



★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★  
Office of Inspector General

---

---

# Semiannual Report to the Congress

October 1, 2015 – March 31, 2016



FEDERAL DEPOSIT INSURANCE CORPORATION



The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the Congress to maintain stability and confidence in the nation's banking system by insuring deposits, examining and supervising financial institutions, and managing receiverships. Approximately 6,400 individuals carry out the FDIC mission throughout the country. According to most current FDIC data, the FDIC insured more than \$6.5 trillion in deposits in 6,182 institutions, of which the FDIC supervised 3,947. As a result of institution failures during the financial crisis, the balance of the Deposit Insurance Fund (DIF) turned negative during the third quarter of 2009 and hit a low of negative \$20.9 billion by the end of that year. Various assessments imposed over the past few years under an FDIC Restoration Plan, along with improved conditions in the industry, have steadily increased the DIF balance to a positive \$72.6 billion as of December 31, 2015. Receiverships under FDIC control as of December 31, 2015, totaled 446, with about \$4.8 billion in assets.



**Office of Inspector General**  
**Semiannual Report**  
**to the Congress**

October 1, 2015 – March 31, 2016

Federal Deposit Insurance Corporation



# Acting Inspector General's Statement



I am pleased to present the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General's (OIG) semiannual report for the period October 1, 2015 through March 31, 2016. The work highlighted in this report reflects our commitment to promote economy, efficiency, effectiveness, and integrity in FDIC programs and operations, and to make a positive impact in the banking industry.

Over the past 6-month period, we issued 6 audit and evaluation reports covering topics including professional liability claims, interest rate risk, financial reporting, and the Freedom of Information Act, and made 12 recommendations for improvements in FDIC programs, activities, and related controls. Our investigations of criminal activity affecting the FDIC and the banking industry resulted in 36 indictments or informations, 39 convictions, 21 arrests, and potential monetary benefits in excess of \$1 billion. Many subjects in these investigations were former bank officers and directors who abused their positions of trust and are now paying a high price for their crimes. We also focused on effectively communicating with stakeholders, expanding our knowledge and understanding of emerging risk areas — most notably with respect to cyber security, and ongoing efforts to increase operational efficiency and promote excellence in our workforce. Accomplishments in these areas are more fully explained in this report within the framework of five goals reflecting our principal areas of emphasis.

Of note during the reporting period, and in keeping with an Inspector General's responsibility to keep the Congress fully and currently informed, I testified before the Committee on Financial Services, Subcommittee on Oversight and Investigations, U.S. House of Representatives, related to our completed inquiry on the *FDIC's Supervisory Approach to Refund Anticipation Loans and the Involvement of FDIC Leadership and Personnel*. That work highlighted areas of concern related to the FDIC's supervisory actions that caused banks to exit the refund anticipation loan business line and prompted frank discussions with FDIC management and the Corporation's Board of Directors. That inquiry is also discussed more fully in this report, and we continue to work with FDIC management and the Board of Directors to address the matters we raised for their consideration. Toward the end of April, I was also asked to appear before the Committee on Science, Space, and Technology; Subcommittee on Oversight; U.S. House of Representatives; to discuss recent cyber security breaches at the FDIC, and that hearing is scheduled for May.

Our office is committed to addressing these types of challenging issues as part of our independent oversight function and in the interest of transparency. There is an inherent tension in the relationship between an OIG and the agency it oversees. Over the past months, while my office and the Corporation may have held differing views on the manner in which the Corporation has handled certain issues, we continue to respect and have not lost sight of the unique roles we play as public servants carrying out our respective missions.

In closing, on behalf of the FDIC OIG, 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 pursue our IG mandate, strive to help the FDIC successfully accomplish its mission, and work in the best interest of the American people.

Fred W. Gibson, Jr.  
Acting Inspector General  
April 2016



# Table of Contents

---

<b>Acting Inspector General's Statement</b>	v
<b>Acronyms and Abbreviations</b>	2
<b>Highlights and Outcomes</b>	4
<b>Strategic Goal Areas</b>	
<b>Goal 1: Quality Audits and Evaluations</b>	9
<b>Goal 2: Impactful Investigations</b>	21
<b>Goal 3: Effective Communications</b>	35
<b>Goal 4: Enhanced Understanding of Emerging Issues</b>	39
<b>Goal 5: Operational Efficiency and Workforce Excellence</b>	43
<b>Reporting Requirements</b>	47
<b>Appendix 1</b>	
Information Required by the Inspector General Act of 1978, as amended	48
<b>Appendix 2</b>	
Information on Failure Review Activity	54
<b>Appendix 3</b>	
Peer Review Activity	56
<b>Congratulations and Farewell</b>	58



# Acronyms and Abbreviations

**BSA** Bank Secrecy Act

**C&C** Cotton & Company LLP

**CEO** chief executive officer

**CFO** chief financial officer

**CFPB** Consumer Financial Protection Bureau

**CIGFO** Council of Inspectors General on Financial Oversight

**CIGIE** Council of the Inspectors General on Integrity and Efficiency

**CIO** chief information officer

**CY-4** Washington Field Office Cyber Squad-4

**DIF** Deposit Insurance Fund

**Dodd-Frank Act** Dodd-Frank Wall Street Reform and Consumer Protection Act

**DOJ** Department of Justice

**DRR** Division of Resolutions and Receiverships

**ECU** Electronic Crimes Unit

**ERO** electronic refund originator

**FBI** Federal Bureau of Investigation

**FDI Act** Federal Deposit Insurance Act

**FDIC** Federal Deposit Insurance Corporation

**FI** financial institution

**FISMA** Federal Information Security Modernization Act of 2014

**FOIA** Freedom of Information Act

**FRB** Board of Governors of the Federal Reserve System

**FY** fiscal year

**GAO** U.S. Government Accountability Office

**GFRS** Governmentwide Financial Report System

**GPRA** Government Performance and Results Act of 1993

<b>IRR</b>	interest rate risk
<b>IRS</b>	Internal Revenue Service
<b>IRS-CID</b>	Internal Revenue Service Criminal Investigation Division
<b>ISM</b>	information security manager
<b>IT</b>	information technology
<b>NARA</b>	National Archives and Records Administration
<b>NCIJTF</b>	National Cyber Investigative Joint Task Force
<b>OIG</b>	Office of Inspector General
<b>OMB</b>	Office of Management and Budget
<b>PII</b>	personally identifiable information
<b>PLC</b>	professional liability claim
<b>PLU</b>	Professional Liability Unit
<b>POAM</b>	plan of action and milestones
<b>RAL</b>	refund anticipation loan
<b>RMS</b>	Division of Risk Management Supervision
<b>SAR</b>	Suspicious Activity Report
<b>SB</b>	Stearns Bank
<b>SBA</b>	Small Business Administration
<b>SEC</b>	U.S. Securities and Exchange Commission
<b>SIGTARP</b>	Special Inspector General for the Troubled Asset Relief Program
<b>TAB</b>	Transportation Alliance Bank
<b>TBC</b>	Tifton Banking Company
<b>TEB</b>	The Equitable Bank
<b>TSP</b>	technology service provider
<b>UCB</b>	United Commercial Bank
<b>USDA</b>	U.S. Department of Agriculture

# Highlights and Outcomes

The FDIC OIG conducts its work in five strategic goal areas that are linked to the OIG's mission. A summary of our completed work during the reporting period, along with references to selected ongoing assignments, is presented below, by goal area. We revised our previous goals as we planned for fiscal year (FY) 2016 and 2017 and will continue to refine performance goals and associated performance measures during the remainder of the fiscal year.

## **Goal 1: Quality Audits and Evaluations** **Conduct quality audits, evaluations, and other reviews to ensure economy, efficiency, and effectiveness in FDIC programs and operations**

We issued six final audit/evaluation reports during the reporting period. Of note, in one we examined the FDIC's process for professional liability claims against directors, officers, and other professionals whose wrongful conduct caused losses to failed institutions, and we made recommendations to the FDIC Legal Division to help ensure such claims are cost effective. We also issued a report in response to a Congressional request sent to most IGs from the Chairman, Committee on Homeland Security and Governmental Affairs, U.S. House of Representatives, requesting that, for the FDIC, we analyze "non-career officials' involvement in the Freedom of Information Act (FOIA) response process." For the most part (48 of 52 cases), we found their involvement was limited to awareness of the requests. The remaining four requests exhibited heightened involvement by the Chairman, select corporate officers, or both, and resulted in: additional information being redacted in one case, additional information being released in two cases, and processing delays in releasing information in two cases. We issued a separate letter to FDIC management with suggested enhancements to the FOIA program. During the past 6-month period, we also issued our annual report under the Federal Information Security Modernization Act, where we concluded that the FDIC's information security program controls and practices are generally effective, but made observations and recommendations related to the information security manager program, security practices related to outsourced information service providers, user access to FDIC information systems, baseline configurations, multifactor authentication for nonprivileged network users, system event logging and monitoring, and the FDIC's infrastructure services contract. We also issued the results of a case study involving the FDIC's approach to institutions with elevated interest rate risk profiles, concluding the FDIC has taken a number of positive steps to emphasize the importance of having risk management practices in place to mitigate the effects of adverse movements in interest rates before they happen.

