FEDERAL DEPOSIT INSURANCE CORPORATION

Office of Inspector General

Semiannual Report to the Congress

April 1, 2014 – September 30, 2014

FDIC

Office of Inspector General

The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the Congress to maintain stability and confidence in the nation's banking system by insuring deposits, examining and supervising financial institutions, and managing receiverships. Approximately 6,800 individuals carry out the FDIC mission throughout the country. According to most current FDIC data, the FDIC insured more than $6.1 trillion in deposits in 6,656 institutions, of which the FDIC supervised 4,217. 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 $51.1 billion as of June 30, 2014. Receiverships under FDIC control as of September 30, 2014, totaled 487, with assets in liquidation totaling about $8.3 billion.

Office of Inspector General
Semiannual Report to the Congress

April 1, 2014 – September 30, 2014

FEDERAL DEPOSIT INSURANCE CORPORATION

Office of Inspector General

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 April 1, 2014 through September 30, 2014. Our work continues to promote economy, efficiency, and effectiveness in FDIC programs and operations, and integrity within the banking industry. 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, received prison sentences of up to 42 months and were ordered to pay millions of dollars in restitution after pleading 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 that received national attention, a former bank director of Montgomery Bank and Trust, Ailey, Georgia, who had earlier faked his own death, pleaded guilty to bank, wire, and securities fraud. Just after the close of the reporting period, he was sentenced to 30 years in prison and ordered to forfeit a total of $51 million, representing the proceeds of his crimes, with restitution to be ordered at a later date. Overall, our investigations during the past 6-month period resulted in 36 indictments, 40 convictions, and more than $78 million in potential monetary recoveries.

With respect to audits and evaluations, we completed a comprehensive review of enforcement actions against institution-affiliated parties and professional liability claims against individuals and entities associated with a failed institution. We conducted this work jointly with the OIGs of the Department of the Treasury and Federal Reserve Board/ Consumer Financial Protection Bureau. In that report, we made seven recommendations intended to enhance regulatory agency enforcement and professional liability programs, with which the agency heads agreed. Of note as well, we issued a material loss review of the failure of The Bank of Union, El Reno, Oklahoma. This was the first material loss review we have conducted since January 2012, reflective of the decline in institution failures as the crisis subsides. In another assignment, we examined the FDIC's controls for safeguarding sensitive information in resolution plans submitted under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). We are also undertaking a broader look at corporate activities related to the Dodd-Frank Act and identifying areas of risk for potential review.

During the reporting period, we continued to examine our internal operations, workload, and resource needs. In light of recent and future attrition in our office, we have focused on succession planning. This focus has resulted in the addition of several new staff at all levels of our organization and changes in responsibilities for other staff, requiring flexibility on the part of all as we adjust to change. We are reexamining our strategic and performance goals to ensure they align with the FDIC's current priorities and the OIG's mission under the Inspector General Act; assessing risks to FDIC programs and activities and to OIG activities; identifying projects and products that will add the most value to the FDIC; looking at our investigative caseload and related activities to be sure they are yielding the best possible outcomes; and revisiting our internal business processes, policies, and procedures to ensure they provide effective and efficient guidance for all aspects of our work.

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

Fred W. Gibson, Jr.
Principal Deputy Inspector General
October 2014

Table of Contents

Acronyms and Abbreviations

AML	anti-money laundering
BOU	The Bank of Union
BSA	Bank Secrecy Act
C&I	commercial and industrial
CEBT	Colorado East Bank & Trust
CEO	Chief Executive Officer
CFI Group	Complex Financial Institutions Group
CHRIS	Corporate Human Resources Information System
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
DIF	Deposit Insurance Fund
DIT	Division of Information Technology
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DRR	Division of Resolutions and Receiverships
EA	enforcement action
ECU	Electronic Crimes Unit
FBI	Federal Bureau of Investigation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FinCEN	Financial Crimes Enforcement Network
FRB	Board of Governors of the Federal Reserve System
GPRA	Government Performance and Results Act of 1993
IAP	institution-affiliated parties
IRS-CI	Internal Revenue Service, Criminal Investigation Division
IT	information technology
MB&T	Montgomery Bank & Trust
NARA	National Archives and Records Administration
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
OPM	Office of Personnel Management
OSBD	Oklahoma State Banking Department
PERSEREC	Personnel Security Records
PLC	professional liability claim
PSSP	Personnel Security and Suitability Program
RMS	Division of Risk Management Supervision
SAR	Suspicious Activity Report
SEPS	Security and Emergency Preparedness Section
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
UCC	Union City Corporation
VA	Department of Veterans Affairs

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 joined the Department of the Treasury and the Board of Governors of the Federal Reserve System/Consumer Financial Protection Bureau OIGs in issuing a report on enforcement actions against institution-affiliated parties and professional liability claims against individuals and entities associated with a failed institution. That report contained seven recommendations to the regulatory agency heads to enhance their enforcement and professional liability programs. Another report we issued addressed the FDIC's response to Bank Secrecy Act (BSA) and anti-money laundering (AML) concerns identified at FDIC-supervised institutions. The three recommendations we made in that report will improve the Corporation's internal controls for addressing BSA/AML concerns during supervisory examinations. Finally, we issued a material loss review of the failure of the Bank of Union, El Reno, Oklahoma, a bank that concentrated in commercial and industrial, and agricultural loans. This is the first material loss review we have conducted since the January 2012 failure of Tennessee Commerce Bank, Franklin, Tennessee. We also completed eight 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 OIG work includes an evaluation of the FDIC's supervisory activities related to cyber threats at financial institutions and their technology service providers.

With respect to investigative work, as a result of cooperative efforts with U.S. Attorneys throughout the country, numerous individuals were prosecuted for financial institution fraud, and we also successfully pursued a number of mortgage fraud schemes. Our efforts in support of bank fraud, mortgage fraud, and other financial services working groups also supported this goal. Particularly noteworthy results from our casework include the pleas and sentencings of a number of former senior bank officials and bank customers involved in fraudulent activities that undermined the institutions and, in some cases, contributed to the institutions' failures. For example, seven former bank officials of First National Bank of Savannah, Savannah, Georgia, were sentenced for their roles in a long-running, complex scheme that contributed to the failure of the bank. Their sentences range from 2 years of probation to 42 months in prison. Restitution was ordered for each of them, and in the case of the former president and chief executive officer, totaled $9.7 million. In another high-profile case, a former bank director of Montgomery Bank and Trust, Ailey, Georgia, who had earlier faked his own death, pleaded guilty to bank, wire, and securities fraud. He misappropriated and embezzled millions of dollars from the bank. He also duped other investors of more than $51 million and lost most of their funds through speculative trading and other investments. In another case, for his role in a $49.6 million mortgage fraud scheme, a former developer was sentenced to 27 years and 3 months in prison.

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, an activity that continues to be mutually beneficial. (See pages 10-26.)

Strategic Goal 2: Insurance

Help the FDIC Maintain the Viability of the Insurance Fund

We did not conduct specific assignments to address this goal area during the reporting period. However, our audit and evaluation work in support of goal 1 fully supports this goal, as does the investigative work highlighted above. In both cases, our work can serve to strengthen the FDIC's supervisory program and help prevent or lessen future failures. Further, the deterrent aspect of investigations and the ordered restitution may help to mitigate an institution's losses and losses to the Deposit Insurance Fund. (See pages 27-28.)

Strategic Goal 3: Consumer Protection

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

In support of this goal area, we collaborated with OIG counterparts on an evaluation assignment to examine the progress that the prudential regulators and the Consumer Financial Protection Bureau have made in establishing coordination for the consumer protection responsibilities that the various parties carry out.

Our Office of Investigations also supports consumer protection through its work. Investigators continue to pursue cases of misrepresentation of FDIC insurance or affiliation where unscrupulous individuals attempt to convince others to invest in financial products allegedly insured by or endorsed by the FDIC. Our Electronic Crimes Unit also responds to instances where fraudulent emails purportedly affiliated with the FDIC are used to entice consumers to divulge personal information and/or make monetary payments. Working with the Corporation's Division of Information Technology and Chief Information Officer's Office, 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 140 such inquiries during the past 6-month period. (See pages 29-31.)

Strategic Goal 4: Receivership Management

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

We did not complete assignments directly related to this goal area during the reporting period. However, as of the end of the reporting period we were conducting two assignments involving receivership management activities. In the first one, we are conducting an audit of 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. Of note in that regard during the reporting period was the Electronic Crimes Unit's assistance related to the successful case involving the First National Bank of Savannah, where forensic support helped prove seven former bank executives guilty of bank fraud. (See pages 32-34.)

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 personnel security and suitability program. This important program seeks to ensure that the FDIC employs and retains only those who meet all federal requirements for suitability and whose employment would not jeopardize the achievement of the corporate mission. We made 10 recommendations in our report to complement ongoing program improvements and to strengthen and sustain associated policies, procedures, and controls. We also completed work in connection with the FDIC's IT project management and issued a report in which we identified key success factors for managing such efforts. Our report noted that ensuring these factors are emphasized and related controls are in place and working could provide greater assurance that projects meet cost, schedule, and requirements expectations. We completed an audit of the controls for safeguarding sensitive information submitted under the Dodd-Frank Act, and made seven recommendations related to access management, encryption and authentication, internal control reviews, and personnel suitability. At the end of the reporting period, we were completing work on our annual Federal Information Security Management Act evaluation and will report those results in our next semiannual report.

We promoted integrity in FDIC internal operations through ongoing OIG Hotline and other referrals and coordination with the FDIC's Divisions and Offices, including corporate ethics officials, as warranted. (See pages 35-41.)

Strategic Goal 6: OIG Resources Management

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

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

We continued to implement our audit/evaluation quality assurance plan to cover the period October 2013 – March 2016 to ensure quality in all audit and attestation engagement work and evaluations, in keeping with government auditing standards and Quality Standards for Inspection and Evaluation. In that regard, we took a number of actions in response to the most recent peer review of our audit operations. We oversaw contracts with qualified firms to provide audit and evaluation services to the OIG to supplement our efforts and provide additional subject-matter expertise.

We encouraged individual growth through professional development by supporting individuals in our office involved in professional organizations, pursuing professional certifications, or attending graduate schools of banking. 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 interns on a part-time basis to promote the interns' professional development and assist us in our work. Our Workplace Excellence Group met to help foster excellence in OIG operations and we selected new members for that initiative.

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

In the area of risk management, in connection with SAS 99 and the annual audit of the FDIC's financial statements, we formulated our perspectives on the risk of fraud at the FDIC for the U.S. Government Accountability Office. We began developing 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 those areas that we had identified as management and performance challenges facing the Corporation for inclusion in its annual report. (See pages 42-50.)

Significant Outcomes
April 1, 2014 – September 30, 2014

Audit and Evaluation Reports Issued	**6**
Questioned Costs and Funds Put to Better Use	**0**
Nonmonetary Recommendations	**27**
Investigations Opened	**44**
Investigations Closed	**36**
OIG Subpoenas Issued	**13**
Judicial Actions:	
Indictments/Informations	**36**
Convictions	**40**
Arrests	**18**
OIG Investigations Resulted in:	
Fines of	**$ 351,850**
Restitution of	**76,672,543**
Asset Forfeitures of	**992,436**
Total	**$ 78,016,829**
Cases Referred to the Department of Justice (U.S. Attorney)	**39**
Cases Referred to FDIC Management	**0**
Proposed Legislation and Regulations Reviewed	**7**
Proposed Draft FDIC Policies Reviewed	**8**
Responses to Requests Under the Freedom of Information Act	**16**

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 FDIC-supervised insured depository institutions. The FDIC is the primary federal regulator for approximately 4,200 FDIC-insured, state-chartered institutions that are not members of the Board of Governors of the Federal Reserve System (FRB) — generally referred to as "state non-member" institutions. As insurer, the Corporation also has back-up examination authority to protect the interests of the Deposit Insurance Fund (DIF) for about 2,440 national banks, state-chartered banks that are members of the FRB, and savings associations regulated by the Office of the Comptroller of the Currency (OCC).

