FEDERAL DEPOSIT INSURANCE CORPORATION

Office of Inspector General

Semiannual Report to the Congress

October 1, 2013 – March 31, 2014

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 7,340 individuals carry out the FDIC mission throughout the country. According to most current FDIC data, the FDIC insured more than $6.0 trillion in deposits in 6,812 institutions, of which the FDIC supervised 4,312. 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 steadily increased to a positive $47.2 billion as of December 31, 2013. Receiverships under FDIC control as of January 31, 2014, totaled 483, with assets in liquidation totaling about $10.8 billion.

Office of Inspector General

Semiannual Report to the Congress

October 1, 2013 – March 31, 2014

FEDERAL DEPOSIT INSURANCE CORPORATION

Acting Inspector General's Statement

I am pleased to present the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General's (OIG) semiannual report for the period October 1, 2013 through March 31, 2014. Over the past 6 months, we have completed a number of investigations, audits, and evaluations. Additionally, we have begun a series of new assignments as we continue to operate in a post-crisis environment. Several highlights from the reporting period follow and are discussed in more detail in our report.

Our investigators, in partnership with the Department of Justice and law enforcement colleagues, successfully brought to justice former bank officials and other bank-affiliated parties who had used their positions of trust to undermine the integrity of the banking system. In one case, for example, seven former officers of the First National Bank of Savannah, Savannah, Georgia, pleaded guilty to a scheme wherein they hid millions of dollars in non-performing loans from the bank, members of the Board of Directors, and federal regulators. In another case, the former chairman and chief executive officer of Summit Bank, Burlington, Washington, was sentenced to 3 years in prison, to be followed by 2 years of supervised release for falsifying regulatory records and was barred from working in a federally insured institution. Overall, our investigations during the past 6-month period resulted in 56 indictments; 49 convictions; and $509.3 million in fines, restitution, and other monetary recoveries.

With respect to audits and evaluations, we completed our review of the Corporation's implementation of its new systemic resolution responsibilities under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), conducted at the request of FDIC Chairman Gruenberg. In that report we made six recommendations intended to better position the Corporation to face future challenges associated with implementing its new resolution authorities. Our annual work under the Federal Information Security Management Act of 2002 led to 15 recommendations to more effectively identify, evaluate, and mitigate risks to the FDIC's information systems and data. Other ongoing audit and evaluation assignments include assessing the FDIC's enforcement actions and professional liability claims against institution-affiliated parties and individuals, further work on the FDIC's controls for safeguarding sensitive information in resolution plans submitted under the Dodd-Frank Act, and a review of cyber attack risks at FDIC-supervised institutions, all of which we will discuss in an upcoming semiannual report.

As we continue to move forward in a post-crisis environment, we are closely examining our own internal operations, workload, and resource needs, in light of lessons learned during the crisis and the changing FDIC environment of today. We have examined the Corporation's performance goals and, through ongoing dialogue with corporate officials, have come to better understand the corporate priorities that drive the daily operations of the FDIC. While some risks to the Corporation's success have subsided as the economy has improved, new threats can emerge, and we are carefully planning those projects that will add the most value to the FDIC and contribute to the successful accomplishment of its mission.

In April, the FDIC OIG marked its 25th anniversary. On March 14, 1989, an FDIC Board resolution recognized that the Inspector General Act Amendments of 1988 required the Corporation to establish an OIG with an Inspector General (IG) who functions under the general supervision of the Chairman, and established that position as of April 17. The FDIC's former Office of Corporate Audits and Internal Investigations (OCAII) was redesignated the OIG. The Director of OCAII became Inspector General, and the incumbent Director Robert Hoffman was designated Acting IG and then IG. Mr. Hoffman retired in 1993 and James Renick was selected by Acting Chairman Andrew "Skip" Hove to serve as IG. In 1993, the Congress designated the IG position at the FDIC as a Presidential appointment, and Mr. Renick was named as Acting IG. On April 29, 1996, Gaston L. Gianni, Jr. became the FDIC's first IG appointed by the President. Jon Rymer was sworn in as the second presidentially appointed IG on July 5, 2006 and resigned to become the Department of Defense IG on September 27, 2013. I have been honored to follow these fine public servants in leading the office as Acting IG following Mr. Rymer's appointment to his new post.

As we acknowledge this 25th anniversary, we are grateful to all of those who have played a part in the evolution of our office. We look to the future with pride and renewed commitment to carrying on the mission of the OIG by ensuring economy, efficiency, effectiveness, and integrity in FDIC programs and operations. We appreciate the continued support of FDIC senior leadership and the Congress as we do so.

Fred W. Gibson, Jr.
Acting Inspector General

April 2014

Table of Contents

1 **Acting Inspector General's Statement**

4 **Acronyms and Abbreviations**

5 **Highlights and Outcomes**

10 **Strategic Goal Areas**

- 10 **Goal 1: Supervision**
  Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly
- 23 **Goal 2: Insurance**
  Help the FDIC Maintain the Viability of the Insurance Fund
- 25 **Goal 3: Consumer Protection**
  Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy
- 30 **Goal 4: Receivership Management**
  Help Ensure that the FDIC Efficiently and Effectively Resolves Failing Banks and Manages Receiverships
- 33 **Goal 5: Resources Management**
  Promote Sound Governance and Effective Stewardship and Security of Human, Financial, Information Technology, and Physical Resources
- 39 **Goal 6: OIG Resources Management**
  Build and Sustain a High-Quality OIG Staff, Effective Operations, OIG Independence, and Mutually Beneficial Working Relationships

47 **Cumulative Results** (2-year period)

48 **Reporting Requirements**

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

52 **Appendix 2**
Information on Failure Review Activity

54 **Appendix 3**
Peer Review Activity

56 **Congratulations and Farewell**

Acronyms and Abbreviations

BPO	Business Process Operations
CEO	Chief Executive Officer
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CSDO	collateral secured debt obligation
DCP	Division of Depositor and Consumer Protection
DIF	Deposit Insurance Fund
DIT	Division of Information Technology
DOA	Division of Administration
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
Fidelity	Fidelity National Information Services, Inc.
Fiserv	Fiserv Federal Systems, Inc.
FISMA	Federal Information Security Management Act
FRB	Board of Governors of the Federal Reserve System
GFRS	Governmentwide Financial Report System
GPRA	Government Performance and Results Act of 1993
IG	Inspector General
IRS-CI	Internal Revenue Service-Criminal Investigation
IT	Information Technology
NCIJTF	National Cyber Investigative Joint Task Force
OCC	Office of the Comptroller of the Currency
OCFI	Office of Complex Financial Institutions
OIG	Office of Inspector General
OMB	Office of Management and Budget
OTS	Office of Thrift Supervision
RMS	Division of Risk Management Supervision
RMS-CFI	RMS Complex Financial Institutions Group
SAR	Suspicious Activity Report
SIFI	systemically important financial institution
SIGTARP	Special Inspector General for the Troubled Asset Relief Program

Highlights and Outcomes

The OIG works to achieve five strategic goals that are closely linked to the FDIC's mission, programs, and activities, and one that focuses on the OIG's internal business and management processes. These highlights show our progress in meeting these goals during the reporting period. A summary of our completed work, along with references to selected ongoing assignments is presented below.

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 report on the FDIC's implementation of systemic resolution responsibilities under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), making six recommendations to better position the FDIC to face future challenges associated with the Dodd-Frank Act. We also completed four 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 after December 31, 2013, and determined whether unusual circumstances existed that would warrant an in-depth review in those cases.

Ongoing audit and evaluation work in this goal area at the end of the reporting period included an evaluation of the financial regulatory agencies' programs for pursuing enforcement actions and professional liability claims that we are conducting jointly with other financial regulatory OIGs; an audit of the FDIC's response to Bank Secrecy Act and anti-money laundering concerns identified at FDIC-supervised institutions; and an evaluation of the FDIC's supervisory approach to cyber attack risks.

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 combated 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 former chairman and chief executive officer of Summit Bank, Burlington, Washington, was sentenced to 3 years in prison to be followed by 2 years of supervised release for falsifying regulatory documents. He was also barred from working in a federally insured institution. In another case, seven former bank officials of First National Bank of Savannah, Savannah, Georgia, pleaded guilty to a long-running, complex scheme that contributed to the failure of the bank. A former vice president for commercial lending at Mutual Bank, Muncie, Indiana, was sentenced to 33 months in prison, followed by 24 months of supervised release. For his role in a multi-million dollar bank and wire fraud conspiracy, a former Raleigh, North Carolina, real estate developer was sentenced to 327 months in prison to be followed by 60 months of supervised release. He was also ordered to pay nearly $12 million in restitution.

Also of note during the reporting period were several successful mortgage fraud cases. In one case, two businessmen and an attorney each received stiff sentences. One was sentenced to 108 months in prison and ordered to pay restitution of $8.8 million. Another was sentenced to 24 months in prison and ordered to pay $5.3 million in restitution. The attorney, a former mortgage loan officer, was sentenced to one year and a day in prison, with restitution of $1.9 million ordered.

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 strengthened our process for regular coordination of enforcement action matters with the Legal Division and RMS, a step that continues to be mutually beneficial. (See pages 10-22.)

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 prevent future losses to the insurance fund by way of findings and observations that can help to prevent future failures, and the deterrent aspect of investigations and the ordered restitution that may help to mitigate an institution's losses and losses to the Deposit Insurance Fund. (See pages 23-24.)

Strategic Goal 3: Consumer Protection

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

We completed our audit related to the FDIC's actions to address consumer protection violations and deficiencies. That audit determined that the FDIC's actions in this regard complied with applicable policies, procedures, and guidelines, and that in general, the regional offices were consistently handling such actions. However, we made four recommendations to improve the FDIC's controls over these activities, with which management concurred. Additionally, we coordinated with OIG counterparts on an assignment to examine the progress that the prudential regulators and the Consumer Financial Protection Bureau have made in establishing coordination for the many consumer protection responsibilities that the various parties carry out.

Our Office of Investigations also supports consumer protection through its work. For example, during the reporting period, as a result of an investigation that we have reported on in the past, a Houston businessman was sentenced to 15 years in prison for his role in a fraudulent investment scheme to steal about $1 million from elderly investors. As part of the scheme, his salesmen sold unregistered securities – collateral debt obligations – falsely claiming they were fully insured by either the FDIC or Lloyd's of London.

Also of note, our Electronic Crimes Unit responded to instances where fraudulent emails purportedly affiliated with the FDIC were used to entice consumers to divulge personal information and/or make monetary payments. Working with the Corporation's Division of Information Technology, 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 130 such inquiries during the past 6-month period. (See pages 25-29.)

Strategic Goal 4: Receivership Management

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

We did not complete assignments in this goal area during the reporting period. However, as of the end of the reporting period, we were planning two new assignments involving receivership management activities. In the first one, we are conducting preliminary research related to the FDIC's controls for identifying securing, and disposing of personally identifiable information in owned real estate properties. In the second assignment, we are examining the FDIC's controls over receivership-related taxes.

We would also note that in connection with the FDIC's new resolution authority for systemically important financial institutions, the 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. (See pages 30-32.)

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 our review of the FDIC's receivership basic ordering agreements for business process operations services. We also completed work in connection with the FDIC's purchase card program and made eight recommendations to strengthen internal controls. We conducted our annual Federal Information Security Management Act of 2002 evaluation of the FDIC's information security program and made 15 recommendations to improve the Corporation's information security controls and practices. We coordinated with FDIC management in the FDIC's data submissions for the governmentwide financial reporting system. Lastly, in connection with the Dodd-Frank Act, we issued the results of our final coordinated review of the status of the implementation activities of the Joint Implementation Plan prepared by the Board of Governors of the Federal Reserve System, the FDIC, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

At the end of the reporting period, we were completing work in the areas of information technology project management, controls for safeguarding sensitive information submitted under the Dodd-Frank Act, and an evaluation of the FDIC's personnel security and suitability program.