As a follow-on to our earlier audit of the FDIC's involvement in the Department of Justice initiative known as "Operation Choke Point," we issued a report of inquiry regarding the FDIC's supervisory approach to refund anticipation loans (RAL), concluding that the FDIC's decision to require banks to exit RALs involved aggressive and unprecedented efforts to use the FDIC's supervisory and enforcement powers, circumvention of certain controls surrounding exercise of enforcement powers, damage to field staff morale, and high costs to the affected institutions. We laid out a number of issues for the FDIC's consideration. FDIC management and the FDIC Board of Directors both responded to our report and committed to taking action by June 30, 2016.

Ongoing assignments in support of this goal include reviews of the FDIC's resolution plan review process, controls for safeguarding sensitive information in those resolution plans, its process for identifying and reporting major security incidents, its monitoring of systemically important financial institutions, and a review of progress the FDIC has made in addressing credentialing and multifactor authentication issues that we highlighted in an earlier audit.

## **Goal 2: Impactful Investigations**

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

Our Office of Investigations (OI) continued its work addressing criminal activity affecting both open and closed financial institutions. A number of cases we highlight in this report were referred to us by the FDIC's Division of Risk Management Supervision and the Division of Resolutions and Receiverships. Cases during the reporting period included those involving former bank directors and officers, employees of the bank, real estate professionals, attorneys, businessmen, and other bank customers. OI also handled several FDIC employee-related matters in the interest of ensuring integrity in FDIC programs and operations, and we are reporting the results of one such case in which a former FDIC attorney was convicted of bank fraud in connection with a short-sale scam. OI special agents continued to partner with U.S. Attorneys' Offices throughout the country and participated actively in working groups with law enforcement partners to leverage knowledge and better address issues of mutual concern. Our special agents also offered training in fraud detection, insider threats, and tracing of funds, and engaged in outreach with groups both internal and external to the FDIC to explain OI's role in combatting criminal activity causing harm to the banking system. Overall investigative results for the reporting period attest to the value of solid working relationships with the Corporation, other OIGs, and law enforcement partners. Our investigations during the past 6 months led to 36 indictments; 39 convictions; 21 arrests; and potential fines, restitution, and asset forfeitures totaling more than \$1 billion.

Finally and importantly, we received positive results on the investigative peer review conducted by the Department of the Treasury OIG, who found that the system of internal safeguards and management procedures for the investigative function of the FDIC OIG in effect for the year ending December 31, 2015, was in compliance with quality standards established by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and applicable Attorney General guidelines.

## **Goal 3: Effective Communications**

### **Communicate effectively with internal and external stakeholders**

In formulating this goal, we took time to reexamine the information needs of the OIG's stakeholders, including the FDIC Board of Directors and FDIC division and office management and their staffs, the Congress, members of the IG community, the Government Accountability Office, Office of Management and Budget, the media, and the general public. We did so in the interest of ensuring that our communications are effective and that the messages we convey are transparent, informative, and clearly understood.

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

We also maintained positive relationships with the Congress and provided timely responses to a number of congressional inquiries. Congressional interaction during the reporting period included the Acting IG's testimony before the Committee on Financial Services, Subcommittee on Oversight and Investigations, U.S. House of Representatives, related to our report on the *FDIC's Supervisory Approach to Refund Anticipation Loans and the Involvement of FDIC Leadership and Personnel*; updates on our work related to involvement by FDIC non-career officials in the FDIC's Freedom of Information Act response process; and information on the status of open, unimplemented recommendations; closed audits, evaluations, and investigations that were not made available to the public; and referrals to the Department of Justice and associated criminal prosecutions.

The OIG fully supported and participated in IG community activities through CIGIE. We coordinated with representatives from the other financial regulatory OIGs on issues of mutual interest. In this regard, the Dodd-Frank Act created the Financial Stability Oversight Council (FSOC) 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. We attended CIGFO meetings and participated on a CIGFO working group to evaluate FSOC's efforts to promote market discipline.

We continue to field allegations through our Hotline system and receive inquiries on varied topics from the public through other means, and we make every effort to respond timely to such contacts. We are in the process of updating and refining our Congressional protocols and also developing a more formal and effective means of handling media requests and inquiries. Ongoing efforts to redesign our external Website are intended to provide more useful content and better serve all stakeholders.

#### **Goal 4: Enhanced Understanding of Emerging Issues** **Continuously seek to enhance OIG knowledge and understanding of emerging and evolving issues affecting the FDIC, OIG, and insured depository institutions**

Our attention to better understanding of emerging issues focused on two matters in particular during the reporting period. First, we expanded our involvement and knowledge of cyber security matters in several ways. We assigned one of our senior managers to serve as a cyber security liaison officer to proactively monitor cyber issues and trends from multiple sources and disseminate pertinent information to interested or affected parties both internal and external to the FDIC. Our information security manager and the OIG Cyber Event Group continued to keep current on possible threats to ensure our readiness to address them. We continued active participation at the FBI's Cyber Task Force in Washington, D.C. and devoted an investigative resource to the National Cyber Investigative Joint Task Force. These efforts are paying dividends in terms of increased knowledge and productive networking and information-sharing opportunities. Additionally, several audit and evaluation assignments are addressing significant information security topics and those efforts further expand our knowledge base.

A second priority area of focus for our office is on the implications of the Dodd-Frank Wall Street Reform and Consumer Protection Act, and in particular during the reporting period, on the responsibilities that our office would be required to fulfill were a systemically important financial institution to fail. These responsibilities would include analyses and reporting on various aspects of the FDIC's liquidation of any covered financial company by the Corporation as receiver under Title II of the Act. We researched the impact of such responsibilities and identified issues relating to scope, frequency, reporting, funding, and coordination efforts that would be needed to successfully meet the mandate of the Dodd-Frank Act. We are continuing to pursue those issues.

## **Goal 5: Operational Efficiency and Workforce Excellence**

### **Maximize OIG operational efficiency and workforce excellence**

We have devoted ongoing attention to activities that would enhance operational efficiencies and help ensure workforce excellence. Among those, we continued efforts to develop and test 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 other electronic repositories. In a related vein, we continued efforts to update the OIG's records and information management program and practices to ensure an efficient and effective means of collecting, storing, and retrieving needed information and documents. We also took steps to maintain a secure, effective, and reliable information technology environment so that we can leverage the tools we use to conduct our work more efficiently. We undertook risk-based OIG planning efforts for audits, evaluations, and — to the extent possible — investigations for FY 2016 and beyond, taking into consideration the goals of, and risks to, FDIC corporate programs and operations and those risks more specific to the OIG. We incorporated such information in broader discussions related to both OIG strategic and performance planning for FY 2016 and 2017.

With an emphasis on our human resources and the talents needed for OIG success, we carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. Positions filled during the reporting period included several human resources professionals, an Associate Counsel, and two new managers for our Office of Audits and Evaluations. We also continued to support members of the OIG pursuing professional training and certifications or attending graduate banking school programs to enhance the OIG staff members' expertise and knowledge and enrolled OIG staff in several different FDIC leadership development programs to enhance their leadership capabilities. Finally, OIG senior management analyzed the OIG's performance management program and the OIG's process for recognizing and rewarding staff in the interest of providing constructive feedback and acknowledging efforts of all staff in a fair, transparent, and consistent manner.