Through September 26, 2014, 14 FDIC-insured institutions failed, compared to 24 in calendar year 2013, 51 in 2012, 92 in 2011, 157 in 2010, and 140 in 2009. As of June 30, 2014, 354 institutions with total assets of $110.2 billion were on the Problem Bank List, down from 411 institutions in March.

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

Prior to passage of the Dodd-Frank Act, in the event of an insured depository institution failure, the Federal Deposit Insurance (FDI) Act required the appropriate regulatory OIG to perform a review when the DIF incurs a material loss. Under the FDI Act, a loss was considered material to the insurance fund if it exceeded $25 million or 2 percent of the failed institution's total assets. With passage of the Dodd-Frank Act, the loss threshold was increased to $200 million through December 31, 2011, $150 million for losses that occurred for the period January 1, 2012 through December 31, 2013, and $50 million thereafter. The FDIC OIG performs the review if the FDIC is the primary regulator of the institution. The Department of the Treasury OIG and the OIG at the FRB perform reviews when their agencies are the primary regulators. These reviews identify what caused the material loss and evaluate the supervision of the federal regulatory agency (including compliance with the Prompt Corrective Action requirements of the FDI Act). Importantly, under the Dodd-Frank Act, the OIG is now required to review all losses incurred by the DIF under the thresholds to determine (a) the grounds identified by the state or federal banking agency for appointing the Corporation as receiver and (b) whether any unusual circumstances exist that might warrant an in-depth review of the loss. Although the number of failures continues to decline, the OIG will conduct and report on material loss reviews and in-depth reviews of failed FDIC-supervised institutions, as warranted, and continues to review all failures of FDIC-supervised institutions for any unusual circumstances.

The passage of the Dodd-Frank Act brought about significant organizational changes to the FDIC's supervision program. In April 2013, the monitoring (Oversight and Risk Analytics Branches) function for systemically important financial institutions within the Office of Complex Financial Institutions (OCFI) was transferred to the Division of Risk

Management Supervision (RMS) and renamed as the Complex Financial Institutions Group (RMS-CFI Group). The institutional knowledge and analysis associated with the RMS-CFI Group is relevant to OCFI's 165(d) plan reviews, orderly liquidation, and international functions, and collaboration across OCFI and the RMS-CFI Group is on-going. The RMS-CFI Group is primarily responsible for monitoring risk within and across large, complex financial companies for back-up supervisory and resolution readiness purposes.

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, the Division of Resolutions and Receiverships (DRR), and the Legal Division to identify and investigate financial institution crime, especially various types of bank fraud. OIG investigative efforts are concentrated on those cases of most significance or potential impact to the FDIC and its programs. The goal, in part, is to bring a halt to the fraudulent conduct under investigation, protect the FDIC and other victims from further harm, and assist the FDIC in recovery of its losses. Pursuing appropriate criminal penalties not only serves to punish the offender but can also deter others from participating in similar crimes. Our criminal investigations can also be of benefit to the FDIC in pursuing enforcement actions to prohibit offenders from continued participation in the banking system. When investigating instances of financial institution fraud, the OIG also defends the vitality of the FDIC's examination program by investigating associated allegations or instances of criminal obstruction of bank examinations and by working with U.S. Attorneys' Offices to bring these cases to justice.

The OIG'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, anti-phishing, and suspicious activity review 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** were 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 the results of our review of the FDIC's enforcement actions (EA) and professional liability claims (PLC) against institution-affiliated parties (IAP) and individuals. Additionally, we completed work regarding the FDIC's program for monitoring compliance with Bank Secrecy Act and anti-money laundering requirements. We also completed a material loss review during the reporting period –that of the failure of Bank of Union, El Reno, Oklahoma. Given the decreasing number of bank failures, we last issued a material loss review in September 2012.

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. Our failed bank review activity for the reporting period is presented in Appendix II.

From an investigative perspective, in support of ensuring the safety and soundness of the nation's banks, we have pursued cases involving fraud in both open and closed institutions. Results of such selected cases are also described below. 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.

Ongoing Dodd-Frank Act Risk Assessment and Monitoring Effort

The OIG is undertaking an ongoing initiative to keep current with the FDIC's efforts associated with implementation of risk management, monitoring, and resolution authorities emanating from the Dodd–Frank Act. Our purpose in doing so is to understand and analyze operational and political issues and emerging risks impacting the FDIC, the financial community, and internal OIG operations and plans. This continuous and focused risk assessment and monitoring enhances our more traditional, periodic OIG risk assessment and planning efforts and assists with the OIG's internal preparation efforts in the event a systemically important financial institution should fail. The assessment and monitoring is intended to provide an informal, efficient means of making management aware of issues and risks warranting attention — it is not being conducted as an audit or evaluation.

During the reporting period, we briefed FDIC senior management regarding our efforts and shared our approach with colleagues on the Council of Inspectors General on Financial Oversight.

Going forward, we anticipate communicating to FDIC management periodic summaries of any issues or risks for management consideration. We will also develop internal OIG products and conduct briefings to inform OIG executives and managers and aid them in their planning efforts.

Enforcement Actions Against Institution-Affiliated Parties and Professional Liability Claims Against Individuals and Entities Associated with a Failed Institution

The federal banking regulators have strong enforcement powers under section 8 of the FDI Act to address violations of law, breaches of fiduciary duty, or unsafe and unsound practices. The financial crisis had a profound and lasting impact on the banking industry and broader economy, resulting in the failure of 465 insured depository institutions (or institutions) over the 5-year period from 2008-2012 and losses totaling $86.6 billion to the DIF. In the wake of the crisis, members of the Congress, the media, and the general public have questioned whether the regulators sufficiently used these powers to hold accountable those individuals whose actions harmed institutions.

The OIGs of the FDIC, Treasury, and FRB/Consumer Financial Protection Bureau conducted a joint evaluation of (1) the regulators' efforts to investigate, pursue, and impose EAs against IAPs and (2) the FDIC's efforts to pursue PLCs against individuals and entities whose actions harmed institutions that ultimately failed. The evaluation focused on the 465 institution failures that occurred during the 5-year period from 2008-2012. These institutions were regulated by the FDIC, FRB, OCC, and the former Office of Thrift Supervision.

EAs against IAPs include removal/prohibition orders, civil money penalties, administrative restitution, and personal cease and desist orders. Removal/prohibition orders are the most severe actions and prohibit an IAP from participating in the affairs of any insured depository institution for life. Accordingly, the statutory criteria for sustaining a removal/prohibition order are rigorous and the regulators must prove three grounds: misconduct, effect of the misconduct, and culpability for the misconduct. To prove culpability, the regulators must show that the IAP exhibited personal dishonesty or a willful or continuing disregard for the safety or soundness of an institution. Proving willful or continuing disregard is particularly difficult, according to the regulators.

The regulators each have similar, formal processes to investigate and impose EAs on IAPs whose actions harmed institutions. These processes generally include an investigative period, agency review, an opportunity for the IAP to consent to the action, and a Notice of Charges if the IAP does not consent. A Notice of Charges triggers a review by an Administrative Law Judge, followed by an agency decision, and potentially an IAP appeals process.

The regulators issued a total of 275 EAs against individuals associated with 87 failed institutions, or 19 percent of the 465 institutions that failed. The majority of these EAs were imposed against institution directors and officers. As of September 30, 2013, potential EAs against IAPs were in-process related to an additional 59 failed institutions. These EAs will ultimately be closed-out or imposed. Of the total 275 EAs imposed, 128 were removal/prohibition orders against IAPs associated with 75 institutions (16 percent of the 465 failed institutions). The joint report notes that this is an increase over the banking crisis of the 1980s and early 1990s where the regulators imposed removal/prohibition orders against IAPs associated with about 6 percent of the institutions that failed from 1985 through 1995.

The Inspectors General determined that several factors appeared to impact the regulators' ability to pursue EAs against IAPs. Those factors included the rigorous statutory criteria for sustaining removal/prohibition orders; the extent to which each regulator was willing to use certain EA tools, such as personal cease and desist orders; the regulators' risk appetite for bringing EAs; EA statutes of limitation; and staff resources, among other things. In connection with these factors, the Inspectors General made recommendations related to evaluating approaches and developing methodologies to support issuing EAs against IAPs where the regulators can show that IAPs exhibited a willful or continuing disregard for safety or soundness and, also, increasing the use of personal cease and desist orders.

As for PLCs, the purpose of the professional liability program is to hold accountable directors, officers, and other professionals who caused losses to failed institutions. When an institution fails, the FDIC as Receiver acquires legal rights, powers, titles, and privileges, which include PLCs. The FDIC's Professional Liability Unit investigates 11 claim areas for each institution failure, regardless of the primary federal regulator, and pursues claims that are both meritorious and expected to be cost-effective. For a PLC to have merit, the FDIC must meet the burden of proof required by the federal or state law that applies to the claim. For a typical tort claim, the FDIC generally must show that the subject individual or entity owed a duty to the institution, breached that duty, and the breach caused a loss to the institution. According to FDIC officials, the threshold for misconduct to sustain a PLC can be lower than that for a removal/prohibition order. To collect on these claims, the FDIC as Receiver typically must sue the individuals or entities for losses resulting from their breaches of duty to the failed institution. Recovery sources include liability insurance policies, fidelity bond insurance policies, and the assets of the individuals or entities pursued.

The FDIC has a formal process for investigating and pursuing PLCs. In that regard, the FDIC completed[1] 430 PLCs and had an additional 305 pending a final result based on litigation or negotiation as of September 30, 2013. In total, the 735 completed and pending PLCs were associated with 193 of the 465 failed institutions (42 percent). Of these 735 completed and pending PLCs, 162 pertained to directors and officers associated with 154 of the 465 failed institutions (33 percent). During the banking crisis of the 1980s and early 1990s, the FDIC brought claims against directors and officers in 24 percent of the failed institutions.

A key factor impacting the pursuit of PLCs was the increased use of insurance policy exclusions as the financial crisis unfolded that excluded or attempted to exclude coverage for claims made by the FDIC as Receiver. Other factors include applicable federal or

---

[1] Completed PLCs comprised settlements and court judgments to pay the FDIC and cases dismissed by the courts. Of the 430 completed PLCs, 379 resulted from settlements, 32 resulted from court judgments, and 19 were dismissed.

state law standards in support of meritorious claims, limited recovery resources, and a court decision pertaining to another agency that resulted in the FDIC limiting its use of tolling agreements to extend the statutes of limitation on PLCs. The Inspectors General recommended that the FDIC research ways to compensate for lost revenues as a result of insurance policy exclusions. The Inspectors General also recommended that the OCC and FRB inform their regulated institutions about the risks related to insurance policy exclusions. Finally, the joint report includes a recommendation that with respect to tracking and reporting PLC expense and recovery information, the FDIC should take steps to provide more institution-specific information to members of its Board of Directors.

The joint report was issued to the Chairman of the FDIC, Chair of the Board of Governors of the Federal Reserve, and Comptroller of the Currency. In their responses, these officials agreed with all recommendations and committed to take responsive actions to address OIG findings.

The FDIC's Response to Bank Secrecy Act and Anti-Money Laundering Concerns Identified at FDIC-Supervised Institutions

FDIC-supervised financial institutions are responsible for developing and administering a program to assure and monitor compliance with the Bank Secrecy Act (BSA) and related regulations (referred to as a BSA Compliance Program). The FDIC is responsible for regularly reviewing BSA Compliance Programs, communicating identified deficiencies and apparent violations to the institution's management and Board of Directors (and other regulatory authorities, as appropriate), and taking supervisory action to address the associated risks.