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 ethics officials, as warranted. (See pages 33-38.)

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 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. On an office-wide level, we re-examined and updated our policies and procedures and enhanced our records management and disposition activities. We provided our Fiscal Year 2015 budget to interested Congressional Committees. This budget reflects $34.6 million to support 130 full-time equivalents, no increase from our Fiscal Year 2014 request.

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*. In that connection, we held a training conference for all audit and evaluation staff to ensure a thorough understanding of revised policies and procedures and use of TeamMate as an assignment tool. 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 or pursuing professional certifications. Our mentoring program continued to further develop a strong cadre of OIG resources. We supported OIG staff members taking FDIC leadership training courses. We also employed an intern on a part-time basis to promote the intern's professional development and assist us in our work. Our Workplace Excellence Group met regularly to help foster excellence in OIG operations.

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; and 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, Investigations Committee, and Council of Counsels to the IGs. 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 submitted the OIG's annual assurance statement to the FDIC Chairman regarding our efforts to meet internal control requirements. We analyzed the Corporation's 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 areas that we identified as management and performance challenges facing the Corporation for inclusion in its annual report. (See pages 39-46.)

Significant Outcomes October 1, 2013 – March 31, 2014	
Audit and Evaluation Reports Issued	**7**
Questioned Costs and Funds Put to Better Use	**0**
Nonmonetary Recommendations	**37**
Investigations Opened	**33**
Investigations Closed	**51**
OIG Subpoenas Issued	**11**
Judicial Actions:	
Indictments/Informations	**56**
Convictions	**49**
Arrests	**39**
OIG Investigations Resulted in:	
Fines of	**$ 253,000**
Restitution of	**492,195,944**
Asset Forfeitures of	**16,865,312**
Total	**$ 509,314,256**
Cases Referred to the Department of Justice (U.S. Attorney)	**28**
Cases Referred to FDIC Management	**1**
Proposed Regulations and Legislation Reviewed	**5**
Proposed Draft FDIC Policies Reviewed	**12**
Responses to Requests Under the Freedom of Information Act	**13**

Strategic Goal 1

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 insured depository institutions. The FDIC is the primary federal regulator for approximately 4,300 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. Historically, the Department of the Treasury [the Office of the Comptroller of the Currency (OCC) and the Office of Thrift Supervision (OTS)] or the FRB supervised other banks and thrifts, depending on the institution's charter. The winding down of the OTS under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) resulted in the transfer of supervisory responsibility for about 60 state-chartered savings associations to the FDIC. About 670 federally chartered savings associations were transferred to the OCC. As insurer, the Corporation also has back-up examination and back-up enforcement authority to protect the interests of the Deposit Insurance Fund (DIF) for 2,500 national banks, state-chartered banks that are members of the FRB, and those savings associations now regulated by the OCC.

The examination of 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 determine 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. Part 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.

The passage of the Dodd-Frank Act brought about significant organizational changes to the FDIC's supervision program. In April 2013, the monitoring function for systemically important financial institutions (SIFIs) 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). According to RMS, the institutional knowledge and analysis associated with the RMS-CFI Group are relevant to OCFI's 165(d) plan reviews, orderly liquidation, and international functions; thus, collaboration across OCFI and the RMS-CFI Group will continue in order to further integrate these groups going forward. 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.

Prior to passage of the Dodd-Frank Act, in the event of an insured depository institution failure, the Federal Deposit Insurance (FDI) Act required the cognizant OIG to perform a review when the DIF incurs a material loss. Under the Federal Deposit Insurance Act (FDI Act), a loss was considered material to the insurance fund if it exceeded the greater of $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 occur 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 federal regulator of the institution. The Department of the Treasury OIG and the OIG at the FRB perform reviews when their agencies are the primary federal 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.

While the OIG's audits and evaluations address various aspects of the Corporation's supervision and examination activities, 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 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'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, cyber fraud, identity theft, and anti-phishing working groups. Additionally, when possible, the OIG engages in industry and other professional outreach efforts to keep financial institutions and others informed on 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 2014 performance goals** are 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 goal, we issued our review of the FDIC's progress in implementing systemic resolution authorities under the Dodd-Frank Act. Additionally, as of the end of the reporting period, several key assignments were ongoing. Specifically, we were reviewing the FDIC's enforcement actions and professional liability claims against institution-affiliated parties and individuals. We were examining the FDIC's program for monitoring compliance with Bank Secrecy Act and anti-money laundering requirements. In light of increased cyber attacks against financial institutions, we were also evaluating the FDIC's supervisory approach to cyber attack risks.

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 four failed bank reviews and had one material loss review underway as of the end of the reporting period. Our failed bank review activity for the reporting period is presented in Appendix 2.

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 described below. As in the past, we also discuss several of our mortgage-fraud related investigations. Importantly, our results would not be possible without the collaboration and assistance of our colleagues at the FDIC and our law enforcement partners throughout the country.

The FDIC's Progress in Implementing Systemic Resolution Authorities

Among other things, the Dodd-Frank Act gave the FDIC broad new authorities to mitigate the risk of SIFIs to the financial stability of the United States and, if necessary, to effect an orderly liquidation. The ability to mitigate risk and resolve SIFIs is critical to fulfilling the FDIC's primary mission of upholding public confidence in the nation's financial system. For that reason, the FDIC Chairman requested that the FDIC OIG review the Corporation's progress in implementing its systemic resolution authorities under the Dodd-Frank Act. We issued the results of our review in November 2013. The objective of our work was to determine the progress made by the FDIC in implementing the Dodd-Frank Act authorities associated with monitoring SIFIs, and resolving one, should that be necessary.

Title I of the Dodd-Frank Act provides tools for regulators to impose enhanced supervision and prudential standards on SIFIs. Title II of the Dodd-Frank Act includes a new orderly liquidation authority that can be invoked when the liquidation of a financial company under the Bankruptcy Code or other applicable law would have serious adverse effects on financial stability in the United States. In August 2010, the FDIC's Board of Directors (FDIC Board) established the OCFI to serve as the focal point for implementing the Corporation's systemic resolution authorities. The FDIC Board intended for OCFI to coordinate with other FDIC divisions and offices for critical expertise and support in certain functional areas to implement the Corporation's systemic resolution authorities.

We reported that the FDIC had made significant progress over the past 3 years towards implementing its systemic resolution authorities under the Dodd-Frank Act. Among other things, the FDIC had:

- Issued a joint regulation and met established timeframes for completing reviews of resolution plans submitted by covered financial companies,
- Entered into agreements with certain foreign regulatory authorities to promote cross-border cooperation, and
- Developed a single-point-of-entry resolution strategy that could be implemented if the exercise of the Title II orderly liquidation authority becomes necessary.

While these accomplishments were notable, we pointed out that more work needed to be done to establish a robust corporate-wide capability for this critical responsibility. In this regard, we made six recommendations to the FDIC Chairman that were intended to better position the FDIC to face future challenges and successfully carry out its systemic resolution authorities under the Dodd-Frank Act. In general, the recommendations were aimed at enhancing the FDIC's long-term strategic planning efforts, strengthening coordination among FDIC divisions, and building out OCFI's infrastructure to support systemic resolution activities.

In responding to our report, the FDIC Chairman concurred with all six of the report's recommendations. We will continue to monitor the FDIC's progress in fully implementing these actions and will re-evaluate the Corporation's readiness, as warranted. We would also note that we are conducting a risk assessment of the FDIC's Dodd-Frank Act-related activities to identify other areas of possible risk that may warrant OIG review.

Successful OIG Investigations Uncover 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.

A number of our cases during the reporting period involve 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 individuals involved in commercial lending activities were also implicated in a number of our cases. The OIG's success in all such investigations contributes to ensuring the continued safety and soundness of the nation's banks.

Community Banker Sentenced to 3 Years in Prison for Falsifying Regulatory Documents

On November 15, 2013, the former chairman and chief executive officer (CEO) of Summit Bank, Burlington, Washington, was sentenced to serve 36 months in prison to be followed by 2 years of supervised release. In addition, as part of his plea deal, the former bank executive was barred from working in a federally insured institution and has already paid a civil monetary penalty of $300,000. The former chairman and CEO of Summit Bank and his son, former president, director, and chief credit officer of the bank, were charged in August 2013 in a one-count criminal information with filing a false Call Report, and both subsequently pleaded guilty to the charge. Summit Bank failed on May 20, 2011 and the estimated loss to the FDIC as a result of the failure is $15 million.

Summit Bank was a small community family-owned bank in Skagit County, Washington, run by the father and son. Summit Bank began running into difficulties when the economy and real estate market took a downturn in 2008, resulting in many borrowers becoming delinquent in their loan payments. In order to disguise the true amount of the past-due loans from regulators, the two orchestrated multiple schemes to make the loans appear to be current so that they did not have to be reported on the quarterly Call Reports used by regulators to monitor the health and soundness of banks.

In his plea agreement, the former chairman and CEO admitted that between 2009 and 2011, he caused the bank to undertake financial transactions related to past-due loans, which concealed the overdue loans in the quarterly reports that went to the FDIC, essentially hiding millions of dollars in loans that were past due, and causing the bank to appear financially healthier than it actually was. For example, in one report on June 30, 2010, the Bank reported past-due loans of approximately $6 million in outstanding loans, payments on which were past-due for 30 or more days. In truth, the bank had at least $13 million in outstanding loans, payments on which were past due for 30 or more days.

The methods used by the father and son to make loans appear to be current at the end of each reporting period included overdrawing borrowers' checking and savings accounts to make loan payments, granting change in terms agreements on past-due loans extending payments, giving nominee loans to family members with the proceeds going towards past-due loan payments, taking collateral for other loans and using it to make loan payments on the past-due loans, taking payments intended for other loans and misapplying them to the past-due loans, advancing on other loans to make the payments

on the past-due loans, and lying to the Board of Directors about the true payment history of past-due loans in order to get change in terms agreements approved. Many of these schemes were carried out without the knowledge or consent of the borrowers.

Source: *This investigation was initiated based on information provided by the FDIC Legal Division and RMS.*
Responsible Agencies: *This investigation was conducted by the FDIC OIG and the Federal Bureau of Investigation (FBI). This case is being prosecuted by the U.S. Attorney's Office for the Western District of Washington.*

Seven Former Bank Officials Plead Guilty in Loan Fraud Scheme

On January 21, 2014, the former city president of the Tybee Island branch and a commercial loan officer of First National Bank of Savannah, Savannah, Georgia, pleaded guilty to two counts of bank fraud for his role in a complex bank fraud scheme. He and six other former bank officers were charged with a long-running conspiracy and fraud scheme that contributed to the demise of First National Bank of Savannah, which failed on June 25, 2010.

The former commercial loan officer was the seventh and final former bank officer to plead guilty in this case. The other six former officers, who pleaded during the period from October 25, 2013 through January 17, 2014, were the president and CEO; executive vice president and chief financial officer; vice president and chief credit officer; city president (Richmond Hill Branch) and commercial loan officer; senior vice president and commercial loan officer; and city president and senior lending officer.

According to the allegations in the indictment, as First National Bank of Savannah's financial condition began to deteriorate, the defendants schemed to hide from the bank, members of the bank's Board of Directors, and federal regulators millions of dollars in non-performing loans. They accomplished the scheme by unlawfully loaning money to unqualified nominees to make interest and other payments on other non-performing loans; enticing others to take over non-performing loans with hidden promises, side deals and other terms unfavorable to First National Bank of Savannah; and recruiting other banks to fund non-performing loans based upon fraudulent misrepresentations about the quality of the loans. To assist in their scheme, the defendants falsified and fabricated numerous bank documents and records.

