wisconsin, Madison, Wisconsin; Colorado Graduate School of Banking, University of Colorado, Boulder, Colorado; and the American Bankers Association Commercial Lending School, Southwestern Methodist University, Dallas, Texas.
2	Employed interns on a part-time basis in the OIG to provide assistance to the OIG.
3	Assigned the OIG's regional office special agents in charge on details to the OIG's headquarters office to serve as the Deputy Assistant Inspector General for Investigations as a learning and professional development opportunity.
4	Enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities.
5	Commenced the OIG's Mentoring Program for 2015, which pairs mentors and mentorees as a means of developing and enriching both parties in the relationship and enhancing contributions of OIG staff to the mission of the OIG.
6	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.

Foster Good Client, Stakeholder, and Staff Relationships

1	Maintained congressional working relationships by communicating with various Committee staff on issues of interest to them; providing them our semiannual report to the Congress; notifying interested congressional parties regarding the OIG's completed audit and evaluation work; monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the Corporation's Office of Legislative Affairs on issues of mutual interest.
2	Communicated with the Chairman, Vice Chairman, FDIC's internal Director, other FDIC Board Members, the Chief Financial Officer, and other senior FDIC officials through the Acting Inspector General's regularly scheduled meetings with them and through other forums.
3	Participated in numerous outreach efforts with such external groups as the Federal Audit Executive Council, Department of Justice, and the Federal Financial Institutions Examination Council to provide general information regarding the OIG and share perspectives on issues of mutual concern and importance to the financial services industry.
4	Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
5	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 of recent actions in OIG cases and providing Office of Investigations' quarterly reports to RMS, DRR, the Legal Division, and other corporate officials 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.
6	Coordinated with the 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.
7	Expanded interactions with international counterparts by meeting with a delegation from the Deposit Insurance Corporation of Japan and sharing information on the mission of the FDIC OIG, our investigative function and coordination with the Department of Justice, and a more in-depth review of two of our recent cases. Also met with the Chief Internal Auditor from the Deposit Insurance Corporation of Canada to exchange information and discuss approaches of the FDIC and our office with respect to the resolution of large, complex entities.

Foster Good Client, Stakeholder, and Staff Relationships (cont'd)

8	Supported the Inspector General community by participating on the CIGIE Audit Committee; attending monthly CIGIE meetings; participating in Assistant Inspectors General for Investigations, Council of Counsels to the IGs, and other meetings; and commenting on various legislative matters through the Legislative Committee.
9	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. Formed part of the team auditing the Financial Stability Oversight Council's oversight of interest rate risk and provided the FDIC OIG's input to the CIGFO's annual report for 2015.
10	Coordinated with the Government Accountability Office on its ongoing efforts related to the annual financial statement audit of the FDIC and on other GAO work of mutual interest.
11	Coordinated with the FDIC's Public Service Provider group on matters regarding inquiries from the public and how best to respond to or refer such inquiries and related concerns.
12	Coordinated with the Department of Justice 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 FDIC's Office of Communications and Chairman's Office of such releases.
13	Responded to multiple requests from the Congress, including with respect to closed investigations, evaluations, and audits that were not disclosed to the public; open and unimplemented recommendations; any instances where the FDIC restricted access to records or other information; investigations of senior FDIC officials; any instances of whistleblower retaliation; and circumstances where the FDIC could claim the ability to deny the Congress access to OIG information. (See related write-up elsewhere in this report.)
14	Coordinated with SIGTARP to provide information on FDIC OIG work related to any SIGTARP matters for inclusion in SIGTARP's quarterly reports to the Congress.
15	Convened meetings of the OIG's Workplace Excellence Council, in keeping with the Corporation's model of the same. The Council undertook a review of the OIG's award program and provided its results to the Acting Inspector General.