**Significant Outcomes**  
(October 1, 2015 – March 31, 2016)

Audit and Evaluation Reports Issued	6
Questioned Costs or Funds Put to Better Use	0
Nonmonetary Recommendations	12
Investigations Opened	58
Investigations Closed	56
OIG Subpoenas Issued	9
<b>Judicial Actions:</b>	
Indictments/Informations	36
Convictions	39
Arrests	21
<b>OIG Investigations Resulted in:</b>	
Fines of	\$70,200
Restitution of	1,054,386,846
Asset Forfeitures of	449,999
Total	\$1,054,907,045
Cases Referred to the Department of Justice (U.S. Attorney)	40
Proposed Regulations and Legislation Reviewed	7
Responses to Requests Under the Freedom of Information/Privacy Act	7

# Goal 1: Quality Audits and Evaluations

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

The OIG's work in support of this goal is largely the responsibility of the OIG's Office of Audits and Evaluations. The OIG's Office of Audits provides the FDIC with professional audit and related services covering the full range of its statutory and regulatory responsibility, including major programs and activities. These audits are designed to promote economy, efficiency, and effectiveness and to prevent fraud, waste, and abuse in corporate programs and operations. This office ensures the compliance of all OIG audit work with applicable audit standards, including those established by the Comptroller General of the United States. It may also conduct external peer reviews of other OIG offices, according to the cycle established by the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

The companion Office of Evaluations evaluates, reviews, studies, or analyzes FDIC programs and activities to provide independent, objective information to facilitate FDIC management decision-making and improve operations. Evaluation projects are conducted in accordance with the *Quality Standards for Inspection and Evaluation*. Evaluation projects are generally limited in scope and may be requested by the FDIC Board of Directors, FDIC management, or the Congress.

Prior to passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), in the event of an insured depository institution failure, the Federal Deposit Insurance (FDI) Act required the appropriate regulatory OIG to perform a review when the Deposit Insurance Fund (DIF) incurs a material loss. Under the FDI Act, a loss was considered material to the insurance fund if it exceeded \$25 million or 2 percent of the failed institution's total assets. With passage of the Dodd-Frank Act, the loss threshold was increased to \$200 million through December 31, 2011, \$150 million for losses that occurred for the period January 1, 2012 through December 31, 2013, and \$50 million thereafter. The FDIC OIG performs the review if the FDIC is the primary regulator of the institution. The Department of the Treasury OIG and the OIG at the Board of Governors of the Federal Reserve System (FRB) and Consumer Financial Protection Bureau perform reviews when their agencies are the primary regulators. These reviews identify what caused the material loss and evaluate the supervision of the federal regulatory agency, including compliance with the Prompt Corrective Action requirements of the FDI Act.

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

### **OIG Work in Support of Goal 1**

In support of this goal during the reporting period, we issued six reports. These reports span various FDIC programs and activities, including professional liability claims, interest rate risk mitigation strategies, information security, and the FDIC's Freedom of Information Act (FOIA) process. Our office also continued the legislatively mandated review of all failed FDIC-supervised institutions causing losses to the DIF of less than the threshold outlined in the Dodd-Frank Act to determine whether circumstances surrounding the failures would warrant further review. Our failed bank review activity is presented in Appendix 2.

At the end of the reporting period, ongoing audit and evaluation assignments were addressing such issues as the FDIC's resolution plan review process, its controls for safeguarding sensitive information in those resolution plans, its process for identifying and reporting major security incidents, its monitoring of systemically important financial institutions, and progress made in addressing credentialing and multifactor authentication activities. Results of this body of ongoing work will be presented in an upcoming semiannual report.

The results of issued audit and evaluation reports are discussed below. Following the discussion of this work, we present the results of a report of inquiry that we issued as a follow-on to an earlier report related to the FDIC's role in the Department of Justice's initiative known as "Operation Choke Point."

## **Opportunities Exist to Better Ensure Professional Liability Claims Are Cost Effective**

After a rigorous review of the factual circumstances surrounding the failure of an insured depository institution, the FDIC may pursue professional liability claims (PLCs) against directors, officers, and other professionals whose wrongful conduct caused losses to those failed institutions. PLCs also include direct claims against insurance carriers and contract rights inherited from the institution under fidelity bonds that institutions purchase to cover losses resulting from dishonest or fraudulent acts by their employees. To collect on these claims, the FDIC often must sue the professionals for losses resulting from their breaches of duty to the failed institution. Professional liability lawsuits are only pursued if they are both meritorious and expected to be cost effective.

The FDIC's professional liability program is intended to maximize recoveries to receiverships and hold those officials who caused losses accountable. The FDIC's Division of Resolutions and Receiverships (DRR) and Legal Division are jointly responsible for the program. DRR Investigations and the Legal Division's Professional Liability Unit (PLU) investigate 11 claim areas for each institution failure and pursue recovery of losses by filing PLCs. The FDIC Board delegated joint authority to the DRR Director and the FDIC's General Counsel to settle, dismiss, or otherwise dispose of non-asset-related suits or claims, which includes PLCs. As such, pursuing PLCs requires a coordinated effort between DRR and PLU.

We conducted a review to evaluate the FDIC's efforts to ensure that PLCs are cost effective. We focused our review on the design of the FDIC's policies, procedures, and other practices associated with managing costs of PLC cases.

We determined that DRR and the Legal Division have procedures and controls in place for ensuring that PLCs are cost effective including, among other things, considering costs to pursue the claim against potential recovery sources; developing a budget for outside counsel fees; capturing PLC-related costs; seeking FDIC Board authority to sue and, where appropriate, settle claims; and drafting reports and holding meetings to periodically monitor case status. Notwithstanding these efforts, we identified additional opportunities to ensure the cost effectiveness of PLCs by

- enhancing coordination between DRR and the Legal Division,
- clarifying how the FDIC determines and reassesses PLC cost effectiveness, and
- better documenting key decisions made throughout the PLC process.

We made six recommendations to strengthen program controls to help ensure that PLCs are cost effective. The FDIC has taken or proposed actions that are responsive to our recommendations.

## The FDIC Addresses Institutions with Elevated Interest Rate Risk Profiles

The FDIC has been concerned that certain institutions are not sufficiently prepared or positioned for sustained increases in, or volatility of, interest rates because rates have been exceptionally low for a prolonged period. To address its concerns, the FDIC's Division of Risk Management Supervision (RMS) has undertaken a number of initiatives, including reiterating supervisory expectations and enhancing its offsite review program to help identify institutions that have potential exposure warranting additional review.

We conducted an evaluation to study RMS' response to institutions with elevated interest rate risk (IRR) profiles. The scope of this study focused on well-rated institutions identified by the FDIC's analysis of Call Report data as of June 30, 2013 as having above average IRR exposure. In total, 98 FDIC-supervised institutions met our study criteria. In our view, focusing on this particular group provided a reasonable way to isolate our attention on the FDIC's supervisory response to IRR. Additionally, studying institutions meeting these criteria was of interest because, historically, regulators have been challenged dealing with ostensibly healthy institutions engaging in risky behavior. Forward-looking supervision is aimed at addressing this issue, thus, our evaluation approach enabled us to assess one application of this initiative.

Our observations, while limited to the group studied, illustrate RMS' application of forward-looking supervision. Employing lessons learned from the financial crisis, RMS has taken a series of steps aimed at emphasizing the importance of having effective risk management practices in place to mitigate the effects of adverse movements in interest rates before they happen. The FDIC's response included reiterating supervisory expectations; enhancing its offsite review program to better identify institutions with above-average IRR exposure; and following up by applying risk-focused examination procedures to further understand institution-specific risks. Further, the FDIC's process encourages examiners to consider the fact that even well-rated institutions can experience financial stress in cases where risks are not properly monitored, measured, and managed. Accordingly, as warranted, we observed that examiners are taking proactive supervisory action and progressive action to encourage banks to take preemptive measures to address risk exposures before their profitability and viability is impacted. For the most part, institutions are responding to examiners' concerns. Importantly, management's responsiveness to supervisory concerns was a key differentiating factor between banks that failed and those that remained viable during the financial crisis.

In responding to the draft report, the Director of RMS stated that RMS intends to continue its vigilant supervision of IRR, and that professional development efforts will remain a priority to ensure that staff have the knowledge and resources to prudently supervise rate sensitivity issues.

## FDIC Information Security Programs and Practices Are Generally Effective, but Some Aspects Warrant Additional Attention

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the FDIC, to perform annual independent evaluations of their information security programs and practices and to report the results to the Office of Management and Budget (OMB). We engaged the professional services firm of Cotton & Company LLP (C&C) to conduct a performance audit to satisfy the OIG's FISMA reporting requirement.

C&C performed audit procedures to evaluate the 10 security control areas outlined in the Department of Homeland Security's June 19, 2015, document entitled, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*. C&C's work included an analysis of selected security controls related to two of the FDIC's general support systems and two major applications, as well as a review of the Corporation's risk management activities related to an outsourced information service provider that facilitated employee recruitment efforts.

FISMA requires federal agencies to develop, document, and implement agency-wide information security programs to provide security for their information and information systems and to support the operations and assets of the agencies, including information and information systems that are provided or managed by another agency, contractor, or other source.