Source: *U.S. Secret Service.*
Responsible Agencies: *This is a joint investigation conducted by the FDIC OIG, Board of Governors of the Federal Reserve System OIG, Department of the Treasury OIG, and the U.S. Secret Service. The case is being prosecuted by the U.S. Attorney's Office for the Southern District of Georgia.*

Former Bank President Pleads Guilty

On October 11, 2013, the former president, Bank of Billings, Billings, Michigan, pleaded guilty to a criminal information in which he was charged with bank fraud and money laundering. He was taken into custody following his court appearance.

Beginning in approximately May 2011 and continuing until he was suspended in May 2012, the former bank president engaged in a scheme to defraud and embezzle funds from the Bank of Billings. As part of the scheme, he caused the bank to grant loans in nominee names and kept the proceeds for himself. He also added debt to loans without the borrower's knowledge and converted the additional funds to his own use. In addition, he advanced funds on bank customers' lines of credit, used a bank credit card, and caused the bank to issue cashier's checks, all of which were converted to his own use. His scheme defrauded the Bank of Billings of approximately $413,905.

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

Former Vice President for Commercial Lending Sentenced for Bank Fraud

On October 29, 2013, the former senior vice president for commercial lending, MutualBank, Muncie, Indiana, was sentenced for bank fraud. She was sentenced to serve 33 months in prison to be followed by 24 months supervised release and was ordered to pay $249,390 in restitution.

In May 2012, MutualBank management became aware of discrepancies concerning several new commercial loans and wire transfers that the former vice president had initiated. A review of the transactions disclosed that false loans were established along with several bogus checking accounts. She used proceeds from the false loans to create three cashier's checks, totaling $590,000, with which she purchased a lake house in Michigan for her personal use. A forensic review of all of her lending activity determined she had used several other false lines of credit. From June 2011 to June 2012, she created five other false lines of credit whose proceeds went to the benefit of other family members, friends, and to refinance her own debts. The fraudulent transactions totaled $1,009,490.

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

Former Branch Manager of Citizens Bank of Pennsylvania Sentenced

On March 27, 2014, a former branch manager of Citizens Bank of Pennsylvania was sentenced to serve 3 months in prison to be followed by 3 years of supervised release. He was also ordered to pay $4,179 in restitution.

The former branch manager opened multiple bank accounts in a customer's name without permission. He used these accounts to access customers' overdraft lines of credit. He then drafted e-checks and conducted online transfers from the victims' accounts to shell companies he controlled. He used the funds for personal gain.

Source: *Citizens Bank of Pennsylvania.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, U.S. Secret Service, and Social Security Administration OIG. The case is being prosecuted by the U.S. Attorney's Office for the Eastern District of Pennsylvania.*

Former Branch Manager Pleads Guilty to Larceny Charges

On March 5, 2014, a former branch manager of Integrity Bank, Camp Hill, Pennsylvania, pleaded guilty to bank larceny charges.

Between May 14, 2012, and March 26, 2013, the former branch manager stole funds by making four unauthorized withdrawals from the time deposit account of an elderly customer. She withdrew the funds and turned them into cashier's checks and used the money for her personal use, including paying her taxes, funding an investment account, and for other personal matters. A total of $125,815 was stolen. She resigned from the bank on March 28, 2013.

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

Former Bank Manager Sentenced

On February 18, 2014, a former bank teller manager at First Midwest Bank of Poplar Bluff, Poplar Bluff, Missouri, was sentenced to serve 27 months in prison to be followed by 5 years of supervised release for her role in an embezzlement scheme. In addition, she was ordered to pay $413,153 in restitution.

Beginning in January 2007 and continuing through at least March 2013, the former manager abused her position as a bank employee by embezzling $397,265 in cash from the bank vault at First Midwest Bank of Poplar Bluff and used the money for her own personal benefit. To further her scheme to defraud the bank, she manipulated the bank's records and created fraudulent cash audit reports to try and hide the embezzlement.

Source: *FDIC 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 Missouri – Cape Girardeau.*

Former Teller Sentenced for Embezzlement

On March 21, 2014, a former head teller at Volunteer State Bank, Portland, Tennessee, was sentenced to serve 21 months in prison, followed by 2 years of supervised release and ordered to pay restitution of $264,009. The Court also ordered forfeiture of $264,010 and barred her from working for a financial institution without prior approval of the Court and the FDIC. She previously pleaded guilty to embezzlement on January 3, 2014.

The former teller was employed at Volunteer State Bank from September 5, 2007 to June 4, 2013, and served as the head teller for the Gallatin branch. As head teller, she was responsible for the cash vault and for balancing the teller currency dispenser. An audit conducted while she was on vacation in May 2013 revealed a cash shortage of $264,010. She was able to avoid detection during prior audits by creating false journal entries and moving the shortage between the vault and the teller currency dispenser.

The former teller ultimately admitted she took the money and falsified journal entries to avoid detection.

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

Former Cashier Sentenced for Misapplication

On October 9, 2013, a former cashier at Brimfield Bank, Brimfield, Illinois, was sentenced after previously pleading guilty to a criminal Information through which she was charged with misapplication. The former cashier was sentenced to serve 21 months in prison to be followed by 60 months of supervised release and was ordered to pay $197,620 in restitution.

From 2004 until October 2012, the former cashier embezzled approximately $200,000 from accounts at Brimfield Bank. She took funds from three separate demand deposit accounts maintained at Brimfield Bank and purchased cashier's checks or bank checks that were used for her benefit or the benefit of her children.

Source: *This investigation was initiated based on information provided by the FDIC RMS, and FBI.*
Responsible Agencies: *This is a joint investigation with the FDIC OIG and the FBI. The case was prosecuted by the U.S. Attorney's Office for the Central District of Illinois.*

Former Raleigh Real Estate Developer Sentenced in Multi-Million Dollar Bank and Wire Fraud Conspiracy

On January 15, 2014, a real estate developer was sentenced for his role in a bank and wire fraud conspiracy. He was sentenced to serve 327 months in prison to be followed by 60 months of supervised release. He was also ordered to pay restitution of $11,946,739.

Beginning in 2002 and continuing until 2006, the developer and others conspired to make false and fraudulent statements on multiple loan documents, HUD-1 settlement statements, and residential real estate appraisal reports associated with properties that he or one of his affiliated investors or entities purchased or sold. The developer operated various real estate companies, including but not limited to Alpine Properties, LLC, and Webb Builders, LLC. Through these and other companies, the developer promised investors financial gain through the purchase, renovation, and resale of distressed residential real estate primarily in low-income neighborhoods. He also orchestrated a scheme whereby property appraisal reports fit within a valuation range that he had designated. Generating the false appraisal documents enabled him, Alpine Properties, LLC, and other co-conspirators to profit and receive loan proceeds in connection with the purchase and sale of the properties. The scheme resulted in lenders, including Crescent State Bank, Raleigh, North Carolina, issuing loans that ultimately defaulted.

Source: *HUD OIG.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, HUD OIG, U.S. Postal Inspection Service, and the FBI. The case was prosecuted by the U.S. Attorney's Office for the Eastern District of North Carolina.*

Real Estate Developer Convicted

On October 17, 2013, a real estate developer was convicted by a jury on 13 counts of bank fraud, conspiracy, misapplication, wire fraud, conspiracy to commit money laundering, and money laundering. On December 5, 2012, the developer was charged for his role in a lot loan program/builder bailout scheme, where he aided and abetted various borrowers to fraudulently obtain loans from banks, including the Bank of Asheville and Pisgah Community Bank, to fund the ailing Seven Falls Golf and River Club Development in Hendersonville, North Carolina. The Bank of Asheville failed on January 21, 2011. Pisgah Community Bank failed on May 10, 2013. Nine defendants, including three bankers, were convicted for their roles in this major bank fraud case. The former Pisgah Community Bank president and the former Bank of Asheville president were both convicted in the scheme that led to the failure of both banks.

Seven Falls was a residential development that the real estate developer owned in Henderson County, North Carolina. He purchased the property in 2006 with a $25 million loan from the National Bank of South Carolina. In 2007, he sold approximately 70 lots in Seven Falls for between $250,000 and $650,000 each. By 2008, he began running out of money and needed a new source of funds. The developer had numerous outstanding loans from the Bank of Asheville, and he was near his statutory lending limit with the bank. From 2008 through 2010, he, along with other co-conspirators, developed the lot loan program and other schemes whereby they recruited straw borrowers to purchase lots and other various properties via bank loans, the proceeds of which would be turned over to the conspirators. He also wrote several large NSF checks to the Bank of Asheville to cover payments on nominee loans exposing the bank to prolonged risk. Most of the loans were from Bank of Asheville and Pisgah Community Bank. The aggregate fraud, which exceeded $23 million, significantly contributed to the failure of the two banks.

Source: *This investigation was initiated based on information provided by the FDIC RMS and the North Carolina Commissioner of Banks.*
Responsible Agencies: *This is a joint investigation by the FBI, IRS-CI, and FDIC OIG. The case was prosecuted by the U.S. Attorney's Office for the Western District of North Carolina.*

Albuquerque Real Estate Project Manager Sentenced

On December 11, 2013, a former project manager employed by the former owner of the Blue Dot Corporation was sentenced to serve 3 months in prison to be followed by 3 years of supervised release, to include 9 months of home detention. He was also ordered to pay restitution to the FDIC in the amount of $560,129.

During the period 2005 to 2006, the former business owner obtained approximately $23 million in construction loans from Columbian Bank and Trust, Overland Park, Kansas, and First Financial Credit Union in order to finance three Albuquerque, New Mexico, commercial projects. The former project manager and the former business owner used their knowledge of the construction draw process to fraudulently obtain project funds for work not performed. The money was used to fund various business-related interests and augment both of their personal lifestyles. Their activities resulted in the misappropriation of more than $1 million in fraudulent draws from Columbian Bank and Trust and First Financial Credit Union related to the subject projects. Subsequent foreclosure on the projects resulted in losses of approximately $17.5 million to the victim institutions and the FDIC.

Source: *FDIC Division of Resolutions and Receiverships (DRR) Failing Bank Report.*
Responsible Agencies: *The FDIC OIG conducted this investigation with assistance from the FBI and IRS-CI. The case was prosecuted by the U.S. Attorney's Office for the District of New Mexico.*

Commercial Loan Customer Pleads Guilty

On January 17, 2014, a commercial loan customer pleaded guilty to one count of bank fraud for his role in a commercial loan fraud scheme. He is scheduled to be sentenced on April 15, 2014.

In September 2006, the loan customer, acting through Riverside Square, LLC, obtained a $13.5 million commercial loan to finance the construction of Riverside Square, LLC. According to the indictment, between January 2007 and June 2008, he fraudulently obtained more than $1 million in loan proceeds from Amcore by submitting false contractor statements, waiver of liens, and contract invoices that requested funds purportedly for permits, construction work, and consulting work for the development. To obtain funds from the bank loan, he allegedly submitted false contractor statements to the bank in which he verified that subcontractors and his company were owed funds for work performed on Riverside Square. The former loan customer submitted, and caused the submission of, false lien waivers and invoices for work performed to the title company, which was designated by Amcore to keep and disburse funds for the project. After these documents were submitted, the bank authorized the title company to disburse funds to the customer and the subcontractors. In one instance, in June 2008, he allegedly obtained an additional $25,000 by altering an invoice from a subcontractor by changing a "6" to an "8" and a "3" to an "8" so that the claimed amount of $163,700 instead read $188,700.

Source: *FDIC DRR.*
Responsible Agencies: *This case is being investigated by the FDIC OIG and is being prosecuted by the U.S. Attorney's Office for the Northern District of Illinois.*

Businessman and Son Plead Guilty in Multi-Million Dollar Commercial Loan Fraud Scheme

On January 10, 2014, a father and son, who were CEO and chief financial officer, respectively, of Quality Concepts, LLC, pleaded guilty to one count of conspiracy to commit bank fraud. In addition, the former chief financial officer pleaded guilty to one count of money laundering.