Enhance OIG Risk Management Activities

1	Undertook risk-based OIG planning efforts for audits, evaluations, and investigations for FY 2015 and beyond, taking into consideration the goals of, and risks to, FDIC corporate programs and operations and those risks more specific to the OIG. Devoted resources to developing a universe of FDIC programs, activities, and risk areas and used corporate performance goals as further input for identifying risk areas and priorities for OIG planned coverage for the FY. Incorporated such information in broader discussions related to longer-term, OIG strategic planning.
2	Attended FDIC Board Meetings, IT/Cyber Security Oversight Group meetings, Complex Financial Institutions Coordination Group 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.
3	Assessed OIG controls in support of the annual assurance letter to the FDIC Chairman, under which the OIG provides assurance that it has made a reasonable effort to meet the internal control requirements of the Federal Managers' Financial Integrity Act, OMB A-123, and other key legislation, and issued the OIG's assurance letter on November 17, 2014.
4	Reviewed the OIG's Continuity of Operations plans to ensure readiness for weather, health, or other crises that could impact OIG staff and operations. Designated April 2015 as OIG Emergency Preparedness Month—to assess and ensure an effective response to an emergency in the Washington, D.C. area, including assessing our shelter-in-place and evacuation practices to ensure safety and a full accounting of employees during an emergency.
5	Provided the Government Accountability Office our perspectives on the risk of fraud at the FDIC. We did so in response to the Government Accountability Office's responsibility under Statement of Auditing Standards No. 99, Consideration of Fraud in Financial Statement Audits.
6	Monitored the management and performance challenge areas that we identified at the FDIC, in accordance with the Reports Consolidation Act of 2000 as we conducted audits, evaluations, and investigations: Carrying Out Dodd-Frank Act Responsibilities, Maintaining Strong IT Security and Governance Practices, Maintaining Effective Supervisory Activities and Preserving Community Banking, Carrying Out Current and Future Resolution and Receivership Responsibilities, Ensuring the Continued Strength of the Insurance Fund, Promoting Consumer Protections and Economic Inclusion, Implementing Workforce Changes and Budget Reductions, and Ensuring Effective Enterprise Risk Management Practices.

Congressional Activity During the Reporting Period

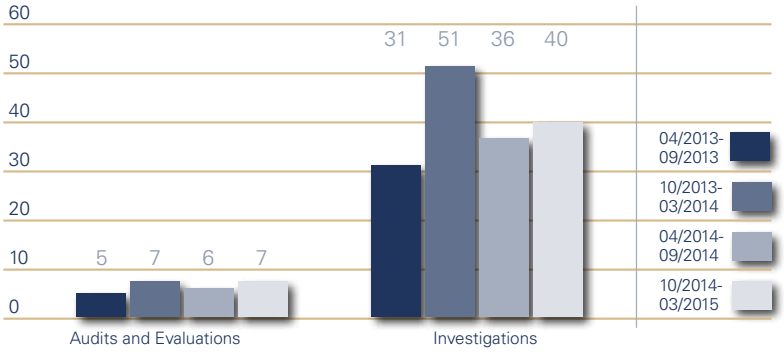
As discussed elsewhere in this report, during the reporting period, we completed work in response to a request from the Ranking Member and Minority Members of the Committee on Financial Services, U.S. House of Representatives, related to the FDIC's efforts to increase senior management diversity. (See write-up on *The FDIC's Efforts to Provide Equal Opportunity and Achieve Senior Management Diversity*.) The FDIC OIG has responded to a number of other Congressional requests during the period, as summarized below:

- Responded to request from 35 Members of the Congress who asked that the OIG investigate the FDIC's involvement with the Department of Justice program known as Operation Choke Point. We responded that in keeping with our Congressional protocols, we would work with the Committee structure in fulfilling our responsibilities. Thus, we advised the Chairman of the House Committee on Financial Services and the Chairman of the House Committee on Oversight and Government Reform, and subsequently the 35 Members, of our approach to the concerns raised regarding Operation Choke Point. First, our Office of Investigations would investigate the serious allegation that a senior official provided false testimony to the Congress. Second, our Office of Audits would review the FDIC's supervisory activities related to Operation Choke Point and determine whether the actions and policies of the FDIC were consistent with applicable laws, regulations, and policy, and with the mission of the FDIC. Both bodies of work were ongoing as of the end of the reporting period. (November 7, 2014)
- Responded to a joint request from the Ranking Members of the Senate Committee on the Judiciary and the Senate Committee on Homeland Security and Governmental Affairs for a biannual report on all closed audits, investigations, and evaluations conducted by our office that were not disclosed to the public. (December 4, 2014)
- Responded to a joint request from the Chairman and Ranking Member of the House Committee on Oversight and Government Reform regarding open and unimplemented recommendations; closed investigations, audits, and evaluations that were not disclosed to the public; and any instances where the FDIC restricted OIG access to records or other information. (March 11, 2015)
- Responded to a joint request from the Chairman, Senate Committee on the Judiciary, and Chairman, Senate Committee on Homeland Security and Governmental Affairs, for any information regarding outstanding unimplemented recommendations; products provided to the agency for comment but not responded to within 60 days; investigations of senior officials where misconduct was found but no prosecution resulted; any instances of whistleblower retaliation; any attempts to interfere with IG independence; instances of resistance or objections to IG oversight activities or restricted or delayed access to information; and closed investigations, audits, and evaluations that were not disclosed to the public. (March 27, 2015)
- Responded to a request from the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs regarding circumstances under which the FDIC Inspector General has or could claim the ability to deny the Congress access to any information in the possession of the FDIC IG. (March 31, 2015)

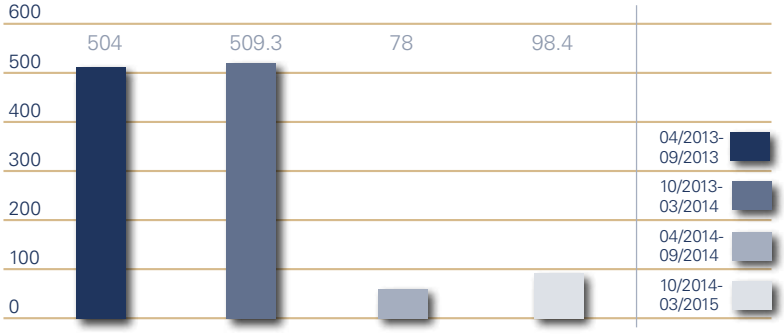
Cumulative Results (2-year period)

Nonmonetary Recommendations	
April 2013 – September 2013	15
October 2013 – March 2014	37
April 2014 – September 2014	27
October 2014 – March 2015	35

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	66
Section 5(a)(1)	Significant problems, abuses, and deficiencies	8-53
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies	8-53
Section 5(a)(3)	Recommendations described in previous semiannual reports on which corrective action has not been completed	67
Section 5(a)(4)	Matters referred to prosecutive authorities	7
Section 5(a)(5) and 6(b)(2)	Summary of instances where requested information was refused	68
Section 5(a)(6)	Listing of audit reports	67
Section 5(a)(7)	Summary of particularly significant reports	8-53
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	68
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	68
Section 5(a)(10)	Audit recommendations more than 6 months old for which no management decision has been made	68
Section 5(a)(11)	Significant revised management decisions during the current reporting period	68
Section 5(a)(12)	Significant management decisions with which the OIG disagreed	68

Evaluation report statistics are included in this report as well, in accordance with the Inspector General Reform Act of 2008.

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:

- Public Law 113-283, the Federal Information Security Modernization Act
- S. 579, the Inspector General Empowerment Act of 2015
- S. 2520, the FOIA Improvement Act of 2014
- H.R. 1211, the FOIA Oversight and Implementation Act of 2013

In addition, we reviewed a number of OMB documents pertinent to our work, as follows:

- Draft of OMB Memorandum 15-xx, regarding audit requirements for federal financial statements
- Draft of OMB Circular No. A-130, Management of Federal Information Resources, appendices—
    - Appendix II, Government Paperwork Elimination Act
    - Appendix III, Security of Federal Information Resources
- OMB Memorandum 15-02, Appendix C to Circular No. A-123, Requirements for Effective Estimation and Remediation of Improper Payments
- OMB Memorandum 15-01, FY 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices

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

The information for this reporting requirement is based on (1) information supplied by the FDIC's Corporate Management Control, Division of Finance, and (2) the OIG's determination of closed recommendations. Recommendations are closed when (a) the Corporate Management Control notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, after the OIG confirms that corrective actions have been completed and are responsive.