Overall, C&C concluded that, except as described below, the FDIC's information security program and practices were generally effective. As part of the firm's work, C&C noted several important improvements in the FDIC's information security program over the last year. Specifically, the FDIC:

- enhanced its patch and vulnerability management program through the creation of a Patch and Vulnerability Management Group and related subgroups that meet regularly to evaluate technical vulnerabilities in the FDIC's information technology (IT) environment and work to implement solutions;
- improved its process for managing known security weaknesses through Plans of Actions and Milestones (POA&Ms) as demonstrated by a reduction in the number of open high-risk POA&Ms from 49 in September 2014 to 26 in August 2015;
- expanded its security metrics reporting, particularly to senior management, which has resulted in increased awareness of information security risks and enabled management to take more proactive measures to improve the FDIC's overall information security posture; and
- revised its corporate information security risk management program policy to better align with NIST guidance.

In addition, the FDIC implemented five of seven previously unaddressed recommendations from our 2013 and 2014 security evaluation reports required by FISMA, and was working to address the remaining two recommendations at the close of the audit.

Notwithstanding these accomplishments, C&C identified aspects of the FDIC's information security program warranting management attention. Of particular note, the duties and role of the FDIC's Information Security Managers (ISM) in addressing information security requirements and risks within the FDIC's business divisions and offices have evolved since the ISM program was established. However, the FDIC had not recently completed a comprehensive assessment to determine whether the skills, training, oversight, and resource allocations pertaining to the ISMs enable them to effectively carry out their increased responsibilities and address security risks within their divisions and offices. In addition, the FDIC had not always ensured the timely completion of outsourced information service provider assessments or the timely review of user access to FDIC information systems. Further, the FDIC had not identified access control weaknesses for an outsourced information service provider that C&C found during its audit.

The FDIC was continuing its work on a multi-year initiative to develop secure baseline configurations for its information systems. Baseline configurations that are documented, implemented, and monitored are a critical control for ensuring that the FDIC's information systems are adequately protected. The FDIC was also working to implement multifactor authentication for nonprivileged network users and, separately, to perform system event logging and monitoring for certain databases. Continued management attention on each of these initiatives is warranted to ensure their success. C&C identified additional findings in the security control areas of risk management and configuration management that are described in the firm's report.

Finally, C&C noted that the FDIC depended heavily upon its infrastructure services contract to support IT operations and implement security controls. C&C noted certain risks associated with the contract that, if not properly managed, could negatively impact the FDIC's IT operations, including its security operations. FDIC officials informed C&C that they were aware of these risks and were taking steps to mitigate them.

The FISMA report contained six recommendations intended to improve the effectiveness of the FDIC's information security program controls and practices. The Acting Chief Information Officer (CIO) and Director, Division of Administration, provided a joint written response to a draft of C&C's report. In the response, FDIC management concurred with all six of the report's recommendations and described planned and completed actions that were responsive to the recommendations.

## Case Study Sheds Light on a Computer Security Incident Involving a Technology Service Provider

As required by 12 CFR Part 364, Appendix B, *Interagency Guidelines Establishing Information Security Standards*, financial institutions (FI) must implement a comprehensive written information security program designed to: ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. The Interagency Guidelines require FIs to develop and implement a risk-based response program to address incidents of unauthorized access to customer information. The Interagency Guidelines also provide that FIs' contractual arrangements shall require that technology service providers (TSP) implement appropriate measures to meet the Interagency Guidelines objectives. The federal banking agencies, including the FDIC, conduct periodic IT examinations at FIs and their TSPs.

In late 2014, we received allegations about a computer security incident potentially involving unauthorized access to unencrypted personally identifiable information (PII) from multiple client FIs residing on a TSP's computer server. We initiated work to evaluate the TSP's and FDIC's handling of the matter with objectives to:

- understand the specifics of the incident and assess the TSP's response and communications;
- evaluate the FDIC's response to, and consideration of, the incident; and
- evaluate the examination coverage of the TSP prior to the incident.

During our evaluation, we became aware of additional information that called into question the credibility of the allegations. Notwithstanding, this incident provided a real world example of challenges that the Corporation, TSPs, and FIs face when assessing and deciding how to respond to potential cyberattack issues.

We learned that following the incident, the TSP conducted an investigation and concluded that adware caused the suspicious activity and identified no evidence of a cyberattack or exfiltration of data. The TSP concluded that the incident did not warrant regulatory or client notification based on applicable regulatory guidance and client contract language. However, contrary to cybersecurity best practices, the TSP did not collect or retain forensics information such as an image of the server or a copy of the adware. Moreover, the TSP did not have computer activity logging controls in place that may have allowed the TSP to determine whether any data had been accessed or exfiltrated.

We concluded that a poor internal control environment and a vague incident response policy limited the TSP's ability to protect against the incident and hampered incident response efforts. We also concluded that the TSP could have done more to notify regulatory authorities of the incident and that the contract language between the TSP and its client FIs could have better defined terms related to incident response and specified notification requirements.

Once the FDIC's RMS Washington Office became aware of the incident, it required the TSP to obtain a forensic investigation and deployed an examination team to review overall TSP network security. However, we concluded that the RMS field office could have escalated the security incident and allegations sooner. The incident demonstrated the importance of having an RMS incident response plan for assessing potentially significant cyber incidents and sufficient enforcement authority over TSPs.

With respect to examination coverage, while the FDIC led joint IT examinations in compliance with examination frequency requirements and implementing guidelines, we had several observations regarding the July 2014 IT examination related to the assigned rating and tone of the examination report, incident response coverage, consideration of third-party reviews, and work paper documentation.

We had made recommendations in a prior report to address several areas identified in this case study and RMS is working to implement those recommendations. Our case study noted that RMS has also issued new guidance for escalating incidents; is developing a corporate plan for responding to significant cyber incidents; is researching whether to draft regulations to govern TSP operations, to include expectations for FI incident notifications; and has established several cyber-related performance initiatives. We are monitoring RMS progress in completing these actions. We also expect to perform further reviews in this area in light of the significant risks that technology services present to the financial industry.

### **Congressional Request Regarding Select Senior Officials' Involvement in the Freedom of Information Act Agency Response Process**

Enacted in 1966, the Freedom of Information Act (FOIA) bestows a right upon the American public to request records created by Executive Branch departments and agencies. FOIA does not require requesters to articulate a reason for the request and creates a presumption of access, so long as the request does not encompass any of the categories of information exempted from the statute. Agencies may withhold or redact records if they contain information that is exempt from FOIA's disclosure requirements. FOIA generally requires an agency to respond within 20 business days after receiving a request, but there are several exceptions to this requirement. The FOIA statute does not set forth expectations of whether, and to what extent, non-career officials can be involved in processing FOIA requests. The FOIA/ Privacy Act (FOIA/PA) Group within the Legal Division has been delegated the authority for processing the FDIC's FOIA requests.

Most federal OIGs, including the FDIC, received a letter from the Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, dated June 23, 2015, requesting that OIGs analyze “non-career officials’ involvement in the Freedom of Information Act (FOIA) response process...for the period of January 1, 2007, to the present.” The letter further requested that if non-career officials were involved in the FOIA response process, the OIG “analyze whether their involvement resulted in any undue delay of a response to any FOIA request or the withholding of any document or portion of any document that would have otherwise been released but for the non-career official’s involvement in the process.”

We responded to the request by analyzing the extent and impact of select senior FDIC officials’ involvement in the FOIA agency response process. We included three non-career officials (the FDIC Chairman, Vice Chairman, and one Schedule C employee) in our review. Further, based on discussions with Committee staff, we also included in the scope of this evaluation four corporate officer positions, which are held by three individuals, at the Deputy to the Chairman level, because the *Bylaws of the Federal Deposit Insurance Corporation* define their powers and duties as having broad authority to act on behalf of the Chairman.

We reported that at the FDIC, the Chairman and the corporate officers that we included in the scope of this evaluation are made aware of requests and responses to FOIA requests that the Legal Division deems to be sensitive, including media or blogger requests. Eleven percent of all FOIA requests the FDIC received from September 16, 2010 through June 30, 2015, were considered sensitive, were from the media or bloggers, or both. Other non-career officials have not been involved in the FOIA process.

We reviewed a non-statistical sample of 52 FOIA requests. For 48 of the 52 FOIA requests, the Chairman’s and select corporate officers’ involvement was limited to awareness through email notices of a sensitive FOIA request when the request was received, weekly reports to the Chairman’s office that included high-level status updates, and an email notice before responsive records were sent to the requester.

Four requests exhibited heightened involvement by the Chairman, select corporate officers, or both that affected how the FDIC responded to the FOIA requests, and such involvement was for more than typical awareness. For those four requests, the heightened involvement resulted in, respectively:

- redaction of more information than what the FOIA/PA Group initially suggested on the basis that the further-redacted information was privileged communications within or between agencies or information that concerned the supervision of financial institutions;
- a 16-business-day delay in the FDIC releasing information;
- a fee waiver rejection being reconsidered and the FDIC waiving fees, and the FDIC releasing more information than what the FOIA/PA Group initially recommended; and
- the FDIC releasing additional information, but a 32-business-day delay in the FDIC releasing the information.