Within the FDIC, RMS has primary responsibility for examining financial institutions for compliance with the BSA and related regulations. Because RMS considers BSA compliance to be a matter of safety and soundness, each on-site risk management examination includes an assessment of the institution's BSA Compliance Program. Any deficiencies in BSA Compliance Programs or apparent violations of BSA-related regulations identified by examiners are documented in reports of examination and visitation reports that are provided to the institution's management and Board of Directors. The FDIC's primary system of record for recording information about BSA examinations and related supervisory activities is the Virtual Supervisory Information on the Net.

We conducted an audit to determine how the FDIC has responded to BSA and anti-money laundering (AML) concerns identified in reports of examination. In doing so, we determined the extent and types of supervisory actions that the FDIC has taken to address BSA/AML concerns. We also assessed the extent to which supervisory actions, including referrals of apparent violations to other federal agencies, comply with applicable statutes; interagency policy and guidance; and FDIC policies, procedures, and guidelines. Further, we evaluated the consistency of RMS's Regional Offices in applying BSA/AML-related policies, procedures, and guidelines.

By way of background, in response to BSA/AML concerns identified in reports of examination, RMS implements supervisory actions ranging from examiner recommendations that address isolated BSA/AML deficiencies to formal EAs that address systemic weaknesses in BSA Compliance Programs. Serious BSA concerns can also result in referrals to the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) for the issuance of civil money penalties.

We reported that during the 4-year period October 1, 2009, through September 30, 2013, the FDIC and/or applicable state regulator cited FDIC-supervised institutions for 3,294 apparent violations of BSA-related regulations, agreed to or issued 175 BSA-related informal and formal EAs, and made 22 referrals to FinCEN for civil money penalties. In addition, the reports of examination and visitation reports that we reviewed identified the specific BSA regulations that were violated, the nature and causes of the violations, the recommended corrective actions, and the institutions' management responses.

Further, follow-up examinations and visitations were generally conducted in a timely manner.

Our review of the FDIC's supervisory actions to address BSA/AML concerns at 51 non-statistically sampled financial institutions found that the actions were generally consistent with applicable statutory requirements, interagency policy and guidance, and FDIC policies, procedures, and guidelines. However, in 4 of 15 cases involving BSA Compliance Program failures and/or repeat apparent violations of BSA program requirements, stronger or earlier supervisory action in the form of a formal enforcement action may have been warranted. Based on the results of subsequent examinations, two of the four institutions took action to improve their BSA Compliance Programs. Although FDIC management provided a rationale for the supervisory approach applied in these cases, promptly issuing formal EAs would have established a supervisory tenor of expectations consistent with interagency policy.

Our review also identified a potential control improvement with respect to recording in the Virtual Supervisory Information on the Net the status and disposition of civil money penalties referrals to FinCEN.

The FDIC has established a number of controls to promote consistency among RMS Regional Offices in applying BSA/AML-related policies, procedures, and guidelines. Such controls include, for example, bimonthly meetings between the Regional Offices and RMS headquarters' Anti-Money Laundering and Risk Analysis Branch to discuss BSA/AML problem institutions, the examination report review process, and periodic internal reviews by RMS' Internal Control and Review Section. In addition, RMS' Regional Offices generally appeared to apply BSA/AML-related policies, procedures, and guidelines in a consistent manner for the institutions that we reviewed. However, Regional Office procedures for monitoring institutions with significant BSA/AML problems were not always current, and we noted differences among these Regional Office procedures.

We made three recommendations to improve RMS' internal controls for addressing BSA/AML concerns identified during examinations of FDIC-supervised institutions. Management concurred with the recommendations and described planned corrective actions to address them.

Material Loss Review of The Bank of Union, El Reno, Oklahoma

On January 24, 2014, the Oklahoma State Banking Department (OSBD) closed The Bank of Union (BOU), and the FDIC was appointed receiver. The FDIC notified the OIG on March 10, 2014, that BOU's total assets at closing were $243.7 million and that the estimated loss to the DIF was $70 million (or 29 percent of BOU's total assets). We engaged KPMG LLP to conduct a material loss review of BOU to determine the causes of BOU's failure and the resulting material loss to the DIF and evaluate the FDIC's supervision of BOU, including the FDIC's implementation of the Prompt Corrective Action provisions of section 38 of the FDI Act.

BOU was chartered in 1900 in Union City, Oklahoma, and became insured by the FDIC in 1959. In 1992, the bank opened an office in El Reno, Oklahoma, which is located approximately 25 miles west of Oklahoma City. BOU relocated its main office to El Reno in 2007 while maintaining a branch office in Union City. The bank also maintained a loan production office in Oklahoma City. Union City Corporation (UCC), a one-bank holding company, owned all of BOU's stock. UCC's principal shareholders consisted of two siblings, each of whom owned 41 percent of UCC's stock. Neither sibling served on BOU's Board of Directors (Board). The chairman of BOU's Board, who also served as the bank's president and chief executive officer (CEO) — herein referred to collectively as the CEO — until November 2013, owned 15 percent of UCC's stock. UCC's remaining shares consisted of treasury stock. BOU was a community bank that offered traditional banking services to local businesses and consumers.

The bank's assets were centered in its loan portfolio, which had large concentrations in commercial and industrial (C&I) and agricultural loans. Most of BOU's C&I loans were made to rural cattle ranching and trucking businesses and were generally secured by assets such as livestock, equipment, single-family residences, and oil and gas leases. The bank's agricultural loans were made to cattle and farming operations and were primarily secured by livestock, ranch land, and trucking and farming equipment.

We reported that BOU failed primarily because its Board and management did not effectively manage the risks associated with the bank's aggressive growth and concentrations in C&I and agricultural loans, particularly in the livestock and trucking industries. Notably, BOU's lending function lacked adequate internal controls and sufficient seasoned loan officers to effectively manage the growth and complexity of the loan portfolio. For example, BOU lacked an adequate loan review function and credit grading system and frequently extended, deferred, and renewed loans without fully assessing the borrowers' ability to repay or adequately inspecting collateral, when appropriate. BOU's oversight and management of account overdrafts was also inadequate. These inadequate internal controls and certain actions of the CEO clouded the true financial condition of BOU's loan portfolio. BOU also had a large and complex borrowing relationship that was not adequately administered, exposing the bank to significant credit risk and losses.

In general, BOU's Board was not sufficiently engaged in overseeing the bank's lending strategies and practices. The Board relied heavily upon the CEO, who exercised significant control over the lending function after the departure of senior lending officials in 2012 and made many of the decisions to originate and renew loans that were ultimately charged off. Significant financial deterioration in BOU's loan portfolio became apparent in 2012, and by the close of the 2013 joint examination, BOU's past due and nonaccrual loans totaled $157.8 million (or 54 percent of the loan portfolio). A substantial portion of these loans consisted of livestock and trucking loans. The bank recognized approximately $157.3 million in loan losses between January 2011 and the bank's failure, depleting its earnings and eroding its capital. The OSBD closed BOU due to the bank's inability to raise sufficient capital to support safe and sound banking operations.

With respect to the FDIC's supervision of BOU, the FDIC, in coordination with the OSBD, provided ongoing supervisory oversight of BOU through regular onsite examinations, visitations, targeted reviews, and various offsite monitoring activities. Through its supervisory efforts, the FDIC identified risks in the bank's operations as early as 2008 and brought these risks to the attention of the institution's Board and management through examination reports, a visitation report, correspondence, and informal and formal EAs. Such risks included inadequate Board and management oversight of the bank's complex structured credit products, lending practices (including loan administration and monitoring), and loan portfolio. With the benefit of hindsight, BOU's practice of continually extending, deferring, and renewing its livestock loans warranted an elevated level of scrutiny because such credits are typically structured as short-term loans that are paid off when the underlying collateral (i.e., livestock) is liquidated. When the structure and purpose of such loans are not properly aligned and enforced, the ability of bank management to effectively monitor the loans and identify performance problems can become compromised.

In the overall context of the examination findings, the February 2011 joint examination resulted in an upgrade to BOU's supervisory ratings, the termination of a memorandum of understanding, and the extension of the on-site examination interval from 12 to 18 months. At that time, BOU was experiencing rapid growth in its agricultural and C&I loans secured primarily by livestock and exhibited weak loan underwriting, administration, and monitoring practices, which were repeat concerns from the prior examination. The February 2011 report of examination recommended that BOU improve its loan administration practices with respect to extensions, deferrals, and renewals. However, BOU did not address those recommendations and continued its practice of extending, deferring, and renewing loans.

We reported that, in retrospect, it would have been prudent for the FDIC to have followed up with the bank to ensure these repeat concerns were promptly corrected. Further, a more comprehensive assessment of BOU's largest borrowing relationship—which primarily involved livestock loans—may have uncovered the bank's practice of using account overdrafts to keep the debt of certain borrowers within the relationship current. In addition, the report of examination was not critical of BOU's inadequate collateral inspections related to livestock loans.

Following the February 2011 joint examination, BOU's CEO assumed significant control over the lending function after the departure of three senior lending officials, and the bank's credit risk exposure increased. The October 2012 examination identified substantial loan losses, significant financial deterioration, and risky management practices that led to the OSBD promptly issuing an order against the bank. Among other things, the order resulted in a $40 million capital injection and significantly limited the bank's ability to extend new credit, helping to expose the degree to which certain borrowers of the bank, including its largest borrowing relationship, were unable to pay their debt. The regulators also raised concern about the independence and reliability of collateral inspections related to BOU's largest borrowing relationship. In response, bank management obtained a new inspection in December 2012 covering much of the collateral supporting the relationship's debt, although examiners later determined that the inspection's independence and reliability were questionable. These supervisory actions, however, could not reverse the substantial losses already embedded in the bank's loan portfolio, which led to the bank's failure.

The FDIC increased its supervisory monitoring and oversight of BOU following the October 2012 examination and, in June 2013, jointly issued a Consent Order with the OSBD against the bank. In conjunction with the October 2013 examination, the FDIC performed a targeted review that identified bank accounts administered by the CEO that were significantly and repeatedly overdrawn without proper approval during 2011 and 2012. In some cases, funds from overdrafts were used to make payments on existing loans and keep borrowers' debt current, and new loans were subsequently made to pay borrower overdrafts and service their debts. Such actions had the effect of clouding the financial condition of the borrowers and the performance of their loans.

Under the FDIC's forward-looking approach to bank supervision, which was re-emphasized to the FDIC examination workforce in 2010, banks with weak risk management practices are subject to increased supervisory analysis and a proactive supervisory response when risks are not properly managed. With respect to BOU's agricultural and C&I loans, including livestock loans, such a response could have involved holding the Board and management to a stronger commitment to address the weak lending practices identified during the February 2011 examination and more promptly following up to confirm that collateral inspections were adequate.

On July 16, 2014, the FDIC issued Financial Institution Letter (FIL)-39-2014, entitled *Prudent Management of Agricultural Credits Through Economic Cycles.* The FIL reminds FDIC-insured institutions that engage in agricultural lending to maintain sound underwriting standards, strong credit administration practices, and effective risk management strategies. These include, for example, analyzing the overall financial status of borrowers, including secondary repayment sources and collateral support levels; documenting all lien perfections; and conducting timely, independent collateral inspections. When an institution fails to adequately implement these lending practices, as was the case with BOU, there is an increased risk to the institution and, ultimately, the DIF.

Based on the supervisory actions taken with respect to BOU, the FDIC properly implemented the applicable Prompt Corrective Action provisions of section 38.