There are currently no significant recommendations from previous semiannual reports on which corrective actions have not been completed.

Table II
Audit and Evaluation Reports Issued by Subject Area

Audit/Evalution Report		Questioned Costs		Funds Put to Better Use
Report Number and Date	**Title**	**Total**	**Unsupported**	
Supervision				
EVAL-15-003 March 18, 2015	The FDIC's Supervisory Approach to Cyberattack Risks		N/A	
AUD-15-003 March 30, 2015	In-Depth Review of the Failure of Vantage Point Bank, Horsham, Pennsylvania		N/A	
Receivership Management				
AUD-15-004 March 31, 2015	The FDIC's Controls for Identifying, Securing, and Disposing of Personally Identifiable Information in Owned Real Estate Properties		N/A	
Resources Management				
AUD-15-001 November 3, 2014	Independent Evaluation of the FDIC's Information Security Program-2014		N/A	
EVAL-15-001 November 28, 2014	The FDIC's Efforts to Provide Equal Opportunity and Achieve Senior Management Diversity		N/A	
AUD-15-002 February 24, 2015	The FDIC's Data Submissions through the Governmentwide Financial Report System as of September 30, 2014		N/A	
EVAL-15-002 February 26, 2015	The FDIC's Controls Over Destruction of Archived Paper Records		N/A	
Totals for the Period		**$0**	**$0**	**$0**

Table III
Audit and Evaluation Reports Issued with Questioned Costs

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

Table IV
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 V
Status of OIG Recommendations Without Management Decisions

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

Table VI
Significant Revised Management Decisions

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

Table VII
Significant Management Decisions with Which the OIG Disagreed

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

Table VIII
Instances Where Information Was Refused

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

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, 2014 through March 31, 2015
(for failures causing losses to the DIF of less than $150 million from January 1, 2012 through December 31, 2013, and less than $50 million for losses that occur on or after January 1, 2014)

Institution Name	Closing Date	Estimated Loss to DIF ($ millions)	Grounds Identified by the State Bank Supervisor for Appointing the FDIC as Receiver	Unusual Circumstances Warranting In-Depth Review?	Reason for In-Depth Review	Due Date or Date Issued
Failure Review Activity – Updated from Previous Semiannual Report						
Reviews Completed During the Reporting Period						
Valley Bank Fort Lauderdale, Florida	6/20/14	$7.7	The bank was insolvent.	No*		
Columbia Savings Bank Cincinnati, Ohio	5/23/14	$5.3	The bank failed to comply with a Consent Order; was critically undercapitalized; and was operating in an unsafe and unsound condition, and insolvency was imminent.	No		
AztecAmerica Bank Berwyn, Illinois	5/16/14	$18	The bank's capital was impaired, and the bank was in an unsound condition and conducting its business in an unsafe and unsound manner.	No		
Allendale County Bank Fairfax, South Carolina	4/25/14	$17.1	The bank was insolvent and the continued operation of the bank was likely to result in an inability to meet the demands of depositors.	No		
Vantage Point Bank Horsham, Pennsylvania	2/28/14	$8.5	The bank had insufficient capital.	Yes	Requested by the Director of RMS due to concerns over de novo institution changes to business plan.	March 30, 2015

* Unusual circumstances involving this bank are being addressed in our material loss review of the affiliated lead bank, Valley Bank, Moline, Illinois.

FDIC OIG Review Activity for the Period October 1, 2014 through March 31, 2015
(for failures causing losses to the DIF of less than $150 million from January 1, 2012 through December 31, 2013, and less than $50 million for losses that occur on or after January 1, 2014)