In completing this evaluation, we observed several issues related to the FDIC’s management of its FOIA program that were not significant in relation to this evaluation’s objective. We shared our observations and suggestions with management separately. Management agreed to review those suggestions and consider appropriate ways to incorporate them into the FDIC’s FOIA program.

In responding to our draft report, the FDIC General Counsel welcomed confirmation from our review that the involvement by the FDIC's non-career officials and select corporate officials in 48 of the 52 cases that we reviewed was limited to awareness of FOIA requests. Further, the General Counsel, as Chief FOIA Officer, addressed the Senate Committee's request for a written certification from the FDIC's Chief FOIA Officer that (1) no non-career officials were involved in the FDIC's response to any FOIA request or (2) if such involvement occurred, the involvement of non-career officials has never resulted in the undue delay of a response to a FOIA request or the provision of less information than would have been provided but for the involvement of the non-career officials.

## **OIG Verifies the FDIC's Data Submissions through the Governmentwide Financial Report System**

We completed an audit to verify whether the FDIC's summary general ledger information agreed with summary information entered into the Department of the Treasury's automated financial reporting tool, the Governmentwide Financial Report System (GFRS), for the FY ended September 30, 2015. This audit did not constitute a financial audit. As such, we did not render an opinion on the FDIC's internal controls over financial reporting or over its financial management systems. The Government Accountability Office (GAO) is responsible for auditing the financial statements of the FDIC and has agreed to provide us with audit assurances, as appropriate, on material line items for the purpose of meeting Treasury Financial Manual requirements associated with agencies, like the FDIC, that operate on a calendar-year basis.

We verified that the FDIC's summary general ledger information agreed with summary information entered into the GFRS for the FY ended September 30, 2015. As part of our work, we verified that the FDIC's data submissions in the GFRS for the calendar year ended December 31, 2014 agreed with the Corporation's audited financial statements for that year. In that regard, the GAO expressed an unmodified opinion on the financial statements of the funds administered by the FDIC in its February 2015 report entitled, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2014 and 2013 Financial Statements* (Report No. GAO-15-289). In addition, we submitted copies of requisite reports and representation letters to the Treasury, GAO, OMB, and/or Department of Justice in accordance with the Treasury Financial Manual.

Our report contained no recommendations.

## **OIG Issues Results of Report of Inquiry: *FDIC's Supervisory Approach to Refund Anticipation Loans and the Involvement of FDIC Leadership and Personnel***

### **Why and How We Conducted This Inquiry**

On December 17, 2014, Chairman Gruenberg requested that the FDIC OIG conduct a "fact-finding review of the actions of FDIC staff" in the Department of Justice's Operation Choke Point. The Chairman's request was prompted by concerns raised by a letter from a member of Congress, dated December 10, 2014, asking that the role of five FDIC officials, and others as appropriate, be examined. Our office addressed the actions of the five FDIC officials in connection with Operation Choke Point in the OIG's September 2015 audit report, *The FDIC's Role in Operation Choke Point and Supervisory Approach to Institutions that Conducted Business with Merchants Associated with High-Risk Activities* (AUD-15-008).

In that report, and as noted in our previous semiannual report, we indicated that we would conduct further work on the role of FDIC staff with respect to the Corporation's supervisory approach to financial institutions that offered a credit product known as a refund anticipation loan (RAL). By way of explanation, a RAL is a particular type of loan product, typically offered through a national or local tax preparation company in conjunction with the filing of a taxpayer's income tax return.<sup>1</sup> Although tax preparation firms were not specifically associated with Operation Choke Point, and RALs are financial products offered by banks and not a line of business related to Operation Choke Point, information we identified in the course of our earlier audit raised sufficient concern to cause us to also review the FDIC's supervisory approach to institutions offering RALs and the roles of FDIC personnel in that process.

Our final report on RALs is based on interviews with knowledgeable individuals and an extensive review and analysis of FDIC internal emails, correspondence, supervisory materials, and other documents.

### **What We Learned**

The FDIC had a lengthy supervisory relationship with institutions offering RALs, dating to the 1980s. In January 2008, the then-FDIC Chairman, Sheila Bair, asked why FDIC-regulated institutions would be allowed to offer RALs.<sup>2</sup> Shortly thereafter, the FDIC began to try to cause banks it supervised, which are the focus of this review, to exit the business line. In late December 2010, the Office of the Comptroller of the Currency (OCC) required an institution it supervised to exit RALs effective with the 2011 tax season. During this time period, the Internal Revenue Service also withdrew access to an underwriting tool it formerly provided to tax preparers and banks that had been used to mitigate certain risks associated with RALs. Ultimately, the FDIC caused all three of its supervised institutions that then continued to facilitate RALs to exit the business in 2011 and 2012.

RALs were, and remain, legal activities, but ultimately were seen by the FDIC as risky to the banks and potentially harmful to consumers.<sup>3</sup> As discussed in our report, the FDIC's articulated rationale for requiring banks to exit RALs morphed over time. The decision to cause FDIC-supervised banks to exit RALs was implemented by certain Division Directors, the Chicago Regional Director, and their subordinates, and supported by each of the FDIC's Inside Directors. The basis for this decision was not fully transparent because the FDIC chose not to issue formal guidance on RALs, applying more generic guidance applicable to broader areas of supervisory concern. Yet the decision set in motion a series of interrelated events affecting three institutions that involved aggressive and unprecedented efforts to use the FDIC's supervisory and enforcement powers, circumvention of certain controls surrounding the exercise of enforcement power, damage to the morale of certain field examination staff, and high costs to the three impacted institutions.

We reported that the Washington Office pressured field staff to assign lower ratings in the 2010 Safety and Soundness examinations for two institutions that had RAL programs. The Washington Office also required changing related examination report narratives. In one instance a ratings downgrade appeared to be predetermined before the examination began. In another case, the downgrade further limited an institution from pursuing a strategy of acquiring failed institutions. The institution's desire to do so was then leveraged by the FDIC in its negotiations regarding the institution's exit from RALs. Although the examiners in the field did not agree with lowering the ratings of the two institutions, the FDIC did not document these disagreements in one instance, and only partially documented the disagreement in another, in contravention of its policy and a recommendation in a prior OIG report.

---

1 The tax preparer, often referred to as an electronic refund originator (ERO), works in cooperation with the financial institution to advance a portion of the tax refund claimed by individuals in the form of a loan. Typically the loan amount would include the tax return preparation cost, other fees and a finance charge.

2 The Chairman's question was raised in the context of an incoming letter from a number of consumer advocacy groups. This letter, together with similar correspondence in 2009, expressed concern that RALs harmed consumers.

3 The FDIC's current and historical policy is that it will not criticize, discourage, or prohibit banks that have appropriate controls in place from doing business with customers who are operating consistent with federal and state law. The FDIC applies this policy to services offered to bank customers, i.e., depositors or borrowers. Because RALs are offered through EROs and are third-party relationships, the FDIC does not believe this policy applies.

The absence of significant examination-based evidence of harm caused by RAL programs could have caused FDIC management to reconsider its initial assessment that these programs posed significant risk to the institutions offering them. However, lack of such evidence did not change the FDIC's supervisory approach. The FDIC's actions also ultimately resulted in large insurance assessment increases, reputational damage to the banks, as well as litigation and other costs for the banks that tried to remain in the RAL business.

The Washington Office also used a cursory analysis of underwriting plans that two banks submitted to show their mitigation of perceived risk to reject those plans. In fact, when the initial review suggested these underwriting plans could effectively mitigate certain risks, the Washington Office narrowed and repeated its request to solicit a different outcome. It appears that the decision to reject the plans had been made before the review was complete. The alleged insufficiency of the underwriting plans also formed the basis for an enforcement action against one of the banks.

While the FDIC's Legal Division believed the pursuit of an enforcement remedy against the banks presented "high litigation risk," the FDIC chose to pursue such remedies. Members of the Board, including the then-Chairman of the Case Review Committee, were involved in drafting the language of a proposed enforcement order and in advising management on the development of supervisory support for the enforcement case. The FDIC also attempted to strengthen its case by pursuing a compliance-based rationale. To that end, in early 2011 the FDIC employed extraordinary examination resources in an attempt to identify compliance violations that would require the bank to exit RALs. This examination effort, in the form of a "horizontal review," involved deploying an unprecedented 400 examiners to examine 250 tax preparers throughout the country and the remaining bank offering RALs. The horizontal review was used as leverage in negotiations to get the final bank to exit RALs. Ultimately, the results of the horizontal review were used for little else.