In responding to our report, management reiterated the causes of BOU's failure and the supervisory activities described in the report. Management also agreed that, in retrospect, it would have been prudent to have followed up with the bank after the February 2011 joint examination to ensure that repeated concerns relative to loan extensions, deferrals, and renewals were properly corrected.

OIG Investigations Address Financial Institution Fraud

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

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

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, attorneys, and other individuals involved in residential and commercial lending activities were also implicated in a number of our cases. These cases are conducted by the OIG's special agents in our headquarters and regional offices and reflect nationwide activity and results. The OIG's working partnerships with the Corporation and law enforcement colleagues in all such investigations contributes to ensuring the continued safety and soundness of the nation's banks.

Seven Former Bank Officials Sentenced in Loan Fraud Scheme

In mid-June 2014, seven former bank officials of the First National Bank of Savannah, Savannah, Georgia, were sentenced for their roles in a complex bank fraud scheme. The long-running conspiracy and fraud scheme contributed to the demise of First National Bank, which failed on June 25, 2010.

As First National Bank'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; 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.

Sentences for the former bank officials were as follows:

- The former president and CEO was sentenced to serve 42 months in prison to be followed by 3 years of supervised release and was ordered to pay $9,749,265 in restitution.
- The former vice president and chief credit officer was sentenced to serve 2 years of probation and was ordered to pay $14,800 in restitution.
- The former city president (Richmond Hill branch) and commercial loan officer was sentenced to serve 10 months in prison to be followed by 3 years of supervised release and was ordered to pay $57,771 in restitution.
- The former executive vice president and chief financial officer was sentenced to serve 20 months in prison to be followed by 3 years of supervised release and was ordered to pay $72,571 in restitution.
- The former city president and chief lending officer was sentenced to serve 38 months in prison to be followed by 3 years of supervised release and was ordered to pay $158,518 in restitution.

- The former senior vice president and commercial loan officer was sentenced to serve 22 months in prison to be followed by 3 years of supervised release and was ordered to pay $157,544 in restitution.
- The former city president of the Tybee Island branch and commercial loan officer was sentenced to serve 38 months in prison to be followed by 3 years of supervised release and was ordered to pay $3,891,870 in restitution.

Source: *U.S. Secret Service.*
Responsible Agencies: *This is a joint investigation conducted by the FDIC OIG, FRB 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 Director Who Faked His Own Death Pleads Guilty to Bank, Wire, and Securities Fraud

On June 5, 2014, a former director at Montgomery Bank & Trust (MB&T), Ailey, Georgia, which failed on July 6, 2012, pleaded guilty to bank fraud, securities fraud, and wire fraud. He also consented to an order of prohibition from further participation in banking and consented to orders of forfeiture representing money judgments in the amount of $51 million. Previously, on July 11, 2012, the former director was indicted by a federal grand jury and charged with bank fraud in the Southern District of Georgia. On January 25, 2013, the former director was indicted in the Eastern District of New York and charged with securities and wire fraud.

According to the plea agreement, beginning in December 2010, the former director convinced a group of investors to invest $10 million in MB&T. Other investors, including MB&T employees, invested an additional $4 million into MB&T. As a result, he was made a director of MB&T and was trusted with investing the bank's liquidity. Over the next 18 months, the former director misappropriated and embezzled the bank's investments, resulting in losses from speculative trading and other investing. To cover up the losses, he provided the bank with fabricated documents, falsely indicating that $17 million was on deposit in the bank's name at a large financial services firm in New York, when in fact, those funds had been lost.

Between June 2009 and June 2012, the former director, through his firm, PFG LLC, raised approximately $51 million from 151 individual investors. He lost the majority of those investors' funds through speculative trading and other investments. To hide the losses, he set up a secure PFG Web site for his investors that depicted account statements with fictitious assets and fabricated investment returns. In addition, on April 29, 2011, as part of his scheme, he caused a wire in the amount of $4,530,000 to be transferred among accounts.

In mid-June 2012, the former director sent acquaintances "suicide letters" in which he admitted he had defrauded MB&T Bank and his PFG investors, and suggested that he planned to kill himself by throwing himself off a high-speed ferry boat after it left the coast of Florida. As a result of the suicide claim, the United States Coast Guard searched for the former director's body, to no avail. In fact, shortly after sending the letters, the former director disappeared. After a several-month search, on December 31, 2013, he was arrested after he presented a false identification to a member of the Glynn County Georgia Sheriff's Department during a routine traffic stop in Brunswick, Georgia. He has remained in custody since that time.

Source: *This case was initiated based on information received from the FDIC RMS.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG and the Federal Bureau of Investigation (FBI). The case is being prosecuted by the U.S. Attorney's Office for the Southern District of Georgia.*

Former Bank Director Convicted for Misapplication

On September 26, 2014, the former director and treasurer, Metropolitan Savings Bank, Pittsburgh, PA, was convicted by a jury on nine counts of misapplication of bank funds.

The former director and treasurer, with the assistance of the former director and vice president of the bank, embezzled approximately $300,000 from Metropolitan between January 2005 and March 2006. The former director and treasurer received seven Metropolitan cashier's checks payable either to himself or to banks or loan servicers which were used to pay off loans that the former director and treasurer had at other institutions. The former director and vice president also sent two wire transfers to mortgage servicing companies to pay off the former director and treasurer's loans. The former director and treasurer did not complete any applications, or sign notes or security agreements for the advances. Metropolitan procedures required all loans to be approved in advance by the Board of Directors. Neither of the two former officers mentioned any of the subject advances to the Board of Directors either before or after they were extended. The former director and vice president is currently serving a 6-year prison sentence for filing false Call reports with the FDIC.

Source: *FDIC DRR and 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 Western District of Pennsylvania.*

Former Senior Vice President Sentenced in Embezzlement Case

On July 22, 2014, the former senior vice president, Grant County Deposit Bank, Williamstown, Kentucky, was sentenced to one year and one day in prison, 3 years of supervised release, and ordered to pay restitution of $93,776. In March, 2014 the former senior vice president pleaded guilty to a one-count Information charging her with embezzlement.

Starting in August 2010 and through July 2013, the former senior vice president used her position and knowledge of the bank's accounting system to embezzle the funds. Using 82 stolen cashier's checks, she moved funds to accounts under her control and in the name her husband. Subsequently, she made 43 entries into the bank's computer system to hide the transactions from bank management and external auditors.

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 Kentucky.*

Former Bank Branch Manager Sentenced

On July 30, 2014, a former branch manager from Guaranty Bank, Springfield, Missouri, was sentenced to serve 46 months in prison to be followed by 5 years of supervised released. She was also ordered to pay restitution of $547,897. The former branch manager had pleaded guilty to a criminal Information on September 12, 2013, in which she was charged with bank fraud, money laundering, and filing a false tax return.

The fraud was detected when the former branch manager issued and authorized three checks on the bank account of a victim who had died the previous day. The former branch manager admitted that, from December 2006 until November 2012, she repeatedly accessed the bank accounts of four elderly bank customers and embezzled a total of $316,598 from those accounts.

The former branch manager submitted transaction tickets, withdrawal slips, and cashier's checks on which she forged the names of the account holders in order to withdraw money from the bank accounts. She used the money for personal matters and expenses. She set the customer accounts to "do not mail" status in order to keep the customers from receiving their bank statements and detecting the theft from their bank accounts.

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

Former Bank Employee Sentenced

On July 14, 2014, a former loan clerk at Exchange State Bank, St. Paul, Kansas, was sentenced to serve one year and a day in prison to be followed by 3 years of supervised release. She was also ordered to pay restitution in the amount of $274,279. The former loan clerk had pleaded guilty for her role in an embezzlement scheme on April 21, 2014.

From August 2007 until May 2013, she embezzled approximately $274,279 and used the money for her personal benefit. She was able to accomplish the theft by diverting funds from the bank's general ledger, diverting interest from a bank-owned deposit account, and making fraudulent advances of unsuspecting borrowers' lines of credit.

Source: *FDIC RMS.*
Responsible Agencies: *The FDIC OIG conducted the investigation with assistance from the U.S. Secret Service. This case is being prosecuted by the U.S. Attorney's Office for the District of Kansas.*

Employee Sentenced for His Role in Commercial Loan Fraud

A joint investigation conducted with the FBI revealed that between December 2006 and February 2008, two developers doing business as Spyglass Properties, LLC, aided by a Spyglass employee, submitted false documentation to ANB Financial in connection with a $17.4 million construction loan to develop an 82-unit condo complex in Salt Lake City, Utah. Loan proceeds were diverted and used to purchase vehicles and real estate and to complete other projects unrelated to the ANB Financial loan.

In connection with this case, on November 9, 2009, asset seizure warrants were unsealed. Assets were seized from one of the developers, including numerous vehicles, bank accounts, and real estate. On December 2, 2009, a criminal Information was filed against the employee charging him with one count of wire fraud. On December 9, 2009, a 24-count Indictment was issued against both developers, charging them with conspiracy, wire fraud, and money laundering.

In a prior reporting period, one of the developers pleaded guilty to wire fraud and money laundering. On September 4, 2013, he was sentenced to serve 12 months and 1 day in prison to be followed by 36 months of supervised release. He was also ordered to pay restitution of $7 million. The other developer was sentenced to serve 12 months and 1 day in prison to be followed by 60 months of supervised release. He was also ordered to pay restitution of $7 million, joint and several with his business associate.

On April 1, 2014, the employee was sentenced to 24 months of probation and ordered to pay $1.7 million in restitution.

Source: *This investigation was initiated based on a referral from the FDIC DRR.*
Responsible Parties: *This is a joint investigation with the FDIC OIG and FBI. This case was prosecuted by the U.S. Attorney's Office for the District of Utah.*

Guilty Pleas and Sentencing for Bank Fraud and Bank Bribery

We participated in an investigation based on a request for assistance from the FBI and United States Attorney's Office, District of Colorado, regarding allegations of fraudulent activities of the former vice president and loan officer of Colorado East Bank & Trust (CEBT), Lamar, Colorado. According to the referral, the former vice president and loan officer had received kickbacks for originating loans in excess of $1.1 million to a CEBT customer and related entities without loan committee approval or proper authority and misrepresented collateral and other material information, resulting in a loss to CEBT of $1,055,918. In addition, the former bank official and customer were thought to have engaged in a "fix and flip" home-purchase scheme.

We conducted a joint investigation with the FBI and the Special Inspector General for the Troubled Asset Relief Program (SIGTARP). On September 25, 2013, both the bank officer and the customer were charged in a 22-count Indictment with bank fraud and bank bribery. On March 24, 2014, the former vice president and loan officer pleaded guilty to bank fraud and bank bribery. On September 30, 2014, he was sentenced to serve 36 months in prison, followed by 4 years of supervised release, and ordered to pay restitution of $1,055,918. On June 26, 2014, the customer pleaded guilty to bank bribery, and his sentencing hearing was set for October 3, 2014.

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

Businessman Pleads Guilty to Bank Fraud

On July, 1, 2014, the owner and president of Curry Auto Leasing pleaded guilty to a one-count criminal Information charging him with bank fraud.

Curry Auto Leasing was engaged in multiple fraudulent transactions related to leases financed by several North Texas financial institutions, including Texas Capital Bank, Dallas, Texas. Curry Auto Leasing is a vehicle and equipment leasing company and finances the leases it secures for its customers through multiple financial institutions. In exchange for financing the lease agreements for Curry Auto Leasing, the lending institution is required to have certain paperwork filed on their behalf to secure the bank's interest in the transactions. The former owner and president is alleged to have falsified, altered, or omitted various paperwork related to the transactions, including lease agreements and vehicle titles, in order to secure money from multiple banks, resulting in losses to those banks of approximately $1 million.