Institution Name	Closing Date	Estimated Loss to DIF ($ millions)	Grounds Identified by the State Bank Supervisor for Appointing the FDIC as Receiver	Unusual Circumstances Warranting In-Depth Review?	Reason for In-Depth Review	Due Date or Date Issued
Reviews Completed During the Reporting Period (cont'd)						
Syringa Bank Boise, Idaho	1/31/14	$4.5	The bank failed to comply with a Consent Order; the capital of the bank was impaired and was below the amount required by law; and the bank was in an unsafe and unsound condition.	No		
Bank of Jackson County Graceville, Florida	10/30/13	$5.1	The bank was imminently insolvent.	No		
Bank of Wausau Wausau, Wisconsin	8/9/13	$13.5	The bank was operating operating in an unsafe manner.	No		
First Community Bank of SW Florida Fort Myers, Florida	8/2/13	$27.1	The bank was imminently insolvent.	No		
Parkway Bank Lenoir, North Carolina	4/26/13	$18.1	The bank was in an unsafe or unsound condition.	No		
Douglas County Bank Douglasville, Georgia	4/26/13	$86.4	The bank could not meet the requirements of minimum levels of capitalization.	No		

FDIC OIG Review Activity for the Period October 1, 2014 through March 31, 2015
(for failures causing losses to the DIF of less than $150 million from January 1, 2012 through December 31, 2013, and less than $50 million for losses that occur on or after January 1, 2014)

Institution Name	Closing Date	Estimated Loss to DIF ($ millions)	Grounds Identified by the State Bank Supervisor for Appointing the FDIC as Receiver	Unusual Circumstances Warranting In-Depth Review?	Reason for In-Depth Review	Due Date or Date Issued
Reviews Pending/Ongoing as of the End of the Reporting Period						
Highland Community Bank Chicago, Illinois	1/23/15	$5.8				
Northern Star Bank Mankato, Minnesota	12/19/14	$5.9				
Eastside Commercial Bank Conyers, Georgia	7/18/14	$33.9				
The Freedom State Bank Freedom, Oklahoma	6/27/14	$5.8				

Peer Review Activity

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

Section 989C of the Dodd-Frank Act contains additional semiannual reporting requirements pertaining to peer review reports. Federal Inspectors General are required to engage in peer review processes related to both their audit and investigative operations. In keeping with Section 989C, 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

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.

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 External Peer Reviews of the 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. Department of State (DOS) and the Broadcasting Board of Governors OIG conducted a peer review of the FDIC OIG's audit organization and issued its system review report on September 17, 2013. In the DOS OIG's opinion, the system of quality control for our audit organization in effect during the period April 1, 2011 through March 31, 2013, had been suitably designed and complied with to provide our office with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. We received a peer review rating of pass.

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

  As of September 30, 2014, we consider all recommendations to be closed.

This peer review report (the system review report and accompanying letter of comment) is posted on our Web site at www.fdicig.gov.

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.

As is customary, we also issued a Letter of Comment, dated April 30, 2014, that set forth findings and recommendations that were not considered to be of sufficient significance to affect our opinion expressed in the system review report. We made 14 recommendations. NARA OIG agreed with 11 of the 14 recommendations, partially agreed with one recommendation, and did not agree with the remaining two recommendations. NARA's planned actions adequately addressed the 11 recommendations with which NARA agreed. With respect to the remaining three, NARA's response included a rationale for its decision not to fully address those recommendations. Estimated completion dates for corrective actions ranged from June 30, 2014 to September 30, 2014. In our last semiannual report, we noted that NARA OIG advised us that it had completed actions on all but two of the agreed-upon recommendations and planned full implementation of the two outstanding recommendations by March 31, 2015. In updating the status for the current reporting period, NARA OIG informed us that it has revised the planned implementation date from March 31, 2015 to September 30, 2015. NARA OIG has posted the peer review report (system review report) on its Web site at www.archives.gov/oig/.

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. The 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 Energy 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 July 31, 2012. The Department of Energy 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 June 22, 2012, was in compliance with quality standards established by the CIGIE and the 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 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.

Our Office of Investigations anticipates being reviewed by the Department of the Treasury OIG in 2015.

Allan Sherman
Retirement

Allan Sherman retired from the FDIC after nearly 32 years of federal service. His career began in 1983 when he joined the Department of the Interior OIG as an auditor. Over the next 4½ years in that office, he advanced steadily in his profession and in 1988 transferred to the Federal Home Loan Bank Board (FHLBB) to continue work as an auditor. In October 1989, in accordance with the Financial Institutions Reform, Recovery, and Enforcement Act of 1989, the FHLBB merged with the FDIC OIG, and along with others from that organization, he joined the FDIC OIG audit staff. Since that time, Allan contributed in numerous ways to the success of the OIG as he worked on teams conducting audits of the FDIC's programs and operations, managed audit staff, and led a number of special projects.