The FDIC also employed what it termed "strong moral suasion" to persuade each of the banks to stop offering RALs. What began as persuasion degenerated into meetings and telephone calls where banks were abusively threatened by an FDIC attorney. In one instance, non-public supervisory information was disclosed about one bank to another as a ploy to undercut the latter's negotiating position to continue its RAL program.

When one institution questioned the FDIC's tactics and behavior of its personnel in a letter to then-Chairman Bair and the other FDIC Board members, the then-Chairman asked FDIC management to look into the complaint. FDIC management looked into the complaint but did not accurately and fully describe the abusive behavior. Nevertheless, the behavior was widely known internally and, in effect, condoned. Other complaints from the banks languished and ultimately were not addressed or investigated independently. Ratings appeals that included these complaints were not considered because they were voided by the FDIC's filing of formal enforcement actions. These complaints were eventually subsumed by settlement processes that, in the case of one bank, appeared to trade improved ratings and the right to purchase failing institutions for an agreement to exit RALs permanently.

## Conclusion and Matters for Consideration

The facts developed by this review strongly reinforced the concerns and issues raised in our earlier audit. We reported that in our view, the FDIC must candidly consider its leadership practices, its process and procedures, and the conduct of multiple individuals who made and implemented the decision to require banks to exit RALs. While we acknowledge that the events described in our report surrounding RALs involved only three of the FDIC's many supervised institutions, the severity of the events warrants such consideration. The FDIC needs to ask how the actions described in our report could unfold as they did, in light of the FDIC's stated core values of integrity, accountability, and fairness. Further, the Corporation must address how it can avoid similar occurrences in the future.

In December 2015, in response to concerns raised in our earlier audit, the FDIC removed the term "moral suasion" from its guidance. We appreciate the central importance of informal discussions and persuasion to the supervisory process; however, we believe more needs to be done to subject the use of moral suasion, and its equivalents, to meaningful scrutiny and oversight, and to create equitable remedies for institutions should they be subject to abusive treatment.

Because our work was in the nature of a review, and not an audit conducted in accordance with government auditing standards, we did not make formal recommendations in the RALs report. However, we requested that the FDIC report to us, 60 days from the date of our final report, on the steps it would take to address the matters raised for its consideration.

## FDIC Management's Response

The OIG transmitted a draft copy of this report to the FDIC on January 21, 2016. We asked the Corporation to review the draft and identify any factual inaccuracies they believed existed in the report. We met with staff from the FDIC, on February 10, 2016, to consider whether any factual clarifications were appropriate, reviewed the documentation they provided, and subsequently made some clarifications to the report. The FDIC provided a written response, and its response did not change our overall view of the facts.

In responding to our report, FDIC management expressed the following perspectives: The FDIC had longstanding supervisory histories with respect to RALs. According to FDIC management, to differing degrees, the institutions engaged in the RAL business had a record of supervisory deficiencies identified by examination staff in both risk management and compliance stemming from their RAL programs. These issues formed the basis for the examination and enforcement actions described in the report. Nonetheless, according to FDIC management, the draft report did identify areas where better communication, both internally and externally, could have improved understanding of the agency's supervisory expectations and bases for action. Additionally, management stated that the draft report described at least one instance in which a former employee – new to the FDIC at the time, and who left the agency that same year – communicated with external parties in an overly aggressive manner. Management emphasized that the FDIC does not condone such conduct, that type of conduct is not consistent with FDIC policy, and steps were taken to address the conduct at the time.

Management committed to providing actions to be taken in response within the 60-day timeframe specified by the OIG. A summary of management's response to our report is available at [www.fdicig.gov/reports16/OIG-16-001.pdf](http://www.fdicig.gov/reports16/OIG-16-001.pdf).

### **Board of Directors' Response to Our Report**

We received a subsequent response to our report from the FDIC Board of Directors. The Board indicated it would undertake a review of the key policy issues raised in the final report for consideration. As a starting point, the FDIC Board reiterated its commitment to the mission, vision, and corporate values of the FDIC. Additionally, the FDIC Board committed to review and consider the following matters:

- the clarity and sufficiency of parameters applied to the use of moral suasion, or its equivalents;
- the adequacy of existing vehicles for examiners and other employees to report what they believe to be inappropriate actions or direction;
- the effectiveness and timeliness of avenues of redress available to banks that believe supervisory powers are not used appropriately; and
- the governance and procedures of the Board and its committees.

### **Interim Actions in Response to the Final Report**

In addition to this Board-level review, the FDIC Board's response identified a number of interim actions that the FDIC could take in the near-term to be responsive to the OIG's concerns and further strengthen the FDIC's supervision programs, as follows:

- Issuance of internal guidance regarding communication with bankers,
- Enhancement of appeals processes,
- Issuance of external guidance regarding expectations for communication and handling of disagreements,
- Issuance of industry guidance on lending through third parties, and
- Independent review to advise whether there is a basis for personnel action or changes to personnel policies.

Finally, the Board indicated that the FDIC would provide a status update of the efforts outlined above by June 30, 2016.

On March 16, 2016, the Acting Inspector General testified before the Committee on Financial Services, Subcommittee on Oversight and Investigations, U.S. House of Representatives, and presented the results of the OIG's inquiry into the RALs matter.



# Goal 2: Impactful Investigations

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

The OIG's Office of Investigations (OI) works closely with FDIC management in RMS, 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. In the case of bank closings where fraud is suspected, OI may send case agents and computer forensic special agents from our Electronic Crimes Unit (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.

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

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

### **OIG Work in Support of Goal 2**

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

Our cases during the reporting period include those involving bank fraud, wire fraud, embezzlement, and mortgage fraud. Many of our bank fraud cases involve former senior-level officials, other bank employees, and customers at financial institutions who exploited internal control weaknesses and whose fraudulent activities harmed the viability of the institutions and ultimately contributed to losses to the DIF. Real estate developers and agents, attorneys, and other individuals involved in residential and commercial lending activities were also implicated in a number of our cases. We are also reporting on a case involving a former FDIC attorney, as an example of our efforts to ensure integrity within the FDIC. The OIG's working partnerships with the Corporation and law enforcement colleagues in all such investigations contribute to ensuring the continued safety and soundness of the nation's banks and help ensure integrity in the FDIC's programs and activities.

## **Bank President Pleads Guilty and Is Sentenced for Conspiracy to Commit Bank Fraud and Major Crimes Against the Government**

On December 4, 2015, the former president and chief executive officer (CEO) of Tifton Banking Company (TBC) pleaded guilty to conspiracy to commit bank fraud and conspiracy to commit major fraud against the United States. He further agreed to a lifetime ban from banking by entering into a stipulation and consent to the issuance of an Order of Prohibition from further participation in banking. On November 12, 2010, TBC was closed by the Georgia Department of Banking and Finance, and the FDIC was named Receiver. The former president and CEO was sentenced on February 25, 2016 to 84 months in prison and ordered to pay \$3,931,018 in restitution.

According to facts stipulated in the plea agreement, the former president and CEO held that position from August 2005 until June 2010. During that time, he was engaged in an ongoing scheme to mislead the bank and its loan committee about loans TBC made to local individuals and businesses. As part of the scheme, he hid past due loans from the FDIC and the TBC loan committee, which resulted in the bank continuing to approve and renew delinquent loans and loans for which the collateral was lacking. Several of the borrowers eventually defaulted on the loans, resulting in millions of dollars in losses to TBC and others.

The former president and CEO admitted that in certain transactions in which he exercised approval authority, he hid his personal and business interests. In one instance, he approved loans to the buyer of a condominium in Panama City Beach, Florida, a condominium that he himself owned. In doing so, he made false representations about the loans to TBC's loan committee and failed to disclose his personal interest in the transaction. When the buyer's loan payments became delinquent, the former president and CEO hid the loans from both the FDIC and state regulators. He received \$50,000 profit from the sale of his condominium in this transaction, the entire purchase price being funded by an unsecured loan to the buyer approved by him. The buyer eventually declared bankruptcy, resulting in a loss of more than \$400,000 to TBC.

The former president and CEO also admitted to making fraudulent representations that led to commercial loan guarantees being issued by the Small Business Administration (SBA) and the U.S. Department of Agriculture (USDA) on two other loan transactions. The loans were made by TBC, and guaranteed by the government agencies, to refinance earlier non-performing commercial loans made by TBC as part of the scheme to mislead bank regulators and hide the bank's true financial condition. Those guaranteed loans resulted in losses to the bank and the agencies of more than \$2 million.