The two, through another company owned by the father, QC Manufacturing, LLC, applied for and received a $5,950,000 commercial loan from Country Bank, Aledo, Illinois, to acquire and rehabilitate Casey Tool and Machine, Casey, Illinois. The rehabilitation portion of the loan was $1.7 million and required the defendants to submit sworn statements and subcontractor waivers. On five separate occasions from May 2010 through June 2010, the co-conspirators submitted false sworn statements to Country Bank. The sworn statements included requests for funding for items that were never completed or were completed for less than what was requested. Country Bank relied upon the falsified sworn statements and funded the $1.7 million in draw requests. The loan was guaranteed by the United States Department of Agriculture and was funded through the American Recovery and Reinvestment Act.

Source: *This investigation was initiated based on a referral from the FBI.*
Responsible Agencies: *This is a joint investigation conducted by the FDIC OIG, FBI, IRS-CI, United States Department of Agriculture OIG, with assistance from the U.S. Postal Inspection Service and the Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP). The case is being prosecuted by the U.S. Attorney's Office for the Central District of Illinois.*

New Jersey Couple Plead Guilty to Conspiracy, Bankruptcy Fraud, and Tax Offenses

A husband and wife pleaded guilty to conspiring to commit mail fraud, wire fraud, loan application fraud, and bank fraud from 2001 through 2008. They admitted to obtaining money from banks and lenders for purchases, home equity lines of credit, and construction loans by means of false and fraudulent pretenses, such as the submission of false tax returns, false IRS form W-2s, false paystubs, and other documents during that time.

In a second scheme, the couple admitted to concealing multiple businesses and assets from the U.S. Bankruptcy Court in Newark, New Jersey. Specifically, they are alleged to have concealed income from a rental property, income from businesses run by the husband, and the wife's true income from a reality television show and related businesses. They also admitted to making false oaths related to the declarations of their true assets and income in their bankruptcy case.

Finally, the husband admitted to failing to file U.S. tax returns for tax years 2000 through 2008. During this timeframe, he failed to report over $1.2 million of income, which resulted in a loss of over $220,000 of tax revenue.

Source: *This investigation was based on a request for assistance from the U.S. Attorney's Office.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, IRS-CI, 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.*

Three Sentenced in Mortgage Fraud Scheme

On March 28, 2014, three individuals were sentenced for their roles in a mortgage fraud scheme. The first, a Houston businessman was sentenced to serve 108 months in prison to be followed by 3 years of supervised release, and ordered to pay restitution of $8,774,289. Another businessman was sentenced to serve 24 months in prison to be followed by 3 years supervised release, and ordered to pay restitution of $5,258,035. The third, an attorney and former mortgage loan officer was sentenced to serve 12 months and one day in prison, to be followed by 3 years of supervised release, and ordered to pay restitution of $1,870,850.

From November 2005 through October 2008, the three defendants obtained more than $17 million in fraudulent mortgage loans, with losses in excess of $2.5 million, from several Houston-area banks, including Fremont Investment & Loan, Brea, California. One of the businessmen fraudulently qualified straw borrowers for mortgage loans, established businesses with bank accounts to collect the loan proceeds, and paid co-conspirators. The other businessman located properties for sale and recruited straw borrowers. The former attorney and mortgage loan officer used her position with Mortgages First Real Estate Services to obtain fraudulent mortgage loans. As part of the conspiracy, the perpetrators developed a pyramid scheme to recruit straw buyers and, for a fee, purchase their credit and use their signatures to obtain area housing under the pretense of the properties being their primary residence. Following the initial purchase, other straw buyers were recruited to flip the property at inflated prices to cover the previous loan and cash out the loan differences for profit and financing purposes. Each recruited straw buyer was then coached to recruit friends and family for new loan application and borrowing activities.

Source: *FBI.*
Responsible Agencies: *The FDIC OIG conducted the investigation with assistance from the FBI. The case was prosecuted by the U.S. Attorney's Office for the Southern District of Texas.*

Sentencing in Mortgage Fraud Case

On March 22, 2014, a straw buyer recruiter who was also a landlord was sentenced for her role in a mortgage fraud scheme. She was sentenced to serve one year and one day in prison to be followed by 3 years of supervised release and was ordered to pay restitution of $485,250.

Between September 2005 and April 2011, another straw buyer recruiter, a closing attorney, a loan officer, and the straw buyer recruiter and landlord, conspired to commit wire fraud. As part of the scheme, the two recruiters promised to pay the straw buyers' monthly mortgage payments on five properties. The straw buyers were either paid or promised a lump sum by the two recruiters in exchange for purchasing the properties. The straw buyers were brought to the loan officer who did not collect any financial information from them yet submitted documents to American Brokers Conduit, Impac Funding, and WMC Mortgage with false information, including false employment verifications, false income verifications, inflated bank statements, false verification of rent statements, and false statements regarding the property being used as a primary residence. A closing attorney involved in the scheme then facilitated the closings. After the lenders wired the loan proceeds to the attorney's account, she did not disburse the loan proceeds in accordance with the HUD-1s. Instead, for example, several unauthorized payments were made directly to those involved in the scheme and some payments were made to the attorney herself and to her legal assistant.

All five of the properties are currently in default and are in various stages of foreclosure.

Source: *This investigation was initiated based on a referral from the FBI through the 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 Eastern District of New York.*

Update: Arrest of Fugitive Former Bank Director

In an unusual turn of events, on December 31, 2013, a former director of Montgomery Bank & Trust (MBT), Ailey, Georgia, was arrested following a routine traffic stop in Glenn County, Georgia. In July 2012, the former director was charged with bank fraud in the Southern District of Georgia; in January 2013, he was also charged with securities fraud and wire fraud in the Eastern District of New York. Prior to his arrest, the former director had last been seen in June 2012, at a ferry terminal in Key West, Florida. He disappeared after writing a letter to acquaintances and regulators that he had lost a large amount of money and that he planned to take his own life.

According to the Georgia indictment, in 2010, an investment group that he controlled before he became a bank director invested approximately $10 million in the failing MBT. He was subsequently made a director of MBT and was put in charge of investing the bank's capital. Over the next 18 months, he allegedly stole, misappropriated, and embezzled over $21 million from MBT. To conceal his fraud, the former director provided MBT officials with bogus account statements that falsely indicated the bank's capital was safely held in an account at a financial services firm.

According to the New York indictment, the former director had managed investment funds–PFG, LLC (PFG) and the Montgomery Growth Fund. Starting in or about June 2009, PFG raised approximately $40 million from approximately 115 investors from across the nation. The former director unsuccessfully invested PFG funds in various equity securities, options, and real estate, including farms in South America. To conceal his losses, he allegedly lied to his investors by posting fake account statements on a secure PFG Web site that fraudulently reflected fictitious assets and fabricated investment returns. Further, as a director of MBT, he invested some of the bank's capital, which he told the bank's management he would invest safely in U.S. Treasury securities. Instead, he lost much of the bank's money through risky investments in equity securities and options. He also embezzled MBT money to pay redemptions to some PFG investors.

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

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	Louisiana	New Jersey	Tennessee
Arizona	Maine	New Mexico	Texas
Arkansas	Maryland	New York	Utah
California	Massachusetts	North Carolina	Vermont
Colorado	Michigan	North Dakota	Virginia
Florida	Minnesota	Ohio	Washington
Georgia	Mississippi	Oklahoma	West Virginia
Illinois	Missouri	Oregon	Wisconsin
Iowa	Nebraska	Pennsylvania	Puerto Rico
Kansas	Nevada	South Carolina	District of Columbia
Kentucky	New Hampshire	South Dakota	

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	The Northern Virginia Real Estate Fraud Initiative Working Group, Manassas, Virginia; Maine Suspicious Activity Report (SAR) Review Team; Maryland Mortgage Fraud Task Force; the New England Mortgage Fraud Working Group; Concord New Hampshire and Boston Massachusetts SAR Review Meetings; Philadelphia Mortgage Fraud Working Group; DC National SAR Review Team.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force; Southern District of Florida Mortgage Fraud Working Group; Northern District of Georgia Mortgage Fraud Task Force; Eastern District of North Carolina Bank Fraud Task Force; Northern District of Alabama Financial Fraud Working Group.
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	Illinois Mortgage Fraud Working Group; Dayton 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.
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 Work Group, North Texas Mortgage Fraud Working Group, Eastern District of Texas Mortgage Fraud Task Force, Texas Attorney General's Residential Mortgage Fraud Task Force, Houston Mortgage Fraud Task Force, 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.

Strategic Goal 2

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.

Since year-end 2007, the failure of FDIC-insured institutions has imposed total estimated losses of more than $89 billion on the DIF. The sharp increase in bank failures over the past several years caused the fund balance to become negative. The DIF balance turned negative in the third quarter of 2009 and hit a low of negative $20.9 billion in the following quarter.

In the aftermath of the financial crisis, FDIC-insured institutions have continued to make steady progress. In light of such progress, the DIF balance has continued to increase, and as of December 31, 2013, the DIF balance was $47.2 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.

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. In addition to the FDIC's examination program, risk-management activities include approving the entry of new institutions into the deposit insurance system, off-site risk analysis, assessment of risk-based premiums, special 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. On-site supervision is augmented by coordination with other federal banking agencies, comprehensive quarterly off-site reviews, the Shared National Credit Program, and other off-site monitoring systems. Annual supervisory plans are developed for each state non-member bank with total assets greater than $10 billion. Supervisory Risk-Resolution Activities Plans are developed for each financial company with over $100 billion in total assets. According to RMS, this collaborative effort with OCFI includes an overview of each consolidated company's strategic direction, the appropriateness of the primary federal regulator's ratings, review of resolution activities, and a prioritization of the risks as well as an action plan to address these risks.

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 2014 performance goal** 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. For example, 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.

Strategic Goal 3

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

Consumer protection laws are important safety nets for Americans. The U.S. Congress has long advocated particular protections for consumers in relationships with banks. The following are but a sampling of Acts seeking to protect consumers:

- **The Community Reinvestment Act** encourages federally insured banks to meet the credit needs of their entire community.
- **The Equal Credit Opportunity Act** prohibits creditor practices that discriminate based on race, color, religion, national origin, sex, marital status, or age.
- **The Home Mortgage Disclosure Act** was enacted to provide information to the public and federal regulators regarding how depository institutions are fulfilling their obligations towards community housing needs.
- **The Fair Housing Act** prohibits discrimination based on race, color, religion, national origin, sex, familial status, and handicap in residential real-estate-related transactions.
- **The Gramm-Leach Bliley Act** eliminated barriers preventing the affiliations of banks with securities firms and insurance companies and mandates new privacy rules.
- **The Truth in Lending Act** requires meaningful disclosure of credit and leasing terms.
- **The Fair and Accurate Credit Transaction Act** further strengthened the country's national credit reporting system and assists financial institutions and consumers in the fight against identity theft.

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 is experiencing and implementing 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 (DCP), 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. Another important priority is financial literacy. 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. Common schemes range from identity fraud to Internet scams such as "phishing" and "pharming."

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 2014 performance goals** are 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 an audit to examine the Corporation's actions to address consumer protection violations and deficiencies. We also coordinated with 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 many consumer protection responsibilities that the various parties carry out.

As noted earlier, our investigative work involving misrepresentation of FDIC insurance or affiliation and protection of personal information supports this strategic goal area and we are reporting on one such case during the reporting period. Further, in response to an increase in the number of consumer inquiries in 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 this goal area are discussed below.

The FDIC's Actions to Address Consumer Protection Violations

We conducted an audit to determine whether the FDIC's actions to address consumer protection violations and deficiencies comply with applicable policies, procedures, and guidelines and the extent to which the actions are consistently handled by DCP's Regional Offices. We engaged the independent professional services firm of KPMG LLP to provide assistance on the audit.