Allan made numerous contributions not only to our office but to the Inspector General community at large. Working through the Audit Committee of the Council of the Inspectors General on Integrity and Efficiency (CIGIE), Allan developed and delivered peer review training for the Inspector General community, served as a peer review subject matter expert when questions arose, advised the Department of Defense OIG in its peer review of the Defense Contract Audit Agency, and helped update versions of the CIGIE peer review guide. He also played a key role in helping to establish, update, and carry out the OIG's Office of Audits and Evaluations' internal policies, procedures, and processes, all in the interest of ensuring quality work. As part of that effort, he prepared quality control plans, which involved managing annual and targeted quality control reviews and associated activities. Allan also led peer reviews of other federal audit organizations on behalf of the FDIC OIG and coordinated with other OIGs conducting peer reviews of our own audit operations. He was largely responsible for our office receiving the highest peer review rating of "pass" over multiple review cycles.

Karen Savia
Retirement

Karen Savia retired from the FDIC after more than 35 years of federal service. After a temporary assignment at the Naval Sea Systems Command and 10 months working at the Department of Education, she began her federal career in earnest in 1981when she joined the U.S. General Accounting Office (GAO) (now the Government Accountability Office) as an auditor. At GAO she worked on program audits and policy evaluations involving a number of federal agencies. Later she became an evaluator-in-charge and an assignment manager, taking on increasing responsibilities during her 10-year career at GAO and traveling the world to do so. In 1991, she joined the Resolution Trust Corporation OIG, specifically to organize and operate the OIG's Fraud Hotline, refer complaints, manage the comment process on Resolution Trust Corporation directives, and perform special projects.

While at the FDIC OIG, Karen managed the OIG's training program and helped promote our participation in graduate schools of banking. She also played a key role in developing the OIG's mentoring program. She spearheaded the OIG's implementation of Zavanta—a new software program to capture and manage the OIG's internal policies, procedures, and processes. Also of note, at the outset of the financial crisis, she partnered with the FDIC's Corporate University to design and deliver a comprehensive 4-day training program for financial regulatory OIGs conducting material loss reviews of failed financial institutions, and she also participated on several of our material loss reviews teams during the banking crisis.

Mike Lombardi
Retirement

Mike Lombardi retired from the FDIC after more than 37 years of federal service. From May 1977 through May 1979, he held temporary appointments at the Department of the Treasury's Bureau of Public Debt, Internal Revenue Service, and Bureau of Labor Statistics as an accounting technician, file clerk, and clerk, respectively. In June 1979, he continued his federal career as a financial assistant with the Federal Home Loan Bank Board (FHLBB) in Washington, D.C. and thereafter spent more than 10 years with the FHLBB with promotions to auditor and supervisory auditor positions. Following the merger of the FHLBB with the FDIC in October 1989, he transferred to the FDIC OIG as a supervisory auditor.

From then until he retired, Mike advanced steadily in his career, taking on increasingly important audit management and supervisory roles and responsibilities and also working for several years early-on at the FDIC as a manager in the OIG's Investigations Unit. Importantly, in the aftermath of the banking crisis of the late 1980s and early 1990s, he helped develop the OIG's program for the conduct of material loss reviews, in accordance with the FDIC Improvement Act of 1991. He also earned certifications as a public accountant in 1981 and fraud examiner in 1990.

Mike's work resulted in substantial improvements in the economy, efficiency, effectiveness, and integrity of the Corporation's programs. This was especially true with respect to assignments involving supervision and consumer protection activities, where Mike's subject matter expertise proved invaluable. Of note, during the most recent financial crisis, in accordance with the Dodd-Frank Wall Street Reform and Consumer Protection Act, he led many material loss reviews, in-depth reviews, and failed bank reviews of failed FDIC-supervised institutions, closely monitored the OIG's program for conducting such reviews, and coordinated with OIGs from the other primary federal regulators to ensure a consistent approach to this challenging work.

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

Please visit our Web site:
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, contractors, and others 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