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

Former Owner of Sacramento Capitals Tennis Team Pleads Guilty to $50 Million Fraud Scheme

On May 8, 2014, the former owner of the now-defunct Sacramento Capitals tennis team pleaded guilty to wire fraud charges for his role in a scheme to defraud individuals, corporations, and financial institutions, including Bridge Bank, San Jose, California, of as much as $50 million.

The former tennis team owner admitted that from 2002 to 2014, he convinced more than 100 victims, including individuals, corporate entities, and financial institutions, to invest in a number of business opportunities by misrepresenting his own financial worth and that of his companies. Those companies, IMG and Relyaid, were involved in the international manufacture, shipment, and distribution of latex gloves. He falsely claimed that these companies did tens of millions of dollars in business with federal agencies every year, most notably the Department of Veterans Affairs (VA). In 2013, he claimed to have more than $125 million in VA contracts alone. In fact, while he did have a contract with the VA, it was only worth up to $25,000 a year. In all, he ultimately obtained well over $150 million from his victims. Contrary to his representations, he used much of the money he obtained to pay himself and his family, make lulling payments to participants in his fraudulent investment schemes, and to pay outstanding debts unrelated to his false representations.

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

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

On May 16, 2014, a father and son, who were the former CEO and chief financial officer (CFO), respectively, of QC Manufacturing, LLC, were sentenced for conspiracy to commit bank fraud. The former CFO was also sentenced for money laundering. The former CEO was sentenced to serve 12 months in prison to be followed by 36 months of supervised release, and was ordered to pay restitution of $1,387,816 to the FDIC, joint and several with his son, the former CFO. The son was sentenced to 12 months of home confinement to be followed by 36 months of supervised release, and was ordered to pay restitution of $1,387,816 to the FDIC, joint and several with his father.

The two, through their company, 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 U.S. 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, and the U.S. Department of Agriculture OIG with assistance from the U.S. Postal Inspection Service and SIGTARP. The case is being prosecuted by the U.S. Attorney's Office for the Central District of Illinois.*

Leader and Organizer of $49.6 Million Mortgage Fraud Scheme Sentenced to 27 Years and 3 Months in Prison

On September 30, 2014, a developer was sentenced for his role as a leader and organizer of a $49.6 million bank fraud and wire scheme, perpetrated from approximately 2003 through 2008. The developer was sentenced to 27 years and 3 months in prison for his role in the fraud scheme.

On July 3, 2014, he and three co-defendants–his ex-wife and two other conspirators–were convicted of conspiracy to commit bank fraud and wire fraud after an 11-day jury trial. He and the two other conspirators were also convicted of various bank fraud offenses.

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

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

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

The developer's ex-wife and the two other conspirators were scheduled to be sentenced at a later date.

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

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

Sentencing in Mortgage Fraud Case

On May 9, 2014, a closing attorney was sentenced in the Eastern District of New York for her role in a conspiracy to commit wire fraud. She was sentenced to 87 months in prison followed by 3 years of supervised release and was ordered to pay $1,205,355 in restitution. In addition, the judge signed a forfeiture order in the amount of $43,701.

As discussed in a prior semiannual report, between September 2005 and April 2011, the closing attorney, along with other straw buyer recruiters and a loan officer, conspired to commit wire fraud. As part of the scheme, the 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 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. The 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.

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.*

Former Massachusetts Attorney Sentenced for Mortgage Fraud

A former attorney practicing in Boston was sentenced on April 9, 2014, for his involvement in a mortgage fraud scheme that resulted in more than $2.5 million in losses. He was sentenced to 33 months in prison and 36 months of supervised release. He was also ordered to pay $977,042 in restitution to defrauded lenders. In November 2013, the former attorney pleaded guilty to wire fraud, mail fraud, and unlawful monetary transactions.

The attorney participated in at least 13 fraudulent real estate transactions involving triple-decker apartment buildings in various sections of Boston, including Dorchester, Roxbury, and Jamaica Plain. For eight of those transactions, he served as the real estate closing attorney representing the mortgage lender. For the other five, he participated as the seller of real property himself. The basic scheme involved recruiting people to buy properties by promising to pay them as much as $40,000 per transaction, which was not disclosed to the lenders. Many of the buyers were also promised that the seller would pay the mortgage for upwards of a year. Also central to the scheme was telling the lenders that each borrower intended to occupy the property as a primary residence, which was not true.

Many of the payments to buyers were made directly from the attorney's law firm bank account on transactions for which he was the closing attorney, but he failed to disclose those payments to the mortgage lenders that he represented. He also received some of the loan proceeds in addition to his legal fees, another fact that was not disclosed to the lender. In one transaction, he received more than $50,000.

Each of the loans given for these 13 transactions went into default, usually 12-18 months after the transaction, and all the properties were sold at foreclosure or through a short sale, resulting in combined losses to the lenders of more than $2.5 million.

Source: *This investigation was initiated based on a referral from the Massachusetts Board of Bar Overseers to the U.S. Attorney's Office for the District of Massachusetts, Boston, Massachusetts.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, U.S. Secret Service, IRS-CI, and the U.S. Postal Inspection Service. The case was prosecuted by the U.S. Attorney's Office for the District of Massachusetts.*

Strong Partnerships with Law Enforcement Colleagues

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

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

We also worked closely with the Department of Justice; FBI; other OIGs; other federal, state, and local law enforcement agencies; and FDIC divisions and offices as we conducted our work during the reporting period.

Keeping Current with Criminal Activities Nationwide

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

OIG Headquarters	Financial Fraud Enforcement Task Force, National Bank Fraud Working Group--National Mortgage Fraud Working Sub-group.
New York Region	The Northern Virginia Real Estate Fraud Initiative Working Group, Manassas, Virginia; Maine Suspicious Activity Report (SAR) Review Team; Maryland Mortgage Fraud Task Force; 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; Northern District of Georgia SAR Review Team; Middle District of Georgia SAR Review Team; South Carolina Financial Fraud Task Force.
Kansas City Region	St. Louis Mortgage Fraud Task Force; Kansas City Financial Crimes Task Force; Minnesota Inspector General Council meetings; Kansas City SAR Review Team; Springfield Area Financial Crimes Task Force; Nebraska SAR Review Team; Iowa Mortgage Fraud Working Group.
Chicago Region	Dayton, Ohio, Area Financial Crimes Task Force; Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Detroit SAR Review Team; Financial Investigative Team, Milwaukee, Wisconsin; Milwaukee Mortgage Fraud Task Force; Madison, Wisconsin, SAR Review Team; Indiana Bank Fraud Working Group.
San Francisco Region	FBI Seattle Mortgage Fraud Task Force, Fresno Mortgage Fraud Working Group for the Eastern District of California, Sacramento Mortgage Fraud Working Group for the Eastern District of California, Sacramento SAR Working Group, Los Angeles Mortgage Fraud Working Group for the Central District of California, Orange County Financial Crimes Task Force-Central District of California.
Dallas Region	SAR Review Team for Northern District of Mississippi, SAR Review Team for Southern District of Mississippi, Oklahoma City Financial Crimes SAR Review Work Group, Austin SAR Review Working Group.
Electronic Crimes Unit	Washington Metro Electronic Crimes Task Force, Botnet Threat Task Force, High Technology Crime Investigation Association, Cyberfraud Working Group, Council of the Inspectors General on Integrity and Efficiency Information Technology Subcommittee, National Cyber Investigative Joint Task Force.

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 $83 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 June 30, 2014, the DIF balance was $51.1 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. Risk-management activities include approving the entry of new institutions into the deposit insurance system, off-site risk analysis, assessment of risk-based premiums, and special insurance examinations and enforcement actions. In light of increasing globalization and the interdependence of financial and economic systems, the FDIC also supports the development and maintenance of effective deposit insurance and banking systems world-wide.

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

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

To help the FDIC maintain the viability of the DIF, the **OIG's 2014 performance goal** was as follows:

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

OIG Work in Support of Goal 2

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

Strategic Goal 3

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

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

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

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

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

Every year fraud schemers attempt to rob consumers and financial institutions of millions of dollars. The OIG's Office of Investigations can identify, target, disrupt, and dismantle criminal organizations and individual operations engaged in fraud schemes that target our financial institutions or that prey on the banking public. OIG investigations have identified multiple schemes that defraud consumers. 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** were 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 did not conduct audit or evaluation work directly related to consumer protection matters. We did, however, coordinate 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 consumer protection responsibilities that the various parties carry out. We also continued efforts to protect consumers by way of our Electronic Crimes Unit's involvement in investigating email schemes that prey on the public.

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

Electronic Crimes Unit Responds to Email and Other Schemes

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

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

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

The OIG’s inquiry intake system supplements the OIG Hotline function. The Hotline continues to address allegations of fraud, waste, abuse, and possible criminal misconduct. However, over the past several years, our office has continued to receive a large number of public inquiries ranging from media inquiries to requests for additional information on failed institutions to pleas for assistance with mortgage foreclosures to questions regarding credit card companies and banking practices. These inquiries come by way of phone calls, emails, faxes, and other correspondence. The OIG makes every effort to acknowledge each inquiry and be responsive to the concerns raised. We coordinate closely with others in the Corporation through the FDIC’s Public Service Provider working group and appreciate their assistance. We handle those matters within the OIG’s jurisdiction and refer inquiries, as appropriate, to other FDIC offices and units or to external organizations. During the past 6-month period, we addressed approximately 140 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, with the exception of systemic failures. 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. In our last semiannual report, we noted that since loss sharing began during the most recent crisis in November 2008, the Corporation had entered into 304 shared-loss agreements. The initial asset balance of the covered assets in these shared-loss agreements was $216.3 billion. As of September 30, 2014, 289 of those shared-loss agreements were still active and 15 were terminated. As of that same date, the balance of assets in those 289 shared-loss agreements was $60.6 billion.

Under these agreements, the FDIC agrees to absorb a portion of the loss — generally 80-95 percent — which may be experienced by the acquiring institution with regard to those assets, for a period of up to 10 years. As another resolution strategy, the FDIC entered into 35 structured sales transactions involving 43,315 assets with a total unpaid principal balance of 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 September 30, 2014, DRR was managing 487 active receiverships with assets in liquidation totaling about $8.3 billion. As receiver, the FDIC seeks to expeditiously wind up the affairs of the receiverships. Once most of 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. Now, as the number of financial institution failures continues to decline, the Corporation is reshaping its workforce and adjusting its budget and resources accordingly. Between January 2012 and April 2014, the FDIC closed three of the temporary offices it had established to handle the high volume of bank failures. In this connection, authorized staffing for DRR, in particular, fell from a peak of 2,460 in 2010 to 1,463 proposed for 2013, which reflected a reduction of 393 positions from 2012 and 997 positions over 3 years. 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** were 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 continued work on 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 played a key role in a very successful case that resulted in seven former bank officers pleading guilty and being sentenced in June 2014 for their roles in 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. 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 government-wide 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 Services Oversight Council formed pursuant to the Dodd-Frank Act. FDIC systems contain voluminous amounts of critical data. The Corporation needs to protect against cyber threats 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.

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, and in late October 2014, the appointment of a new permanent CIO was announced.) Under the new organizational alignment, the CIO reports directly to the FDIC Chairman in fulfilling these strategic responsibilities and acts 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 is 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 helps ensure that the Chief Information Security Officer is able to provide an independent perspective on security matters to the CIO and ensures 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** were 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 three assignments in support of this goal area. We conducted a review the FDIC's Personnel Security and Suitability Program. We completed work in connection with the FDIC's IT project management. We also issued the results of an IT security-based review of the protection of sensitive information in Dodd-Frank Act resolution plans. At the end of the reporting period, among other assignments, we were completing our Federal Information Security Management Act of 2002 evaluation of the FDIC's information security program for 2014, and conducting work in such areas as travel card controls, controls over the destruction of archived paper records, and controls over outside counsel costs associated with professional liability claims. Completed reviews are summarized on the following pages.