TBC was closed by the Georgia Department of Banking and Finance in November 2010 due to its poor financial condition. At that time, TBC had not repaid \$3.8 million it had received from the Department of Treasury's Troubled Asset Relief Program.

**Source:** *This investigation was initiated based on information received from the FBI, Valdosta, Georgia, and the FDIC's DRR.*

**Responsible Agencies:** *This is a joint investigation by the FDIC OIG, FBI, Special Inspector General for the Troubled Asset Relief Program (SIGTARP), SBA OIG, USDA OIG, and the Tifton County Sheriff's Office. The case is being prosecuted by the U.S. Attorney's Office for the Middle District of Georgia and the Department of Justice, Criminal Division, Fraud Section, Washington, D.C.*

## **Conspirator Sentenced to Over 5 Years in Prison for \$3.8 Million Mortgage Fraud Scheme**

The founder of AO Consulting, LLC, and AORE Investments Inc., who was a self-proclaimed financial consultant, was sentenced on February 26, 2016 to 61 months in prison followed by 5 years of supervised release for conspiracy, wire fraud, and aggravated identity theft arising from a mortgage fraud scheme. To carry out the scheme, he used the names of immigrants and students, along with false financial information, to obtain \$3.8 million in home mortgage loans to buy approximately three dozen row houses in Baltimore, all but one of which are in default or foreclosure. As part of his sentencing, he was ordered to pay restitution of \$3,356,581.

According to his plea agreement, the so-called financial consultant agreed to purchase row houses in Baltimore City from a co-conspirator who had acquired the houses as part of his real estate business. The co-conspirator invested in Baltimore residential real estate and controlled four companies that bought and sold residential real estate. The consultant purchased the houses at prices far in excess of their actual market value. In return, the realtor kicked back a substantial portion of the purchase price to him, which he used to pay for the down payments and closing costs for most of the properties; to pay a commission to the individuals whom he persuaded to allow him to use their names to purchase the properties (“the straw purchasers”); to pay referral fees to individuals who referred other straw purchasers to him; and to compensate himself for his participation in the scheme. In all, from June 2009 to November 2010, the “consultant” purchased 35 row houses from the realtor. The financing received on these transactions totaled approximately \$3.8 million, and he received commission payments from the realtor in excess of \$1.2 million.

To perpetrate the scheme, the consultant persuaded approximately three dozen immigrants and students to purchase the row houses under their names. Although none of these “straw purchasers” had any experience in real estate transactions, nor the funds needed to buy the properties, he told each straw purchaser that he would prepare the loan application; manage the property after its purchase by finding renters, collecting the rent, and paying the mortgage; and would pay the straw purchaser \$7,000 to \$8,000 after the transaction closed. He further promised to sell the property in 3 years and give the individual up to 80 percent of the sale proceeds. He also paid thousands of dollars in additional commissions to those straw purchasers who referred other individuals to him as potential buyers for similar transactions.

He ultimately admitted that he falsely represented in the loan applications the straw purchasers’ assets and earnings, and that the property would be the primary residence of the purchaser. He also provided fraudulent earnings and bank statements for the purchasers, to document the false information provided in the loan application. He provided the necessary funds for the down payment and the buyer’s share of the closing costs, causing the settlement statement form to inaccurately reflect that the down payments and closing costs had been paid by the straw purchasers.

Following the closings, he retained the keys to each property and assumed the responsibility for finding renters and making the required monthly mortgage payments. The named purchasers never lived in the properties. He eventually allowed all of the mortgages to go into default.

After a fire occurred at one of the row house properties purchased through a straw purchaser, the “consultant” falsely identified himself as the straw purchaser to the insurance company in order to collect \$106,500 in insurance paid for repair of the property. He cashed the check, which was made out to the straw purchaser and the bank holding the mortgage, and used the funds for his own purposes. He did not notify the bank that the funds to repair the property had been received, nor did he arrange to make or pay for any repairs to the property.

The realtor involved in the case previously pleaded guilty to conspiring to commit mail, wire, and bank fraud arising from the mortgage fraud schemes resulting in losses totaling approximately \$1.2 million. He was sentenced to 19 months in prison and ordered to pay restitution of \$1,182,822. In a related case, a co-conspirator — a loan officer for a mortgage brokerage company — was sentenced to 18 months in prison for conspiring to commit bank fraud and was also ordered to pay restitution of \$1,182,822.

**Source:** Federal Housing Finance Agency (FHFA) OIG.

**Responsible Agencies:** This was a joint investigation by the FDIC OIG, Housing and Urban Development OIG, FBI, and the FHFA OIG.

### **Sentencing in Factoring Fraud Case**

In a case involving Transportation Alliance Bank (TAB), Salt Lake City, Utah, two businessmen were sentenced for their part in a fraudulent scheme that caused substantial losses to the bank. This case involved a practice termed “factoring,” which involves the following steps: You perform a service for your customer. You then send your invoice to a factoring company. You subsequently receive a cash advance on your invoice from the factoring company. The factoring company then collects full payment from your customer. Finally, the factoring company pays you the rest of your invoice amount, minus a fee.

On February 5, 2016, the CEO and president of Impact Solutions Consulting (ISC), Kennesaw, Georgia, and the chief financial officer (CFO) of ISC were sentenced for making false statements to the bank. The former CEO and president was sentenced to serve 36 months in prison to be followed by 36 months of supervised release, while the former CFO was sentenced to serve 12 months and a day in prison to be followed by 36 months of supervised release. The Court will issue a restitution order at a later date.

ISC provided consulting and project management services in addition to mapping fiber optic cable routes for Verizon. ISC submitted invoices to Verizon after it had completed the mapping services and awaited payment of those invoices by Verizon. To increase cash flow, ISC established factoring relations by which it sold receivables to a factor in exchange for a percentage of the face value of the receivable. In January 2011, ISC began a factoring relationship with TAB. ISC created a website, Verizonsuppliers.com, that initially was supposed to track internal work orders and invoices associated with Verizon. Employees of TAB became concerned with the length of time ISC had uncollected receivables from Verizon. The two businessmen provided access to TAB employees to the Verizonsuppliers.com website and portrayed the website as being a Verizon site through which TAB could verify the validity of outstanding receivables. Between 2011 and 2012, the two received accurate invoicing data related to Verizon work performed by ISC and they consulted and agreed how much to inflate the true amounts prior to presenting a false invoice to TAB for factoring. In the end, the bank suffered a financial loss of \$6,340,024 because of the grossly inflated invoices.

**Source:** OI and FBI initiated.

**Responsible Agencies:** This is a joint investigation by the FDIC OIG and the FBI, Salt Lake City Division. The case is being prosecuted by the U.S. Attorney's Office for the District of Utah.

### **Two Former Executives of Transportation Alliance Bank and Stearns Bank Sentenced**

In December 2015, two former executives of Transportation Alliance Bank (TAB), Salt Lake City, Utah, and Stearns Bank, NA (SB), St. Cloud, Minnesota, were each sentenced for their role in a bank fraud. The former president of TAB, who had earlier been the vice president of SB, was sentenced to serve 30 months in prison to be followed by 36 months of supervised release and was ordered to pay restitution of \$13,000,000 to TAB and \$75,000 to the FDIC.

His co-conspirator, the former vice president of TAB, who had also served as operations manager of SB, was sentenced to 2 years of supervised release and was ordered to pay restitution of \$10,000 for her role in the scheme. Previously, she had paid a civil monetary penalty of \$75,000 to the FDIC and agreed to a lifetime ban from banking.

From approximately January 2008 through March 2010, the two former bank executives misused their positions at SB by advancing bank funds to two student loan companies, NextStudent and Cology, without proper authorization from the bank. NextStudent and Cology were factoring clients of SB and the defendants advanced funds to the two companies by causing false invoices to be created with SB's factoring system and then "purchasing" the fraudulent invoices. The former president and his co-conspirator created or caused false entries to be created within SB computers, bank records, and reporting systems to conceal the fraudulent nature of the unsecured advances. In 2010, the former president and his co-conspirator left SB and went to work at TAB. Shortly after they arrived at TAB, the SB factoring portfolio, including the NextStudent and Cology accounts, was purchased by TAB at the recommendation of the two. The scheme of unsecured lending continued at TAB until 2012 when the fraud was exposed.

**Source:** *OI initiated.*

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

### **Former Loan Broker Sentenced**

On February 22, 2016, a former loan broker was sentenced to serve 12 months and one day in prison to be followed by 60 months of supervised release. He was also ordered to pay restitution in the amount of \$4,268,772 to Broadway Federal Bank, FSB, Los Angeles, California, and \$38,609 to the Internal Revenue Service (IRS).