By way of background, within the FDIC, DCP has primary responsibility for examining institutions for compliance with fair lending, privacy, and various other consumer protection laws and regulations. Examiners document the results of their work in compliance examination reports, which are provided to the institution's management and Board of Directors. Examiner recommendations and discussions with management generally result in the correction of identified violations and deficiencies. However, when such efforts are not successful, or when violations or deficiencies are significant, the FDIC may take stronger steps in the form of informal supervisory actions or formal enforcement actions against an institution or responsible individuals. Such actions can include the assessment of civil money penalties or orders to pay restitution to consumers who were harmed because of violations. The FDIC typically performs follow-up examinations or onsite visits within 12 months of completing an examination that assigns a "4" or "5" compliance rating.

DCP has developed a formal consultation process that requires officials in the Regional Offices and the Washington Office to consult on significant, unusual, and emerging supervisory matters, including supervisory actions, violations of certain laws and regulations, and weak compliance ratings. The consultation process is intended to help ensure appropriate, consistent, and timely consideration of such matters.

We found that the FDIC's actions to address the consumer protection violations and deficiencies that we reviewed generally aligned with applicable policies, procedures, and guidelines. In addition, compliance examination reports identified the specific laws and regulations that were violated, the nature and causes of the violations, the recommended corrective actions, and the responses of the institutions' management.

Further, follow-up examinations or visits were conducted timely, and civil money penalties that the FDIC issued were well supported and documented and included a legal opinion that addressed consideration of applicable laws, violations, mitigating factors, and monetary penalties.

While such results are positive, we found that the FDIC's compliance information systems used to record, track, and monitor consumer compliance activities did not always contain pertinent information on the following compliance activities:

- The basis for decisions on whether and what type of supervisory action should be taken,
- Restitution to consumers, and
- Consultations among DCP officials regarding proposed supervisory actions.

In some cases, this information was maintained outside of the FDIC's compliance information systems in memoranda and other documents. Recording and tracking key supervisory information in a consistent and centralized manner helps to ensure its reliability, reduces the amount of time and effort needed to locate information and respond to inquiries, and mitigates the risk associated with staff turnover. Such an approach also provides increased assurance of consistency in the supervision of institutions.

As for regional operations, DCP has established a number of internal controls to promote consistency among its Regional Offices in the handling of actions to address violations and deficiencies. Such controls include the Compliance Examination Manual, the Formal and Informal Action Procedures Manual, the National Review Examiner Manual, a consultation process, restitution tracking procedures, and the compliance examination

report review process. The FDIC also established the Case Review Committee and has issued guidance to examiners on consumer protection matters to help ensure a consistent supervisory approach. Further, the supervisory matters that we reviewed, including actions taken to address violations and deficiencies, generally appeared to be consistently handled by DCP's Regional Offices. However, we did note differences among DCP's regional consultation policies and procedures that the FDIC should consider as part of its initiative to update those procedures for consistency with recently-issued national consultation procedures.

Our report also includes an observation that DCP's guidance to examiners on assigning compliance ratings allows more flexibility than the definitions provided in the Uniform Interagency Consumer Compliance Rating System. DCP officials informed us that there have been high-level discussions among Federal Financial Institutions Examination Council participants about the need to clarify the Uniform Interagency Consumer Compliance Rating System ratings definitions.

We made four recommendations that are intended to improve DCP's internal controls for addressing consumer protection violations and deficiencies identified during compliance examinations. Management concurred with all four recommendations. With respect to the report's observation, the Director, DCP, plans to contact other agencies to discuss the matter.

Office of Investigations Works to Prevent Misrepresentations of FDIC Affiliation

Unscrupulous individuals sometimes attempt to misuse the FDIC's name, logo, abbreviation, or other indicators to suggest that deposits or other products are fully insured or somehow connected to the FDIC. Such misrepresentations induce the targets of schemes to trust in the strength of FDIC insurance or the FDIC name while misleading them as to the true nature of the investments or other offerings. Abuses of this nature not only harm consumers, they can also erode public confidence in federal deposit insurance. As discussed below, during the reporting period, a Texas man received a stiff sentence for his role in a scheme involving misrepresentation of FDIC affiliation that victimized senior citizens.

Houston Man Sentenced to 15 Years for Investment Scheme Involving Misuse of FDIC Symbol

On February 24, 2014, a Houston businessman was sentenced to serve 15 years in prison. He previously pleaded guilty on September 9, 2013, to a state charge of misapplication of fiduciary property in excess of $200,000.

The investigation revealed that the former businessman devised a fraudulent investment scheme and stole approximately $1 million from 10 investors. He used independent salesmen to advertise and sell unregistered securities referred to as collateral secured debt obligations (CSDOs). The salesmen falsely advertised FDIC-insured certificates of deposit paying high interest rates (above the actual market rate) in local newspapers. When investors responded to the advertisements, they were steered into the CSDOs. Investors were deceived into believing that the CSDOs were secure and fully insured by either the FDIC or Lloyd's of London. By the end of 2008, all the investors' money was gone, and analysis of the bank accounts revealed that the former businessman had spent the money on personal expenses such as house or rent payments, Mercedes car payments, meals at restaurants, cash withdrawals, and legal and accounting fees.

Source: *Enforcement Division of the Texas State Securities Board, the U.S. Attorney's Office, and the FBI.*
Responsible Agencies: *This is a joint investigation conducted by the FDIC OIG and FBI. The case was prosecuted by the Harris County District Attorney's Office.*

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 our last semiannual report, 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. During the reporting period, the ECU continued to investigate the source of the fraudulent communications and is now coordinating with other entities who may have been victimized by the same group of scammers.

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 130 such matters.

Strategic Goal 4

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 DRR'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.

- The **resolution process** involves valuing a failing federally insured depository institution, marketing it, soliciting and accepting bids for the sale of the institution, considering the least costly resolution method, determining which bid to accept, and working 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. Throughout the recent crisis, the FDIC was called upon to handle failing institutions with significantly larger numbers of insured deposits than it has dealt with in the past. The sheer volume of all failed institutions, big and small, has posed challenges and risks to the FDIC.

Under the Dodd-Frank Act, the FDIC was given new resolution authority for large bank holding companies and systemically important non-bank financial companies. 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. As noted earlier, OCFI works in concert with RMS, DRR, and the Legal Division in carrying out systemic resolution activities.

Franchise marketing activities are at the heart of the FDIC's resolution and receivership work. The FDIC pursues the least costly resolution to the DIF for each failing institution. Each failing institution is subject to the FDIC's franchise marketing process, which includes valuation, marketing, bidding and bid evaluation, and sale components. The FDIC is often able to market institutions such that all deposits, not just insured deposits, are purchased by the acquiring institution, thus avoiding losses to uninsured depositors.

Through purchase and assumption agreements with acquiring institutions, the Corporation has entered into shared-loss agreements (SLA). Since loss sharing began in November 2008, the Corporation had entered into 304 SLAs as of February 28, 2014. As of that same date, 290 of those SLAs were still active and 14 were terminated. The initial asset balance of the covered assets in these SLAs was $216.3 billion. The balance as of February 28, 2014 was $73.3 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 has entered into 35 structured sales transactions involving 43,315 assets with a total unpaid principal balance of about $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 January 31, 2014, DRR was managing 483 active receiverships with assets in liquidation totaling about $10.8 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.

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. As the number of financial institution failures continues to decline, the Corporation has made changes affecting resolution and receivership activities. The FDIC closed the West Coast Office and the Midwest Office in January 2012 and September 2012, respectively, and closed the East Coast Office in early April 2014. 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. Proposed authorized staff for 2014 was 916.

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 2014 performance goals** are 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, we began planning for two assignments in this area. In one, we are conducting preliminary research related to the FDIC's controls for identifying securing, and disposing of personally identifiable information in owned real estate properties. In the second assignment, we are examining the FDIC's controls over receivership-related taxes. Efforts of our ECU as they relate to bank closings support this goal and are described below.

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 the Failure of the First National Bank of Savannah, Savannah, Georgia

Over the past months, the ECU has played a key role in a very successful case that resulted in seven former bank officers pleading guilty to a long-running loan fraud scheme. (See write-up on First National Bank of Savannah earlier in this report.) The ECU provided invaluable assistance in establishing the involvement of the seven different defendants in this complex case. Much of the ECU's focus was on email traffic between the seven. Working closely with government prosecutors, the ECU searched voluminous electronic files to determine more precisely what emails were sent, opened, responded to, or forwarded, along with the timing of the various exchanges. Unraveling the various chains of communication was critical to developing evidence for prosecution purposes. In total, the ECU analyzed more than 317,000 emails.

The ECU further assisted by maintaining the bank's email server, file server, and banking system server after the main branch was officially closed. The former bank's IT manager helped the ECU set up these servers in an FDIC location, and the ECU accessed them for the prosecutors throughout the investigation to obtain electronic loan files, appraisals for various commercial properties, the exchange email database, bank employee user files, and other pertinent information.

As an additional challenge, about 4 months before the scheduled trial date, the banking system server crashed, so the ECU coordinated with the assuming bank to obtain a duplicate image of this particular server. The ECU was able to load the image on a forensic tower so that it was easily accessible to the prosecutors in establishing their case. In addition, the ECU set up the same virtual image on another computer so that this same information could be accessed by the defense attorneys in a separate secluded environment, as necessary.

Strategic Goal 5

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. As noted earlier, the FDIC closed the West Coast Office and the Midwest Office in January 2012 and September 2012, respectively, and closed the East Coast Office in early April 2014. 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.

To fund operations, in December 2013, the Board of Directors approved a $2.39 billion corporate operating budget for 2014, 10.9 percent lower than the 2013 budget. In conjunction with its approval of the 2014 budget, the Board also approved an authorized 2014 staffing level of 7,199 positions, down from 8,053 authorized at the time, a net reduction of 854 positions. This was the third consecutive reduction in the FDIC's annual operating budget, and the 2014 budget is the lowest annual budget since 2008.

The FDIC's operating expenses are paid from the DIF, and consistent with sound corporate governance principles, the Corporation's financial management efforts must continuously seek to be efficient and cost-conscious, particularly in a governmentwide environment that is facing severe budgetary constraints and other economic and fiscal uncertainties.

From an IT perspective, with heightened activity in the financial services industry and economy, the FDIC has engaged 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 Stability Oversight Council formed pursuant to the Dodd-Frank Act. FDIC systems contain voluminous amounts of critical data. The Corporation needs to protect against cyberthreats 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.

As we noted in our last semiannual report, in July 2013, the FDIC Chairman announced significant organizational changes in the FDIC's IT management and governance arena. Specifically, the FDIC separated the function of day-to-day management of the Division of Information Technology (DIT) from the role of broad oversight of information systems and security through the establishment of a separate Chief Information Officer (CIO). Given current IT developments and risks, the CIO role requires a full-time incumbent with broad strategic responsibility for IT governance, investments, program management, and information security. A new Acting CIO was named in 2013. Under the new organizational alignment, the CIO reports directly to the FDIC Chairman in fulfilling these responsibilities and will act as the Chairman's key advisor on IT and information security issues and concerns.

Additionally, under this new organizational alignment, the Director of DIT now reports to the CIO and will be responsible for managing the IT function at the FDIC and identifying and implementing effective and efficient technological solutions. Further, the reporting relationship of the Chief Information Security Officer and his branch changed from reporting within DIT to reporting directly to the CIO. This realignment will ensure that the Chief Information Security Officer is able to provide an independent perspective on security matters to the CIO and will ensure that the separate CIO position has the authority and primary responsibility to implement an agency-wide information security program.

Finally, a key component of overall corporate governance at the FDIC is the FDIC Board of Directors. Even as the financial system and economy continue to make steady progress in the aftermath of the financial crisis, the Board will likely face challenges in leading the organization, accomplishing the Chairman's priorities, and coordinating with the other regulatory agencies on issues of mutual concern and shared responsibility. Enterprise risk management is a related aspect of governance at the FDIC. Notwithstanding a stronger economy and financial services industry, the FDIC's enterprise risk management activities need to be attuned to emerging risks, both internal and external to the FDIC, and the Corporation as a whole needs to be ready to take necessary steps to mitigate those risks as changes occur and challenging scenarios present themselves.