The FDIC's Personnel Security and Suitability Program

The FDIC's Personnel Security and Suitability Program (PSSP) is designed to ensure that the Corporation employs and retains only those persons who meet all federal requirements for suitability (i.e., character, reputation, honesty, integrity, trustworthiness) and whose employment or conduct would not jeopardize the accomplishment of the Corporation's duties or responsibilities. A high-quality program is essential to minimizing the risks of unauthorized disclosures of sensitive information and to helping ensure that information about individuals with criminal activity or other questionable behavior is identified and assessed as part of the process for granting or retaining clearances. Further, potential missed red flags in the backgrounds of individuals who have recently committed serious crimes have brought renewed public and Congressional attention to the criticality and quality of background checks.

We conducted an evaluation to determine whether the FDIC is carrying out its PSSP efficiently and effectively. In doing so, we evaluated (1) FDIC management's overall administration of the program, including the extent to which applicable policies and procedures are in place and being followed; (2) oversight and administration of the contract supporting the program; and (3) the nature, extent, allowability, and reasonableness of costs incurred under the contract supporting the program. We engaged BDO USA, LLP to assist in this review, which covered the period from January 2011 through July 2013.

During our evaluation, the PSSP was in a state of transition and various aspects of the program were evolving and being improved. In furtherance of those efforts, we reported that the FDIC could strengthen controls in the following areas:

Overall Program Administration. Most preliminary clearance and adjudication determinations we reviewed were completed appropriately. However, we questioned a number of decisions and found that some decisions lacked support; not all background investigations performed were commensurate with a position's risk level designation; some background investigations were not timely; and many investigation case files were missing key documentation. We concluded that our test results could be attributed to weaknesses in policies and procedures, and management resource issues such as continuity and span of control. The Security and Emergency Preparedness Section (SEPS) indicated that it made a number of program changes following our testing period and realized meaningful program improvements in late 2013 and early 2014, to name a few:

- Eliminating case backlogs, thereby reducing processing times, both on the front-end for background investigation submissions to the Office of Personnel Management (OPM) and the back-end for completed case adjudications;
- Implementing the use of OPM's e-QIP system for electronic submission of background investigation questionnaires for all employees and contractors to reduce case review time and processing errors;
- Reviewing all FDIC position descriptions to ensure they had appropriate position sensitivity determinations; and
- Reorganizing SEPS and hiring an experienced Security Operations Unit manager to provide day-to-day supervision and management of the security support contract and federal staff.

SEPS also began an effort to digitize background investigation files and automate the PSSP process through an enterprise content management platform, known as the Personnel Security Records (PERSEREC) project. This effort is intended to improve records management, program efficiency, and performance reporting.

Contract Oversight. Most contractor charges that we reviewed were supportable and contract modifications were appropriately executed. However, we identified a few exceptions related to contractor overtime hours, labor category mix, the timely signature of modifications, and written approvals for key personnel changes. Further, while we determined that most contractor staff met minimum qualifications, we identified two staff that did not. Finally, we concluded that contract oversight could be strengthened by SEPS establishing better criteria for measuring contractor production and performance. SEPS developed weekly performance metrics, including contractor metrics, in May 2013. Implementation of the PERSEREC project should help to improve the reliability of underlying performance metric data and automate and enhance performance reporting.

Records Management. We reported that records management controls over PSSP files, which include extensive amounts of sensitive personally identifiable information, needed improvement. These weaknesses create inefficiency and present risks to the FDIC. The transition to PERSEREC should mitigate these weaknesses and inefficiencies.

Information Systems. Data we reviewed in the Division of Administration systems used to capture preliminary clearance data and provide management reporting — the Background Investigation Review Tracking System and the Corporate Human Resources Information System (CHRIS) — were not reliable and, in some cases, redundant. SEPS officials indicated that once PERSEREC is fully operational, the Background Investigation Review Tracking System will be retired. SEPS also expects to implement a business process management system in 2015 that will integrate with PERSEREC, CHRIS, and OPM systems to automatically update background investigation case information and track the status of cases. SEPS will need to ensure that it builds adequate workflow process controls into the automation effort to address the weaknesses noted in our report.

As we completed our testing, it was too early to fully assess the effectiveness of SEPS' operational improvements, hiring of new management and key staff, and ongoing and planned automation efforts. Nevertheless, we considered those efforts in forming our recommendations.

We made 10 recommendations intended to complement ongoing PSSP program improvements and to strengthen and sustain associated policies, procedures, and controls. In its response to our report, management concurred and described steps it had already taken that we confirmed were sufficient to close three of the recommendations.

Finally, in connection with this assignment, we performed limited 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. In this regard, we identified potential risk areas and suggested that the FDIC further examine aspects of this issue, which the Corporation committed to doing.

IT Project Management

IT projects involve all FDIC divisions and offices and are critical to the FDIC's operations and successful accomplishment of the Corporation's mission, goals, and objectives. In addition, the FDIC invests significant funding and internal resources in such projects. For example, as of December 31, 2013, the FDIC's incurred costs for projects completed or in process during 2012 and 2013 were approximately $111.7 million.

The FDIC's CIO plays a key role in both IT governance and IT project management at the FDIC. Specifically, the CIO is responsible for ensuring that all capital investment projects are consistent with the IT strategies and objectives of the Corporation, including those related to architectural alignment, security, and resource optimization. The CIO also ensures that proposed systems development projects are adequately planned, estimated, resourced, and monitored throughout the development life cycle.

The FDIC's Board of Directors approves funding for capital investments, including IT projects, involving estimated costs of $3 million or more and receives updates on those projects and the performance of the portfolio as whole on a quarterly basis. The FDIC's IT projects are governed by three entities—the Capital Investment Review Committee, the CIO Council, or the Corporate Management Council—depending on the cost and nature of the project.

IT project management is considered to be the day-to-day discipline of organizing and managing resources (e.g., people and budget) so a project delivers intended requirements within defined scope, quality, time, and cost constraints. Implementing the process is a shared responsibility among DIT, the FDIC division or office sponsoring an IT project (client), and the IT contractor responsible for developing the application.

We conducted an evaluation to (1) assess the extent to which the FDIC's IT projects are meeting their cost, schedule, and requirements expectations; (2) identify factors that promote project success or prevent projects from meeting expectations; and (3) identify opportunities for strengthening the FDIC's controls for monitoring IT projects.

We determined that most Capital Investment Review Committee and CIO Council projects completed or in process during 2013 met planned schedules, were within 10 percent of annual budgeted expenses, and met user expectations. Still, perceptions and anecdotes persist that FDIC IT projects are sometimes too costly, experience delays, or do not deliver promised specifications. During our evaluation, the CIO Council used an annual budget process to monitor IT project costs. We concluded that the CIO Council could enhance its cost monitoring by evaluating total project costs against initial project budgets. Doing so would more readily show to what extent individual projects, and the portfolio as a whole, meet life-cycle cost expectations. The FDIC's Project Management Office was developing metrics for tracking projects against initial project budgets at the time we were completing our fieldwork. Further, the Acting CIO indicated that he would continue to have dialogues with those having key roles in IT governance and project management regarding metrics being used to determine project success. Based on these ongoing efforts, we determined that a recommendation associated with these matters was not warranted.

With respect to six projects in process or completed in 2012 that we selected for in-depth review, four of the six had been completed. Three of the completed projects met both schedule and cost expectations, while the other project missed the original estimated completion date by 1 year, and actual cost far exceeded the original budget. The two projects that were in process were both behind schedule and ran the risk of experiencing cost overruns.

As a result of our interviews and analysis of these projects, we identified the following aspects of the IT project management process that were key factors in project success or contributed to challenges, depending on whether and how well they were carried out:

- Thoroughly planning and scoping the IT project.
- Ensuring developers understand the FDIC's environment.
- Managing IT project collaboration and communication.
- Implementing an effective milestone review process.
- Preparing a dedicated testing team.
- Assigning independent risk managers.

Ensuring that these factors are emphasized and the related controls are in place and working during ongoing and future IT projects could provide greater assurance that the projects meet cost, schedule, and requirements expectations. We thus recommended that the Acting CIO advise client division and offices, IT project teams, DIT intersecting organizations, and appropriate governance bodies of the key factors in project success or challenges and related controls we identified in this report and determine whether guidance in any of these areas needed to be strengthened.

The Acting CIO concurred with this recommendation and described completed and planned corrective actions in his response.

The FDIC's Controls for Safeguarding Sensitive Information in Resolution Plans Submitted Under the Dodd-Frank Act

Section 165(d) of the Dodd-Frank Act and the FDIC's Final Rule, entitled *Resolution Plans Required*, dated November 1, 2011, require large, systemically important financial companies to submit resolution plans, sometimes referred to as "living wills," to the FDIC and to the FRB. The intent of this requirement is for a large financial company to describe how it could be resolved under the U.S. Bankruptcy Code without serious adverse effects on U.S. financial stability. The resolution plans required by section 165(d) and the Final Rule contain sensitive information.

The Final Rule established staggered schedule for submitting resolution plans based on the amount of total non-bank assets that financial companies own. The first group of filers consisted of 11 companies with $250 billion or more in non-bank assets. Nine of these companies submitted initial resolution plans by July 1, 2012, and the remaining two companies submitted initial plans by October 1, 2012.

The FDIC and FRB jointly reviewed the resolution plans to determine whether they would facilitate an orderly resolution of the company under the U.S. Bankruptcy Code. Within the FDIC, OCFI had primary responsibility for reviewing the resolution plans submitted by the first group of financial company filers. The results of the FDIC's reviews, including findings and analyses, are contained in electronic and hard-copy documents referred to as Review Materials. The FDIC has determined that Review Materials constitute sensitive information.

We conducted an audit to determine whether the FDIC's controls for safeguarding sensitive information in resolution plans submitted under section 165(d) are consistent with applicable information security requirements, policies, and guidelines. Our audit focused on the controls that the FDIC had in place to safeguard resolution plans submitted by the first group of financial company filers, as described above.

We conducted our work in two phases. During the first phase, we assessed the FDIC's controls over sensitive resolution plan information and briefed FDIC management in February 2013 on our preliminary observations. During the second phase, we determined the status of actions that had been taken to address our preliminary observations as of February 2014.

Initially, we found that the FDIC's controls for safeguarding sensitive information in resolution plans submitted under section 165(d) of the Dodd Frank Act were not fully consistent with applicable information security requirements, policies, and guidelines.

Among other things, we found that the security level of sensitive resolution plan information had not been formally categorized in accordance with federal standards, key OCFI security policies and procedures needed to be updated and finalized, access controls needed to be strengthened, and the role and level of resources allocated to OCFI's internal review and information security functions needed to be assessed.

Throughout 2013, and prior to the close of our audit in February 2014, the FDIC was taking actions to address our preliminary observations and strengthen security controls. Of particular note, the FDIC:

- formally categorized sensitive resolution plan information, including Review Materials, consistent with federal standards;
- assigned an Information Security Manager from another FDIC division to help establish and implement security controls over sensitive information maintained by OCFI;
- updated and formally approved key OCFI security policies and procedures;
- strengthened controls over the management of hard-copy resolution plans and Review Materials;
- began requiring security guards to use individual access codes when entering secured workspaces where resolution plans and Review Materials are stored to promote accountability; and
- developed a formal internal review manual and plan that address information security.

Our final report noted that the actions taken by the FDIC since the start of our audit significantly improved security over sensitive resolution plan information. We did, however, make seven recommendations related to access management, encryption and authentication, internal control reviews, and personnel suitability.

In their responses, the Director, OCFI, and the Acting CIO concurred with all recommendations and described ongoing and planned actions to address our findings.