To promote sound governance and effective stewardship and security of human, financial, IT, and physical resources, the **OIG's 2014 performance goals** are 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 five assignments in support of this goal area. We conducted a review of the FDIC's receivership basic ordering agreements for business process operations services. We also completed work in connection with the FDIC's purchase card program. We conducted our annual Federal Information Security Management Act of 2002 (FISMA) evaluation of the FDIC's information security program, and we coordinated with FDIC management in the FDIC's data submissions for the governmentwide financial reporting system. Finally, we joined the Treasury and FRB/Consumer Financial Protection Bureau OIGs in issuing our final joint review related to the transfer of OTS personnel and functions to the OCC, FRB, and FDIC, pursuant to the Dodd-Frank Act. These reviews are summarized below.

The FDIC's Receivership Basic Ordering Agreements for Business Process Operations Services

As noted earlier in this report, when an insured financial institution fails, the FDIC is appointed receiver by the chartering authority. In its receivership capacity, DRR manages the assets of a failed bank to preserve or enhance their value and disposes of them as quickly as possible. The FDIC uses a number of IT applications to facilitate the management, marketing, and servicing of assets, and has relied heavily on the use of contractors and failed bank staff to carry out its receivership obligations, including outsourcing Business Process Operations (BPO) services. The work of BPO contractors covers pre-closing, closing, and post-closing activities involved in a failed bank's closure.

On April 22, 2010, the FDIC executed Receivership Basic Ordering Agreements for BPO services, one to Fiserv Federal Systems, Inc. (Fiserv) and the other to Fidelity National Information Services, Inc. (Fidelity). As of early February 2014, the FDIC had awarded 280 task orders totaling $190,930,363 to Fiserv and 230 task orders for a total value of $166,862,204 to Fidelity under their respective agreements.

A Receivership Basic Ordering Agreement is used to expedite the acquisition of goods and/or services in support of failing or failed institutions and is similar to a Basic Ordering Agreement except it is limited to awards in support of DRR and is not assigned a monetary value or a contract ceiling. Rather, dollar value ceiling controls are established at the task order level, allowing DRR the ability to formulate requirements and resultant cost estimates as needs become better defined. DRR uses the Receivership Basic Ordering Agreement vehicle for obtaining various services such as receivership assistance, loan servicing and collections, asset valuations, and BPO.

We conducted an audit to determine whether payments made by the FDIC to Fiserv and Fidelity were adequately supported, allowable under the terms of the contracts, and reasonable. We also performed work related to task orders awarded by the FDIC to Fiserv and Fidelity for implementing a toolkit called InfoSphere to be used in converting failed bank information from a bank's data processing system into the FDIC's systems. We wanted to determine whether contractor tasks and deliverables were within the scope of the task order statements of work and associated billings were reasonable.

We determined that DRR has established and implemented various control activities for overseeing Fiserv and Fidelity to help ensure that the contractors meet their respective performance objectives and comply with contract provisions. DRR also has a robust invoice review process, including weekly meetings with Fiserv and Fidelity to discuss labor charges and monthly meetings to discuss travel charges, to help ensure that contractor claims for labor and travel costs are appropriate and supportable.

To test the adequacy of these controls, we reviewed simple random samples of 280 Fiserv and Fidelity labor and travel cost charges incurred during 2012. We verified labor charges against the price schedule in the contract and qualifications in contractor employee resumes. We verified travel charges against supporting travel receipts and government lodging and per diem rates. We found no exceptions.

As part of our testing, we also verified the contract deliverable that the FDIC received for each sampled labor charge. In regard to evaluating the reasonableness of charges associated with the InfoSphere task orders, 17 of the 280 charges we tested were expenses incurred while performing work under the InfoSphere task orders, and we concluded that these charges were reasonable. In addition, we judgmentally selected labor charges under the InfoSphere task orders and concluded that these charges were reasonable.

During the course of our audit, we became aware of contract actions and unanticipated funding increases that illustrate a need for greater DRR and Division of Administration (DOA) coordination when planning for program needs that will involve contractors. We also identified instances where contractor employees in travel status were not always using hotel tax exemption forms when incurring lodging expenses in any of the 11 states that offer the exemption for hotel occupancy taxes.

We made four recommendations intended to strengthen controls for monitoring the performance of BPO contractors that cover pre-closing, closing, and post-closing activities for failed banks and enhancing acquisition team coordination. We referred the matter of hotel tax exemption forms to FDIC management for further study because it may provide an opportunity to reduce contractor travel expenses in these and other FDIC contracts. FDIC management officials agreed with all recommended actions.

The FDIC's Purchase Card Program

The Government Charge Card Abuse Prevention Act of 2012, while not applicable to the FDIC, requires executive agencies that issue and use purchase cards (P-Cards) and convenience checks to establish and maintain appropriate safeguards and internal controls over those forms of payment. The statute also requires Inspectors General covered by the Act to conduct periodic risk assessments and audits of agency P-Card and convenience check programs. Consistent with the spirit of the Act, we conducted an audit of the FDIC's P-Card Program. We engaged the independent firm of Reed & Associates, CPAs, Inc., to provide technical assistance during the audit.

The FDIC participates in the governmentwide charge card program known as the General Services Administration SmartPay 2 Program. Under the program, the General Services Administration manages a set of master contracts with major U.S. financial institutions through which agencies and organizations may obtain charge card services to accomplish their mission. In 2008, the FDIC entered into a 10-year contract under the program with U.S. Bank National Association. The contract authorizes U.S. Bank National Association to issue P-Cards to designated FDIC employees and to bill the FDIC for cardholder purchases. The contract also provides for the use of convenience checks in order to accommodate purchases from vendors who do not accept P-Cards.

Within the FDIC, DOA has overall responsibility for administering the P-Card Program. Key roles in the program include an Agency Program Coordinator who is responsible for the day-to-day administrative oversight of the P-Card Program, Division/Office Coordinators who serve as liaisons with DOA and oversee their division's or office's compliance with the program, and Approving Officials who are responsible for monitoring cardholders, reviewing and approving purchases and charges, and ensuring that charges are adequately supported. The FDIC had processed 22,455 P-Card and convenience check transactions totaling $23.3 million during 2012. At the close of 2012, the FDIC had 571 active cardholder accounts.

We determined that the FDIC had established a number of internal controls intended to minimize the risk of improper transactions under the P-Card Program that were generally consistent with recognized best practices identified by the Office of Management and Budget (OMB), the Government Accountability Office, and others. Such controls include written policies and procedures governing the use of P-Cards and convenience checks, mandatory training for cardholders and Approving Officials, and various risk management controls, such as periodic internal reviews and reconciliations of cardholder statements. Further, the FDIC's card service provider – U.S. Bank National Association – implemented certain controls to prevent and detect improper transactions. While these controls address many recognized best practices, we found that the FDIC could improve the effectiveness of its P-Card Program controls by:

- Making greater use of transaction data to detect patterns, trends, and anomalies that may be indicative of potential fraud or misuse;
- Performing periodic, program-level reviews of cardholder purchase limits to ensure they remain appropriate and monitoring convenience check transactions for compliance with established purchase limits;
- Conducting periodic, program-level assessments of the reasonableness of the ratio of Approving Officials to cardholders and the volume of transactions that Approving Officials are responsible for reviewing;
- Ensuring that cardholder accounts are disabled in a timely manner when cardholders leave the FDIC;
- Prohibiting cardholders from using the P-Card to purchase non-monetary awards on their own behalf; and
- Reviewing and clarifying, as appropriate, the role and responsibilities of the Division/Office Coordinator.

We made eight recommendations to strengthen internal controls related to the P-Card Program. FDIC management concurred with all of them.

Independent Evaluation of the FDIC's Information Security Program – 2013

FISMA requires federal agencies, including the FDIC, to perform annual independent evaluations of their information security programs and practices and to report the evaluation results to OMB.

We conducted our annual audit to evaluate the effectiveness of the FDIC's information security program and practices and engaged the independent professional services firm of KPMG LLP to perform audit procedures in certain security control areas during the audit.

In conducting our work, we performed audit procedures to evaluate the 11 security control areas outlined in the Department of Homeland Security's November 30, 2012 document entitled, *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*. We evaluated the effectiveness of security controls in these areas by designing audit procedures to assess consistency between the FDIC's security controls and FISMA requirements, OMB policy and guidelines, and applicable National Institute of Standards and Technology standards and guidelines. Our work included testing of selected servers and desktops and a review of the FDIC's oversight of an outsourced information service provided by Innovative Discovery.

We concluded that the FDIC had established and maintained many information security program controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable National Institute of Standards and Technology standards and guidelines. Notably, the FDIC had established security policies and procedures in almost all of the security control areas we evaluated. The FDIC was also working to develop a formal concept-of-operations document that describes a corporate-wide approach to information security continuous monitoring.

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

The ECU 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 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.

To address current and emerging risks in the IT and information security environments, the FDIC made significant changes to its security governance structure during 2013. As noted earlier in this semiannual report, such changes included the realignment of the roles and responsibilities of the CIO, Chief Information Security Officer, and Information Security and Privacy Staff. The FDIC also established an IT/Cyber Security Oversight Group to provide a senior-level forum for addressing cyber security threats and developments impacting both the FDIC and the banking industry. Such changes are positive and better position the FDIC to address information security risks from a corporate perspective. We plan to more fully assess the implementation of these security governance changes as part of our future audit and evaluation work.

Notwithstanding these accomplishments, we determined that continued management attention and control improvements are needed to more effectively identify, evaluate, and mitigate risk to the FDIC's information systems and data, particularly in the areas of Incident Response and Reporting, Risk Management, Configuration Management, Outsourced Information Systems and Services, and Contingency Planning. Specifically, the

FDIC needed to strengthen its incident response policies and procedures to address sophisticated, cyber-based security incidents and update its corporate information security risk management policy to reflect changes in its risk management processes and governance. The FDIC can also take additional steps to help ensure that certain servers and workstations are patched to protect against known vulnerabilities. In addition, we reported that greater emphasis needs to be placed on assessing risks associated with the FDIC's outsourced information systems and services where limited progress has been made in the last year. Finally, further analysis is warranted to ensure that information systems supporting mission essential functions can be recovered within the timeframes needed to support those functions.

Our report contains 15 recommendations intended to improve the effectiveness of the FDIC's information security program controls and practices. In many cases, the FDIC was already working to strengthen security controls in these areas during our audit.

The FDIC's Data Submissions through the Governmentwide Financial Report System as of September 30, 2013

Many federal agencies, including the FDIC, were required to provide financial information for the fiscal year ended September 30, 2013, to the Department of the Treasury for inclusion in the annual Financial Report of the United States Government. We conducted an audit to determine whether the FDIC's summary general ledger information agreed with summary information entered into the Governmentwide Financial Report System (GFRS) for the fiscal year ended September 30, 2013.

We verified that the FDIC's summary general ledger information agreed with summary information entered into the GFRS for the fiscal year ended September 30, 2013. As part of our work, we verified that the FDIC's data submissions in the GFRS for the year ended December 31, 2012, agreed with the Corporation's audited financial statements for that year. In addition, we submitted copies of requisite reports and representation letters to the Treasury, U.S. Government Accountability Office, OMB, and Department of Justice in accordance with the Treasury Financial Manual.

Our report did not contain recommendations.

Joint Review Conducted by the OIGs of the Department of the Treasury, Board of Governors of the Federal Reserve System, and the FDIC

We issued the results of our final semiannual review of the implementation of the Joint Implementation Plan (Plan) established to carry out Dodd-Frank Act provisions related to the transfer of the former OTS powers, authorities, and functions. The Dodd-Frank Act requires that we, jointly with the Department of the Treasury and the Board of Governors of the Federal Reserve System Offices of Inspector General, provide a written report on the status of the implementation of the Plan every 6 months until the Plan is implemented.