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 and the CIO 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.

Strategic Goal 6

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

While the OIG's audit, evaluation, and investigation work is focused principally on the FDIC's programs and operations, we also hold ourselves to high standards of performance and conduct. We seek to develop and retain a high-quality staff, effective operations, OIG independence, and mutually beneficial working relationships with all stakeholders. A major challenge for the OIG over the past few years was ensuring that we had the resources needed to effectively and efficiently carry out the OIG mission at the FDIC, given a sharp increase in the OIG's statutorily mandated work brought about by numerous financial institution failures, the FDIC's substantial resolution and receivership responsibilities, and its new resolution authorities under the Dodd-Frank Act. All of these activities required vigilant, independent oversight. Now that the crisis has eased and economic conditions are improving, we have a bit more discretion in planning our work and have been able to focus attention on certain corporate activities that we have not reviewed for some time. Still, however, we are facing future attrition in our OIG workforce. As a result, we are closely monitoring our staffing and taking steps to ensure we are positioned to sustain quality work even as OIG staff leave.

To ensure a high-quality staff, we must continuously invest in keeping staff knowledge and skills at a level equal to the work that needs to be done, and we emphasize and support training and development opportunities for all OIG staff. We also strive to keep communication channels open throughout the office. We are mindful of ensuring effective and efficient use of human, financial, IT, and procurement resources in conducting OIG audits, evaluations, investigations, and other support activities, and have a disciplined budget process to see to that end.

To carry out our responsibilities, the OIG must be professional, independent, objective, fact-based, nonpartisan, fair, and balanced in all its work. Also, the Inspector General and OIG staff must be free both in fact and in appearance from personal, external, and organizational impairments to their independence. As a member of the Council of the Inspectors General on Integrity and Efficiency (CIGIE), the OIG 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, 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 GPRA Modernization Act of 2010 was signed into law on January 4, 2011.

The OIG supports GPRA and is committed to applying its principles of strategic planning and performance measurement and reporting to our operations. The OIG's Business Plan 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. Importantly, the OIG is currently re-examining the strategic and performance goals and related activities that have guided our past efforts to determine whether they continue to provide the best framework within which to carry out our mission.

To build and sustain a high-quality staff, effective operations, OIG independence, and mutually beneficial working relationships, the **OIG's 2014 performance goals** were 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 (FY) 2016 budget proposal to the FDIC Chairman, proposing a budget of $34.6 million, to fund 130 authorized positions, which reflects no change from our FY 2015, FY 2014, and FY 2013 budgets. Upon the Chairman's approval, we submitted the budget for inclusion in the President's budget.

2 Continued to monitor, track, and control OIG spending, particularly as it relates to OIG travel-related expenses, use of procurement cards, and petty cash expenditures.

3 Continued efforts to develop a new investigative case management system and worked to better track audit and evaluation assignment milestones and costs and to manage audit and evaluation records located in TeamMate or on shared drives or SharePoint sites.

4 Continued efforts to update the OIG's records and information management program and practices to ensure an efficient and effective means of collecting, storing, and retrieving needed information and documents. Took steps to increase awareness of the importance of records management in the OIG, including through communications to OIG staff in headquarters and field locations.

5 Continued using our inquiry intake system to capture and manage inquiries from the public, media, Congress, and the Corporation, in the interest of prompt and effective handling of such inquiries. Participated with the FDIC's group of Public Service Providers to share information on inquiries and complaints received, identify common trends, and determine how best to respond to public concerns.

6 Continued to refine our redesigned OIG Intranet site to provide a more useful, efficient work tool for all OIG staff.

7 Carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. Positions filled during the reporting period included an IT Audit Manager; Information Security Manager; Associate Counsel; two Special Agents in Charge; and entry- to mid-level audit, evaluation, and investigative staff.

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

1 Continued to implement the OIG's Quality Assurance Plan for October 2013 – March 2016 to ensure quality in all audit and attestation engagement work and evaluations, in keeping with government auditing standards and *Quality Standards for Inspection and Evaluation*. As part of those efforts, completed implementation of recommendations made to our office in the most recent peer review of our audit operations.

2 Oversaw contracts to qualified firms to provide audit and evaluation services to the OIG to enhance the quality of our work and the breadth of our expertise as we conduct audits and evaluations, and closely monitored contractor performance.

3 Participated in planning and attended the FDIC's Annual Accounting and Auditing Conference to offer OIG staff and others continuing professional education in matters relating to the current economic environment, emerging risk areas, and changes to accounting and auditing standards and practices.

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 Completed 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 Conducted 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 Commented extensively on draft versions of CIGIE's *Guide for Conducting Peer Reviews of Audit Organizations of Federal Offices of Inspector General*, which was approved by CIGIE membership in September 2014.

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. Held a post-banking school session for five current enrollees to share knowledge and experiences of their training.

2 Employed interns on a part-time basis in the OIG to provide assistance to the OIG.

3 Assigned the OIG's regional office special agents in charge on details to the OIG's headquarters office to serve as the Deputy Assistant Inspector General for Investigations as a learning and professional development opportunity.

4 Enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities.

5 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 Provided one of the members of the OIG's Counsel's Office to serve as a Special Assistant U.S. Attorney for a case and trial involving bank fraud. This opportunity allowed the Associate Counsel to apply legal skills as part of the prosecutorial team in advance of and during the trial.

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 Principal Deputy Inspector General's regularly scheduled meetings with them and through other forums.

3 Participated in numerous outreach efforts with such external groups as the Federal Audit Executive Council, Department of Justice, and the Federal Financial Institutions Examination Council to provide general information regarding the OIG and share perspectives on issues of mutual concern and importance to the financial services industry.

4 Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.

5 Kept RMS, DRR, the Legal Division, and other FDIC program offices informed of the status and results of our investigative work impacting their respective offices. This was accomplished by notifying FDIC program offices of recent actions in OIG cases and providing Office of Investigations' quarterly reports to RMS, DRR, the Legal Division, and 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 8 proposed or revised corporate policies related to, for example, the FDIC's corporate password standards and the FDIC's records and information management. Made suggestions to increase clarity and specificity of these and other draft policies, as needed.

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

8 Supported the Inspector General community by participating on the CIGIE Audit Committee; attending monthly CIGIE meetings; and participating in Investigations Committee, Council of Counsels to the IGs, and other meetings; and commenting on various legislative matters through the Legislative Committee.

9 Communicated with representatives of the OIGs of the federal banking regulators and others (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. Formed part of the team auditing the Financial Stability Oversight Council's compliance with its transparency policy and provided input to the CIGFO's annual report for 2014.

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, including sharing information regarding the Whistleblower Protection Enhancement Act of 2012.

12 Coordinated with the Department of Justice and U.S. Attorneys' Offices throughout the country in the issuance of press releases announcing results of cases with FDIC OIG involvement and routinely informed the FDIC's Office of Communications and Chairman's Office of such releases.

13 Responded to Senators Grassley and Coburn's request for a listing of all closed investigations, evaluations, and audits that were not disclosed to the public covering the period April 1, 2013 through March 31, 2014.

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. Incorporated such consideration in broader discussions related to longer-term, OIG strategic planning.

2 Attended FDIC Board Meetings, IT/Cyber Security Oversight Group meetings, Dodd-Frank Act working 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 overall preparedness for and handling of unanticipated or emerging risks affecting the Corporation.

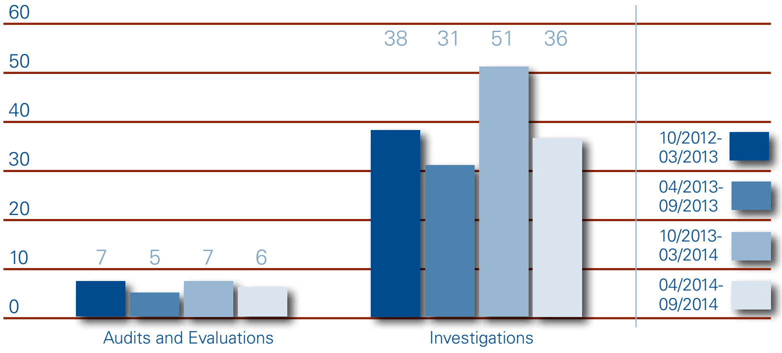
5 Met with representatives of the Government Accountability Office to share our perspectives on the risk of fraud at the FDIC. We did so in response to the Government Accountability Office's responsibility under Statement of Auditing Standards No. 99, Consideration of Fraud in Financial Statement Audits.

6 Monitored the management and performance challenge areas that we identified at the FDIC, in accordance with the Reports Consolidation Act of 2000 as we conducted audits, evaluations, and investigations: Carrying Out 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.

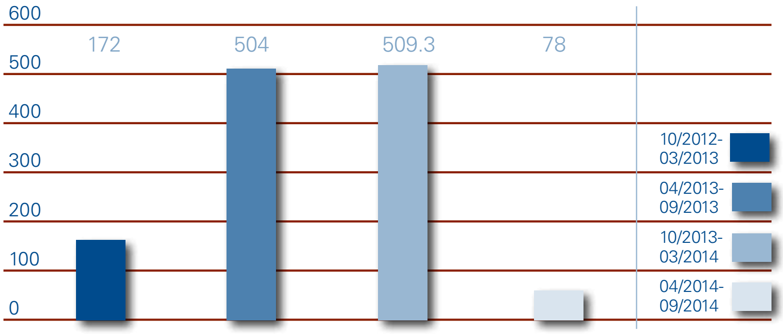
Cumulative Results (2-year period)

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

Products Issued and Investigations Closed



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



Reporting Requirements

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

Reporting Requirements		Page
Section 4(a)(2)	Review of legislation and regulations	52
Section 5(a)(1)	Significant problems, abuses, and deficiencies	10-41
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies	10-41
Section 5(a)(3)	Recommendations described in previous semiannual reports on which corrective action has not been completed	52
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	54
Section 5(a)(6)	Listing of audit reports	53
Section 5(a)(7)	Summary of particularly significant reports	10-41
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	54
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	54
Section 5(a)(10)	Audit recommendations more than 6 months old for which no management decision has been made	54
Section 5(a)(11)	Significant revised management decisions during the current reporting period	54
Section 5(a)(12)	Significant management decisions with which the OIG disagreed	54

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 continuing efforts to monitor and/or comment on proposed federal legislation concerning (1) cybersecurity with respect to federal systems, (2) the reliability of information provided on agency Web sites regarding agency payments made to grantees and contractors, (3) changes to existing law (Federal Information Security Management Act of 2002) requiring that OIGs annually evaluate and report on the effectiveness of their agency's information security practices and programs, and (4) public disclosure information in OIG reports concerning vulnerabilities in agency security systems.

In connection with these efforts, the OIG considered the following:

S. 2519, the *National Cybersecurity and Communications Integration Act of 2014*;

S. 994, the *Digital Accountability and Transparency Act of 2014* or *DATA Act*, now Public Law 113-01;

S. 2521, the *Federal Information Security Modernization Act of 2014*;

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

H.R. 1211, the *FOIA Oversight and Implementation Act of 2014*.

We have also commented over time to the CIGIE Legislation Committee on a bill related to testimonial subpoena power. The bill was in draft until it was incorporated in mid-September 2014 in H.R. 5492, *The Inspector General Empowerment Act of 2014*.

We also considered possible legislation related to OIG oversight of small agencies that the Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Financial and Contracting Oversight, had been drafting. The focus of this legislation was to address two issues: the need for independent oversight of approximately 40 federal government agencies/entities that do not have an Inspector General and the effectiveness of small OIGs in the context of many mandated reviews and the overhead associated with operating independently. We engaged in interagency discussion, principally with representatives of the other financial regulatory OIGs.