During this reporting cycle, our OIG audit team focused primarily on the FDIC's final actions to implement the Plan. These actions relate to the Section 322 requirement to protect transferred OTS employees from certain pay and other personnel actions during the 30-month period following the transfer. We determined that the FDIC complied with this requirement of the Act. The report contained no recommendations and did not require a formal response from FDIC management. Corporation officials did, however, express general agreement with the audit results during the reporting process.

Strategic Goal 6

The OIG Will Build and Sustain a High-Quality OIG 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 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.

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 adheres to the *Quality Standards for Federal Offices of Inspector General*. Further, the OIG conducts its audit work in accordance with generally accepted government auditing standards; its evaluations in accordance with *Quality Standards for Inspection and Evaluation*; and its investigations, which often involve allegations of serious wrongdoing that may involve potential violations of criminal law, in accordance with *Quality Standards for Investigations* and procedures established by the Department of Justice.

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 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, as noted earlier in this report, 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 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 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 lays the 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.

To build and sustain a high-quality staff, effective operations, OIG independence, and mutually beneficial working relationships, the **OIG's 2014 performance goals** are 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 performance goals follows.

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

1. Provided the OIG's Fiscal Year 2015 budget to the Senate and the House Appropriations Committees, Subcommittees on Financial Services and General Government. This budget requests $34.6 million to support 130 full-time equivalents, reflecting no change from our Fiscal Year 2014 budget, based on corporate workload assumptions of bank failures and resolution activity expected in calendar year 2014 and beyond.
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 internal training sessions and other 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. Launched our redesigned OIG Intranet site to provide a more useful, efficient work tool for all OIG staff.
7. Initiated 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.
8. Developed an approach to a new contract for IT audit and evaluation services.
9. Carried out retirement training for OIG investigative staff in certain regional offices to ensure a thorough understanding of applicable retirement policies and procedures for those holding law enforcement positions.

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

1 Implemented 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 that plan, held a 2-day training conference for audit and evaluation staff on policies and procedures and TeamMate updates.

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 become more knowledgeable of current information in the regulatory agency accounting and auditing profession.

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 Conducted the peer review of the audit operations of the OIG at the National Archives and Records Administration OIG, to ensure that the system of quality control for its audit organization had been suitably designed and complied with to provide that office with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

6 Prepared to conduct 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.

7 Coordinated the Inspector General (IG) community's audit peer review activities for OIGs governmentwide as a continuation of former FDIC IG Jon Rymer's leadership of the CIGIE Audit Committee to ensure a consistent and effective peer review process and quality in the federal audit function.

8 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.

9 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.
2	Employed an intern on a part-time basis in the OIG to provide assistance to the OIG.
3	Represented the CIGIE Audit Committee in the Office of Personnel Management's initiative to close skills gaps associated with six mission-critical positions, including the auditor 511 position.
4	Enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities.
5	Continued an active OIG Mentoring Program, 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	Sponsored lunch-time Webinars and other learning forums on a variety of topics relevant to the OIG in the interest of providing additional opportunities for professional development for OIG staff.

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; attending or monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the Corporation's Office of Legislative Affairs on issues of mutual interest.

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 IG'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 the Chairman's Office 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. Reviewed 12 proposed or revised corporate policies related to, for example, the FDIC's procedures for providing reasonable accommodation for employees with disabilities, pre-exit clearance procedures for FDIC employees, and the FDIC's merit promotion plan. Made suggestions to increase clarity and specificity of these and other draft policies. Provided more substantive comments on the FDIC's proposed directive related to IT development and suggested strengthening controls related to FDIC travel cards.

Foster Good Client, Stakeholder, and Staff Relationships

8	Supported the IG community by participating on the CIGIE Audit Committee, including providing training on and overseeing the community's audit peer review process; attending monthly CIGIE meetings; and participating in Investigations Committee, Council of Counsels to the IGs, and Professional Development Committee meetings; and commenting on various legislative matters through the Legislative Committee.
9	Communicated, as appropriate, with representatives of the OIGs of the federal banking regulators and others (FRB, Department of the Treasury, National Credit Union Administration, Securities and Exchange Commission, Farm Credit Administration, Commodity Futures Trading Commission, Federal Housing Finance Agency, Export-Import Bank, SIGTARP, Department of Housing and Urban Development) to discuss audit and investigative matters of mutual interest and leverage knowledge and resources. Participated on CIGFO, as established by the Dodd-Frank Act, with the IGs from most of the above-named agencies.
10	Coordinated with the Government Accountability Office on its ongoing efforts related to the annual financial statement audit of the FDIC.
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	Formed part of the CIGFO working group conducting work related to the Financial Stability Oversight Council's compliance with its transparency policy.
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. Explored means of ensuring positive staff working relationships and excellence in the OIG's internal operations and activities.

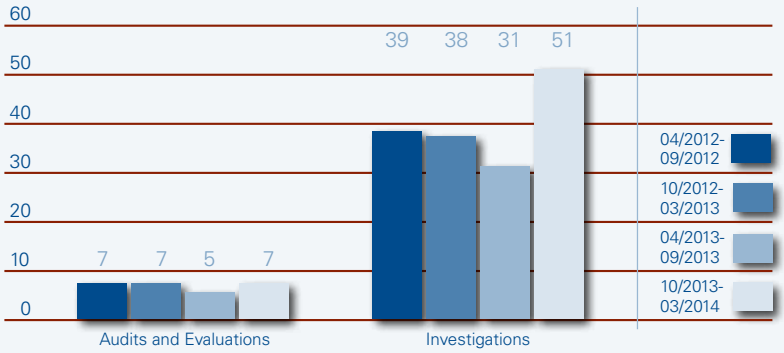
Enhance OIG Risk Management Activities

1	Undertook risk-based OIG planning efforts for audits, evaluations, and investigations for fiscal year 2014 and beyond, taking into consideration the goals of, and risks to, FDIC corporate programs and operations and those risks more specific to the OIG. Used corporate performance goals as a basis for identifying risk areas and potential gaps in OIG planned coverage for the fiscal year.
2	Attended FDIC Board Meetings, IT/Cyber Security Oversight 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.
4	Coordinated with the FDIC Chairman's Office and other senior FDIC management officials to discuss debt ceiling contingency measures and overall preparedness for and handling of other unanticipated or emerging risks affecting the Corporation.
5	Performed research on the FDIC's policies, procedures, and controls related to hiring foreign nationals as employees or contractors in the context of applicable U.S. export control and immigration laws and identified related risk areas for the FDIC's attention.
6	Provided representatives of 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.
7	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 Systemic Resolution Responsibilities, Strengthening IT Security and Governance, Maintaining Effective Supervision and Preserving Community Banking, Carrying Out the Ongoing Resolution and Receivership Workload, 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.

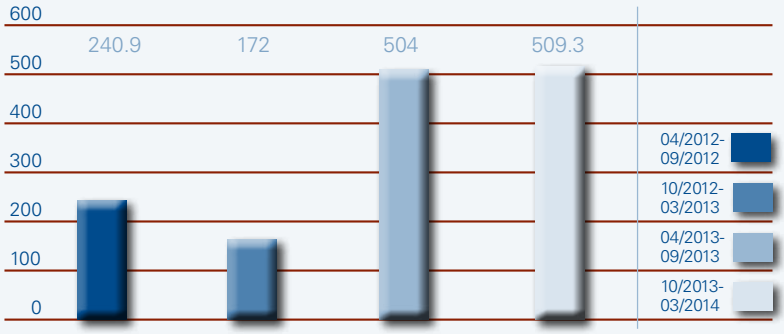
Cumulative Results (2-year period)

Nonmonetary Recommendations	
April 2012 – September 2012	21
October 2012 – March 2013	27
April 2013 – September 2013	15
October 2013 – March 2014	37

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	49
Section 5(a)(1)	Significant problems, abuses, and deficiencies	10-38
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies	10-38
Section 5(a)(3)	Recommendations described in previous semiannual reports on which corrective action has not been completed	50
Section 5(a)(4)	Matters referred to prosecutive authorities	9
Section 5(a)(5) and 6(b)(2)	Summary of instances where requested information was refused	51
Section 5(a)(6)	Listing of audit reports	50
Section 5(a)(7)	Summary of particularly significant reports	10-38
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	51
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	51
Section 5(a)(10)	Audit recommendations more than 6 months old for which no management decision has been made	51
Section 5(a)(11)	Significant revised management decisions during the current reporting period	51
Section 5(a)(12)	Significant management decisions with which the OIG disagreed	51

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

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

Review of Legislation and Regulations

The FDIC OIG's review of legislation and regulations during the past 6-month period involved the following activities:

- We continued efforts to monitor and/or comment on proposed federal legislation concerning (1) the reliability of information provided on agency Web sites regarding agency payments made to grantees and contractors, (2) changes to existing law (FISMA) requiring that OIGs annually evaluate and report on the effectiveness of their agency's information security practices and programs, and (3) protecting from public disclosure information in OIG reports concerning vulnerabilities in agency security systems.

  In connection with these efforts, the Office of Counsel considered the following:

  S. 994, the *Digital Accountability and Transparency Act of 2014* or DATA Act;

  S. 1953, the *Oversight Workforce Improvement Act*;

  H.R. 1468, the *Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2013* or SECURE IT; and

  H.R. 1163, *Federal Information Security Amendments Act of 2013*.

- In addition, the Office of Counsel considered the implications of an OMB memorandum dealing with continuous monitoring of agency IT systems, namely M-14-03, *Enhancing the Security of Federal Information and Information Systems*. This memorandum contains various requirements for agencies to fulfill in 2014, including the development of a strategy for continuous monitoring of information security, and additional questions for Inspectors General to respond to as part of the IGs' annual FISMA evaluations.

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

This table shows the corrective actions management has agreed to implement but has not completed, along with associated monetary amounts, as applicable. In some cases, these actions may differ from the initial recommendations made in our reports. However, the OIG has agreed that the planned actions meet the intent of the initial recommendations. The information in this table is based on (1) information supplied by the FDIC's Corporate Management Control (CMC), Division of Finance, and (2) the OIG's determination of closed recommendations. Recommendations are closed when (a) CMC 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.

Report Number, Title and Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
Management Action in Process		
EVAL-13-002 Comprehensive Study on the Impact of the Failure of Insured Depository Institutions January 3, 2013	3	Strengthen examiner documentation requirements related to examination methodologies and examination procedures performed to assess an institution's appraisal program. (Implementation scheduled for June 2014.)

Table II
Audit and Evaluation Reports Issued by Subject Area

Report Number and Date	Title	Questioned Costs		Funds Put to Better Use
		Total	Unsupported	
Supervision				
AUD-14-001 November 14, 2013	The FDIC's Progress in Implementing Systemic Resolution Authorities under the Dodd-Frank Act		N/A	
Consumer Protection				
AUD-14-004 March 28, 2014	The FDIC's Actions to Address Consumer Protection Violations and Deficiencies		N/A	
Resources Management				
AUD-14-002 November 21, 2013	Independent Evaluation of the FDIC's Information Security Program – 2013		N/A	
AUD-14-003 February 27, 2014	The FDIC's Data Submissions through the Governmentwide Financial Report System as of September 30, 2013		N/A	
AUD-14-005 March 26, 2014	Transfer of Office of Thrift Supervision Functions Is Completed		N/A	
AUD-14-006 March 31, 2014	The FDIC's Receivership Basic Ordering Agreements for Business Process Operations Services		N/A	
AUD-14-007 March 31, 2014	The FDIC's Purchase Card Program		N/A	

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

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.

Appendix 2

Information on Failure Review Activity

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

FDIC OIG Review Activity for the Period October 1, 2013 through March 31, 2014
(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 after December 31, 2013)

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						
Covenant Bank Chicago, Illinois	2/15/13	$21.8	The bank was conducting its business in an unsafe and unsound manner.	No		
Frontier Bank LaGrange, Georgia	3/8/13	$51.6	The bank's financial condition did not permit it to meet certain capital requirements of a consent order.	No		
Heritage Bank of North Florida Orange Park, Florida	4/19/13	$30.2	The bank was insolvent.	No		
Pisgah Community Bank Asheville, North Carolina	5/10/13	$8.9	The bank was in an unsafe and unsound condition to transact business.	Yes	In-Depth Review will address the FDIC's overall supervisory strategy for Pisgah and other failed subsidiary institutions of Capitol Bancorp Ltd., including the consideration and use of the FDIC's cross-guarantee liability authority.	

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						
Chipola Community Bank Marianna, Florida	4/19/13	$10.3				
Parkway Bank Lenoir, North Carolina	4/26/13	$18.1				
Douglas County Bank Douglasville, Georgia	4/26/13	$86.4				
Sunrise Bank Valdosta, Georgia	5/10/13	$17.3				
Central Arizona Bank Scottsdale, Arizona	5/14/13	$8.6				
Banks of Wisconsin Kenosha, Wisconsin	5/31/13	$26.3				
1st Commerce Bank North Las Vegas, Nevada	6/6/13	$9.4				
First Community Bank of SW Florida Fort Myers, Florida	8/2/13	$27.1				
Bank of Wausau Wausau, Wisconsin	8/9/13	$13.5				
Community South Bank Parsons, Tennessee	8/23/13	$72.5				
Sunrise Bank of Arizona Phoenix, Arizona	8/23/13	$17				
The Community's Bank Bridgeport, Connecticut	9/13/13	$7.8				
Bank of Jackson County Graceville, Florida	10/30/13	$5.1				
Syringa Bank Boise, Idaho	1/31/14	$4.5				
Vantage Point Bank• Horsham, Pennsylvania	2/28/14	$8.5				

• **Vantage Point Bank:** At the request of FDIC management, we will be performing an in-depth review to (1) determine the causes of the bank's failure and the resulting loss to the DIF and (2) evaluate the FDIC's supervision of the bank, including the FDIC's implementation of the Prompt Corrective Action provisions of section 38 of the FDI Act. The scope of the review will include emphasis on the bank's deviation from its business plan and the FDIC's supervisory response to address the associated risks.

Appendix 3

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.

In responding to the recommendations, we committed to completing recommended actions by February 28, 2014. We completed responsive actions by that date.

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 Smithsonian Institution OIG

The FDIC OIG completed a peer review of the audit operations of the Smithsonian Institution (SI), and we issued our final report to that OIG on September 21, 2011. We reported that in our opinion, the system of quality control for the audit organization of the SI OIG, in effect for the 15-month period ended March 31, 2011, had been suitably designed and complied with to provide the SI OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. The SI OIG received a peer review rating of pass.

As is customary, we also issued a Letter of Comment, dated September 21, 2011, 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 11 recommendations, with which the SI OIG agreed. SI OIG indicated it would complete all corrective actions related to the findings and recommendations no later than March 31, 2012. SI OIG has posted its peer review report (the system review report and accompanying letter of comment) on its Web site at www.si.edu/oig/.

In our semiannual report as of March 31, 2012, we reported that the SI OIG reported completed actions on 4 of our 11 recommendations. SI OIG was also updating its audit manual to reflect the Fiscal Year 2011 revision to government auditing standards and recommendations from our peer review. As of September 30, 2012, SI OIG reported that actions on all recommendations in our peer review report had been completed.

Ongoing FDIC OIG Audit Peer Review Activity

We completed a peer review of the audit organization of the National Archives and Records Administration OIG and issued our report in April 2014. We will report the results of that review in our next semiannual report.

Investigative Peer Reviews

Quality assessment peer reviews of investigative operations are conducted on a 3-year cycle as well. Such reviews result in a determination that an organization is "in compliance" or "not in compliance" with relevant standards. These standards are based on *Quality Standards for Investigations* and applicable Attorney General guidelines. 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 FDIC OIG conducted a peer review of the investigative function of the National Aeronautics and Space Administration OIG during June through August 2011. We issued our final report to NASA OIG on November 10, 2011. We reported that, in our opinion, the system of internal safeguards and management procedures for the investigative function of the NASA OIG in effect for the period ending December 31, 2010 was in full compliance with the quality standards established by CIGIE and Attorney General guidelines. We also issued a letter of observations but made no recommendations in that letter.
- 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 CIGIE and applicable Attorney General guidelines. These safeguards and procedures provided reasonable assurance of conforming with professional standards in the planning, execution, and reporting of FDIC OIG investigations.

Ongoing FDIC OIG Investigative Peer Review Activity

We are conducting a peer review of the investigative function of the Environmental Protection Agency OIG. We will report the results of that review in an upcoming semiannual report.

Congratulations and Farewell

Valerie Toyer
Retirement

Valerie Toyer retired from the FDIC after nearly 32 years of federal service. Her federal career began in 1980, when she served as a clerk-typist on a temporary appointment at the Department of Health, Education, and Welfare (now the Department of Health and Human Services). She subsequently served in similar roles at the Department of the Navy and Environmental Protection Agency. In 1983, she began full-time clerical work at the U.S. Department of Agriculture. In early 1985, she transferred to the National Aeronautics and Space Administration OIG where she began her career as a criminal investigator, and she followed that assignment with a transfer to the Department of Energy OIG. She joined the FDIC OIG in November 1991 and served a key role in our Office of Investigations for more than 22 years, serving as a Special Agent.

Valerie handled a number of sensitive FDIC employee cases during her time at the FDIC. As a desk officer, she was responsible for conducting peer reviews of other OIGs and for coordinating peer reviews of our own investigative operations. She also performed internal quality reviews to help ensure that our office met applicable standards promulgated by the IG community and the Attorney General guidelines.

Valerie helped to foster constructive working relationships with FDIC management, other OIGs, U.S. Attorneys' Offices, and fellow law enforcement groups. She also imparted her knowledge and guided new investigative staff when they joined the FDIC OIG workforce.

Gene Szczenski
Retirement

Gene Szczenski retired from the FDIC after more than 35 years of federal service. He began his career in 1978 as an Auditor at the Department of Health, Education, and Welfare (now the Department of Health and Human Services) in New York, New York. In 1980, he transferred to Washington, D.C. to become an Auditor in the FDIC's Office of Corporate Audits and Internal Investigations, the predecessor organization to the FDIC OIG, where he was promoted to Senior Auditor positions. In 1984, he was reassigned as a Computer Systems Audit Specialist, and he was promoted to Senior Microcomputer and Audit Applications Specialist in 1985. In 1990, he was reassigned as a Senior Audit Specialist with the FDIC OIG and subsequently promoted to Audit Manager in the Automated Resources Branch. From 1991 through 2014, he served as a Deputy Assistant Inspector General, Director of the Information Technology Resources Branch, and an Information Technology (IT) Specialist within the OIG, handling increasingly complex and challenging assignments during those years.

Gene applied his technical expertise and coordinated with others in the FDIC to ensure the OIG's IT environment, including hardware and software, was safe and secure; willingly assisted OIG staff with their questions; and helped address numerous IT-related issues. He also coordinated closely with the FDIC's Division of Information Technology and fostered mutually beneficial working relationships to ensure proper testing and implementation of OIG systems on the FDIC network. Of importance to the day-to-day operations of the OIG, he helped ensure that OIG systems such as STAR and IDS provided audit, evaluation, and investigative staff and OIG senior leadership with reliable, helpful assignment management tools.

Farewell to Former FDIC IG
Jon T. Rymer

Jon Rymer returned to FDIC headquarters on February 18, 2014, for a farewell reception honoring his contributions as the FDIC IG for 7 years. FDIC Chairman Martin Gruenberg, FDIC Director Jeremiah Norton, Comptroller of the Currency Thomas Curry, former FDIC Chairman Sheila Bair, FDIC management officials, and staff members of the OIG attended the reception. Acting Inspector General Fred Gibson welcomed the guests. Former Chairman Bair spoke of her earliest interactions with Mr. Rymer when he became IG, recalling that they had joined the FDIC at about the same time. She commented on the positive working relationship that they had during the 5 years that they worked together. Chairman Gruenberg expressed his appreciation for Mr. Rymer's leadership and reaffirmed the value of the OIG at the FDIC. Of Mr. Rymer, he said, "The FDIC is a better, stronger, more effective agency because of him." He then presented the former IG with a Board Resolution honoring his service to the FDIC and the nation.

The OIG sincerely appreciates all aspects of Mr. Rymer's service to our country and to the FDIC. We bid Mr. Rymer a fond farewell and wish him the best in his new role as Department of Defense Inspector General.

Left to right: FDIC Chairman Martin Gruenberg, Former FDIC IG Jon T. Rymer, Former FDIC Chairman Sheila Bair.

Design: FDIC/DOA/CSB/Graphic Design and Printing Unit

History of the FDIC OIG

1974	The Office of Management Systems and Financial Audits consisted of eight people and was headed by Robert E. Barnett – who later became Chairman of the FDIC. This office conducted all audits and information technology operations for the Corporation. No Audit Committee existed and staff did not work under professional accounting and auditing or U.S. General Accounting Office standards.
October 1975	The office became the Office of Corporate Audits, and by 1979, the office began developing an investigative function.
December 6, 1982	In a Board Resolution, the responsibilities of the Office of Corporate Audits were redefined and the name of the office was changed to Office of Corporate Audits and Internal Investigations (OCAII). The office reported to the Appointive Director (that is – the Director representing the political party not in power at the time) and the Budget and Management Committee – comprised of Division and Office heads from the Corporation. This organizational relationship did not prove to be an ideal one.
May 18, 1984	A Board resolution established that OCAII would report to the Chairman and laid out responsibilities of a new Audit Committee.
April 17, 1989	The provisions of a Board Resolution that was signed on March 14, 1989, became effective. This resolution recognized that the Inspector General Act Amendments of 1988 required the Corporation to establish an Office of Inspector General (OIG) with an Inspector General (IG) who would function under the general supervision of the Chairman. OCAII was redesignated the OIG. The position of Director of OCAII became Inspector General, and the incumbent Director, Robert Hoffman, was designated Acting IG and then IG.
August 1989	The Financial Institutions Reform, Recovery, and Enforcement Act of 1989 established that the Federal Home Loan Bank Board (FHLBB) OIG would merge with the FDIC OIG. By October 1989, many FHLBB staff had joined the FDIC.
1993	Mr. Hoffman retired and James Renick was selected by Acting Chairman Andrew C. Hove, Jr., to serve as Inspector General.
December 17, 1993	Congress amended the IG Act through passage of the Resolution Trust Corporation (RTC) Completion Act, which included designating the IG position at the FDIC a Presidential appointment. Mr. Renick began to serve as Acting Inspector General.
January 1, 1996	The RTC's sunset in December 1995 led to a number of RTC OIG staff merging back into the FDIC OIG.
April 29,1996	Gaston L. Gianni, Jr., became the FDIC's first presidentially appointed IG, appointed by President William J. Clinton.
December 2004	Mr. Gianni retired from federal service and named Patricia M. Black, his Deputy IG, as Acting IG.
January 2005	Ms. Black began service as Deputy and Acting IG.
February 14, 2006	Jon T. Rymer was nominated by President George W. Bush to be FDIC IG.
June 22, 2006	Mr. Rymer was confirmed by the Senate as FDIC IG.
July 5, 2006	Mr. Rymer was sworn in as FDIC IG.
September 27, 2013	Mr. Rymer resigned as FDIC IG to become Department of Defense IG and named Principal Deputy IG, Fred W. Gibson, Jr., as Acting IG.
April 17, 2014	**25th Anniversary of the FDIC OIG.**

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

Please visit our Web site:
www.fdicig.gov

OIG Hotline

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