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

This table generally shows the corrective actions management has agreed to implement but has not completed, along with associated monetary amounts, as applicable. In some cases, these corrective actions are different from the initial recommendations made in the audit 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, Division of Finance and (2) the OIG's determination of closed recommendations. Recommendations are closed when (a) the Corporate Management Control notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, after the OIG confirms that corrective actions have been completed and are responsive.

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

Table II
Audit and Evaluation Reports Issued by Subject Area

Audit/Evalution Report		Questioned Costs		Funds Put to Better Use
Report Number and Date	**Title**	**Total**	**Unsupported**	
Supervision				
EVAL-14-002 July 25, 2014	Enforcement Actions and Professional Liability Claims Against Institution-Affiliated Parties and Individuals Associated with Failed Institutions	N/A		
AUD-14-009 August 21, 2014	The FDIC's Response to Bank Secrecy Act and Anti-Money Laundering Concerns Identified at FDIC-Supervised Institutions	N/A		
AUD-14-010 September 10, 2014	Material Loss Review of The Bank of Union, El Reno, Oklahoma	N/A		
Resources Management				
AUD-14-008 July 3, 2014	The FDIC's Controls for Safeguarding Sensitive Information in Resolution Plans Submitted Under the Dodd-Frank Act	N/A		
EVAL-14-001 July 14, 2014	The FDIC's Information Technology Project Management Process	N/A		
EVAL-14-003 August 7, 2014	The FDIC's Personnel Security and Suitability Program	N/A		
Totals for the Period		**$0**	**$0**	**$0**

Table III
Audit and Evaluation Reports Issued with Questioned Costs

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

Table 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 April 1, 2014 through September 30, 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
Failure Review Activity – Updated from Previous Semiannual Report						
Reviews Completed During the Reporting Period						
The Community's Bank Bridgeport, Connecticut	9/13/13	$7.8	The bank was insolvent and in such condition that it was unsafe and unsound to continue business.	No		
Chipola Community Bank Marianna, Florida	4/19/13	$10.3	The bank was imminently insolvent.	No		
Sunrise Bank of Arizona Phoenix, Arizona	8/23/13	$17	The bank was critically undercapitalized.	Yes	*	
Community South Bank Parsons, Tennessee	8/23/13	$72.5	The bank was operating in an unsound condition and manner. It was unable to continue its normal operations.	No		
1st Commerce Bank North Las Vegas, Nevada	6/6/13	$9.4	The bank was critically undercapitalized.	Yes	*	
Banks of Wisconsin Kenosha, Wisconsin	5/31/13	$26.3	The bank was operating in an unsafe manner.	No		
Central Arizona Bank Scottsdale, Arizona	5/14/13	$8.6	The bank was critically undercapitalized.	Yes	*	
Sunrise Bank Valdosta, Georgia	5/10/13	$17.3	The bank was critically undercapitalized.	Yes	*	

* The in-depth review will address the FDIC's overall supervisory strategy for these institutions (and for Pisgah Community Bank, Asheville, North Carolina — as reported in our prior semiannual report), all of which are failed subsidiaries 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						
Eastside Commercial Bank Conyers, Georgia	7/18/14	$33.9				
The Freedom State Bank Freedom, Oklahoma	6/27/14	$5.8				
Valley Bank Moline, Illinois	6/20/14	$51.4		Yes	The scope of the review will include emphasis on the FDIC's supervisory efforts associated with assessing and responding to the quality and performance of bank management with respect to the bank's president and CEO, who had a troubled history in the banking industry.	
Valley Bank Fort Lauderdale, Florida	6/20/14	$7.7				
Columbia Savings Bank Cincinnati, Ohio	5/23/14	$5.3				
AztecAmerica Bank Berwyn, Illinois	5/16/14	$18				
Allendale County Bank Fairfax, South Carolina	4/25/14	$17.1				
Vantage Point Bank Horsham, Pennsylvania	2/28/14	$8.5		Yes	FDIC management requested an in-depth review. 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.	

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 (cont'd)						
Syringa Bank Boise, Idaho	1/31/14	$4.5				
Bank of Jackson County Graceville, Florida	10/30/13	$5.1				
Bank of Wausau Wausau, Wisconsin	8/9/13	$13.5				
First Community Bank of SW Florida Fort Myers, Florida	8/2/13	$27.1				
Parkway Bank Lenoir, North Carolina	4/26/13	$18.1				
Douglas County Bank Douglas County Bank	4/26/13	$86.4				

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.

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

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

FDIC OIG Peer Review of the National Archives and Records Administration OIG

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

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

Investigative Peer Reviews

Quality assessment peer reviews of investigative operations are conducted on a 3-year cycle as well. Such reviews result in a determination that an organization is "in compliance" or "not in compliance" with relevant standards. These standards are based on *Quality Standards for Investigations* and applicable Attorney General guidelines. The Attorney General guidelines include the *Attorney General Guidelines for Offices of Inspectors General with Statutory Law Enforcement Authority* (2003), *Attorney General Guidelines for Domestic Federal Bureau of Investigation Operations* (2008), and *Attorney General Guidelines Regarding the Use of Confidential Informants* (2002).

- The 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 the CIGIE and the applicable Attorney General Guidelines. These safeguards and procedures provided reasonable assurance of conforming with professional standards in the planning, execution, and reporting of FDIC OIG investigations.

Ongoing FDIC OIG Investigative Peer Review Activity

We have completed fieldwork for the peer review of the investigative function of the Environmental Protection Agency OIG and will issue the results of that review in our next semiannual report. Our Office of Investigations anticipates being reviewed by the Department of the Treasury OIG in 2015.

Congratulations and Farewell

Arlene Boateng

Retirement

Arlene Boateng retired after more than 37 years of federal service. She began her career in 1976 when working as a summer aid with the National Transportation Safety Board. In 1977, she joined the Department of Justice (DOJ) on a temporary appointment, where she worked as a clerk and clerk typist, and in 1978, she was promoted on a temporary appointment to the position of accounting clerk at DOJ. In 1980, she joined the Bureau of Engraving and Printing at the U.S. Department of the Treasury as an accountant, and in 1982, transferred to the Department of the Treasury's OIG where she continued her career as an accountant. In 1983 she began working as an auditor in the FDIC's Office of Corporate Audits and Internal Investigations – the predecessor organization to the FDIC OIG. She was reassigned to the Dallas Regional Office in 1986 to set up an audit and investigative presence in that location, a testament to her leadership qualities. For nearly 31 years at the FDIC OIG — in both headquarters and Dallas — she achieved great success and was promoted to a senior auditor and later a senior audit specialist position.

Arlene's audits and evaluations over the years resulted in substantial improvements in the economy, efficiency, and effectiveness of financial and administrative operations of the Corporation, for example through her work on the OIG team assisting the Government Accountability Office (formerly General Accounting Office) in its audit of the FDIC's financial statements and through her efforts on other OIG assignments. She also contributed during the most recent financial crisis to the FDIC OIG's important material loss review audits and failed bank reviews of failed FDIC-supervised institutions. Of special note, she was instrumental in performing multiple internal quality assurance reviews of the FDIC OIG's audit activities and also formed part of the FDIC OIG team conducting the peer reviews of other federal OIGs.

John Lucas

Retirement

John Lucas retired from the FDIC after nearly 28 years of federal service. He entered the government in September 1987 as a presidential management intern at the Department of Defense OIG. Less than a year later, he was reassigned as a criminal investigator — a career path that he pursued with excellence over the years. In 1989 he transferred to the Government Accountability Office, and by 1990 had joined the FDIC OIG in Washington D.C. During his tenure with the FDIC OIG, he worked in two of our field locations: Schaumburg and Elk Grove Village, Illinois. Then, in 1995 he was reassigned to our Chicago Office, where he served and led with distinction, including for the past 3½ years as Special Agent in Charge.

Of special note, John's work involving fraud on the part of a bank officer and two customers of Universal Federal Savings Bank led to stiff sentences for the perpetrators and millions of dollars in ordered restitution. His efforts on this case were recognized by the Inspector General community with an Award for Excellence in October 2007. In another of his cases, a former loan officer and assistant vice president of Citizens Bank of Newburg, Rolla, Missouri, pleaded guilty and was sentenced for his role in a conspiracy. Commenting on that case, the Assistant U.S. Attorney wrote to John: "In my 10 years of experience as a federal prosecutor, the work you have done and are doing on this case exemplifies a standard for how federal agents should operate and how federal investigations ought to be handled in every case."

John served as an outstanding representative of the OIG over the past years by developing and fostering constructive working relationships with FDIC regional management, U.S. Attorneys' Offices, and fellow law enforcement groups. He also successfully recruited and then mentored new agents for the Office of Investigations and called upon his vast experience to teach and develop these new investigators.

Derek Evans
Retirement

Derek Evans retired from the FDIC after more than 25 years of federal service. He began his career in 1989 as a criminal investigator at the U.S. Secret Service, Department of the Treasury, in Tampa, Florida. Over the next 10 years, he was promoted and transferred to Secret Service offices in both New Jersey and Washington D.C. In October 1999, he joined the OIG at the Department of the Interior, working in Lafayette, Louisiana, and Atlanta, Georgia, over a period of more than 3 years. He transferred to the FDIC OIG's Atlanta Office in August 2005 and served with distinction in that location as a criminal investigator and later in New York, as the Special Agent in Charge of that of that region until his retirement.

Throughout his career, Derek worked to promote integrity in federal programs and operations and, importantly, in the banking industry while at the FDIC. Of special note, he played a key role in several complex, significant cases for the FDIC OIG, including a case involving the former president and chief executive officer of the Park Avenue Bank, New York, New York, who pleaded guilty to fraud on the Troubled Asset Relief Program, securities fraud, self-dealing, bank bribery, and embezzlement of bank funds. During his last week in the FDIC OIG, he joined the U.S. Attorney for the District of Maryland in announcing the sentencing of a mortgage company owner to more than 3 years in prison in a $1.3 million fraud scheme.

Derek served as an outstanding representative of the OIG by developing and fostering constructive working relationships with FDIC regional management, U.S. Attorneys' Offices, and fellow law enforcement groups. He also successfully recruited new agents for the Office of Investigations and guided these new agents — all in the interest of ensuring a first-class cadre of investigators in the FDIC OIG.

Andy Peterson
Retirement

Andy Peterson retired from the FDIC after more than 29 years of federal service. After active duty service in the U.S. Army from October 4, 1985 through April 1, 1990, he began his career as a criminal investigator in November 1990 at the Department of Justice's Drug Enforcement Administration in Albany, New York. Over the next 18 years, he advanced steadily in his career and was promoted along the way. He transferred to the FDIC OIG's New York office in January 2009, where he served as a criminal investigator until his retirement.

The OIG appreciated Andy's versatility, flexibility, and willingness to travel wherever the office needed him. In that regard, he assisted agents in multiple OIG locations in promoting integrity in the FDIC's programs and operations and, importantly, in the financial services industry as a whole.

Andy served as an outstanding representative of the OIG by developing and fostering constructive working relationships within the OIG and with FDIC regional management, U.S. Attorneys' Offices, and law enforcement colleagues.

Congratulations to CIGIE Award Winner

The OIG congratulates **Joe Moriarty**, OIG Special Agent in Charge, Chicago Regional Office, for his efforts on the investigation of the Bank of the Commonwealth. Mr. Moriarty was acknowledged, along with law enforcement partners from the U.S. Attorney's Office, Eastern District of Virginia; FBI; IRS; SIGTARP; and FRB at the October 21, 2014 CIGIE Annual Awards Ceremony, with an Award for Excellence "for outstanding cooperation in uncovering and investigating a multimillion dollar bank, securities, and Troubled Asset Relief Program fraud scheme."

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.

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