Between February 2007 and March 2010, the bank's loan officer submitted loan applications on behalf of numerous churches in Los Angeles and the surrounding areas. The bank would pay rebates to loan brokers who brought the loans to the bank. The loan broker in this case admitted he submitted materially false and inflated financial figures to the bank. The bank provided mortgage loans to the churches, relying on the false financial information the loan broker had submitted. The estimated loss suffered by Broadway Federal Bank for these loans was \$19,781,814.

**Source:** *SIGTARP.*

**Responsible Agencies:** *This is a joint investigation by the FDIC OIG, SIGTARP, IRS Criminal Investigation Division (CID), and the FBI Long Beach Division. The case is being prosecuted by the U.S. Attorney's Office for the Central District of California, Los Angeles.*

### **Former Bank President Sentenced**

On January 27, 2016, the former president of D'Hanis State Bank, Hondo, Texas, was sentenced to serve 24 months in prison to be followed by 36 months of supervised release. She was also ordered to pay \$817,892 in restitution. On April 15, 2015, the former bank president was indicted on charges of bank fraud and embezzlement by a bank officer, and she subsequently pleaded guilty to one count of wire fraud on June 10, 2015.

This investigation was initiated based on allegations that the former bank president concealed an "outage" of \$830,000 in a D'Hanis State Bank correspondent bank account at Frost Bank. In October 2014, D'Hanis State Bank was purchased by Vantage Bank Texas, San Antonio, Texas, and the outage was discovered during the integration of network systems and data migration. On November 25, 2014, Vantage Bank determined the financial statements of D'Hanis State Bank were out of balance. The former president acknowledged she had known of the out-of-balance condition for several years, and had intentionally covered up the outage.

According to court records, from January 2012 until September 2014, the former president prepared and filed false Consolidated Reports of Condition and Income (Call Reports) with federal and state bank regulators on behalf of the bank that overstated assets by about \$830,000. Moreover, she emailed those false reports to the prospective buyer of the bank — Vantage Bank, who relied on the false Call Reports in deciding to purchase the bank. She also acknowledged that at least \$100,000 of the \$830,000 outage was attributed to personal bills she had paid with cashier's checks drawn on D'Hanis State Bank.

**Source:** FDIC RMS.

**Responsible Agencies:** This was a joint investigation with the FBI, U.S. Secret Service, and the FRB OIG. The matter was prosecuted by the U.S. Attorney's Office for the Western District of Texas.

### **Former Bank President Sentenced to 97 Months in Bank Fraud Scheme**

On January 28, 2016, the former president and chief executive officer of Arvest Bank, Fayetteville, Arkansas, was sentenced to serve 97 months in prison to be followed by 24 months of supervised release. He was sentenced for his role in a loan fraud scheme affecting at least 24 financial institutions. He was also ordered to pay \$4,914,929 in restitution.

The former bank president obtained business and personal loans from financial institutions located mostly in the Western District of Arkansas. As collateral for these loans, he pledged uncertified restricted shares of Arvest Bank stock held in his employee stock plan at the bank. He repeatedly pledged the same shares of stock, valued at less than \$500,000, to obtain more than \$6 million in loans from 24 different financial institutions. He also directed and caused his subordinate staff at Arvest Bank to sign various documents that falsely assured the lenders that the shares of stock pledged as collateral were unencumbered and available to satisfy the loans in the event of default. The former president later defaulted on the loans, resulting in a loss of about \$5 million to the financial institutions.

**Source:** This investigation was initiated based on a referral from an independent source.

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

### **Former Bank President Sentenced in Nominee Loan Scheme**

On February 23, 2016, the former chairman, CEO, and president of Lafayette State Bank, Mayo, Florida, was sentenced to serve 36 months in prison to be followed by 5 years of supervised release. He was also ordered to pay restitution in the amount of \$734,412 to Lafayette State Bank. On August 26, 2015, the former bank executive pleaded guilty to one count of bank fraud for his role in a nominee loan fraud scheme.

The FDIC's RMS conducted an examination of Lafayette State Bank in April 2014. During the course of the examination, FDIC examiners identified irregularities in loans that had been made on behalf of the former bank president's family members. The investigation determined that he had used his position at the bank to obtain nominee loans from the bank in the names of several of his family members. Specifically, he and other bank officials falsified loan applications and diverted over \$700,000 disbursed by the bank. The former bank president approved all of the loans. He also made, and caused to be made, fraudulent representations in documents used to support the loans. Members of bank's Board of Directors either did not approve the loans, or approved the loans based on their reliance of fraudulent representations regarding the purpose of the loans.

**Source:** FDIC RMS.

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

## Investigation of “R.A.C.K. BOYZ” Scheme Results in Guilty Pleas

The OIG conducted an investigation based on a request for assistance from the U.S. Attorney’s Office for the Northern District of Indiana regarding bank and wire fraud against numerous banks. These banks included Bank of America, Citibank, JP Morgan Chase, Fifth Third Bank, Woori American Bank, TCF Bank, and Wells Fargo Bank. The investigation revealed that numerous individuals had devised and participated in a scheme where they manufactured or otherwise obtained counterfeit checks, recruited third-party participants who were willing to offer up their bank account information and debit cards, deposited these fraudulent checks into the third-party account holders’ bank accounts (typically through the use of ATMs), and finally withdrew the deposited funds (typically using an ATM or a money order purchased from places such as Walmart).

In this type of scheme, the withdrawals and purchases occur before the drawer bank receives the check and notifies the deposit account bank that the check deposited is fraudulent. The subjects then use the funds obtained from the fraud scheme for their own benefit. The subjects typically obtain the third-party account information and debit cards by paying the account holders for the use of their information. When approached by investigators, the third-party participants claim that their account information and debit card, complete with PIN, have been stolen. This scheme is known as “crackin’ cards” and the subjects in this case refer to themselves on Facebook as the “R.A.C.K. Boyz.” According to analysis done by the FBI, the R.A.C.K. Boyz scheme has defrauded the banks of over \$800,000.

Cracking cards schemes have become a popular method of obtaining illicit funds in Chicago and surrounding areas. The schemes often involve numerous participants, including some individuals thought to be affiliated with street gangs. Schemers use various methods to recruit bank customers to give up their debit cards and PINs, including approaching individuals at parties, schools, or on the street, and using social media outlets, such as Instagram and Facebook, to advertise opportunities for making fast cash by sharing a portion of the fraud proceeds.

On October 23, 2014, a criminal complaint detailing bank and wire fraud charges was filed and six subjects were arrested. On November 19, 2014, the defendants were indicted. All of the defendants have now pleaded guilty, the first pleading in April 2015 and the final pleading during the reporting period on February 19, 2016.

**Source:** U.S. Attorney’s Office, Northern District of Indiana.

**Responsible Agencies:** This is a joint investigation by the FBI, IRS-CID, and FDIC OIG. The case is being prosecuted by the U.S. Attorney’s Office for the Northern District of Indiana.



## Former United Commercial Bank Chief Operating Officer and Chief Credit Officer Ordered to Pay Restitution Totaling Nearly \$1 Billion

On November 9, 2015, the former chief operating officer (COO) and chief credit officer (CCO) of United Commercial Bank (UCB), San Francisco, California, was ordered to pay restitution totaling \$946,737,000. He was ordered to pay the FDIC \$648,000,000 and the Troubled Asset Relief Program \$298,737,000.

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

**Source:** *In May 2009, UCB Holdings, the bank's holding company, made a public announcement that an internal investigation was initiated and its 2008 year-end financial statements could not be relied upon. Once the results of the internal investigation were disclosed to the Board of Directors, the Board reported the results of the internal investigation to DOJ.*

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

## Former Credit Union Officer Pleads Guilty to Embezzlement

On January 20, 2016, the former vice president of accounting at the Houston Police Federal Credit Union pleaded guilty to a criminal Information charging one count of embezzlement from a financial institution.

The embezzlement was ultimately discovered following the bank executive's retirement in February 2015. At that time, a credit union customer brought in a "stale" check to have it re-issued. A "stale" check is an old check that has been issued by the credit union but never cashed. When credit union records showed that the former vice president of accounting had already re-issued the stale check, the credit union conducted an audit of her banking activity.

The audit revealed that from January 1997 until her retirement, she had embezzled at least \$1,247,785 by various means, including, but not limited to, re-issuing stale checks. The credit union maintained a ledger of its stale checks which showed that she re-issued stale checks to credit card companies to pay her personal credit card bills. This included a February 4, 2015, re-issued stale check in the amount of \$7,800 to pay her Chase Bank credit card bill. Some of the re-issued checks even had her credit card number handwritten on them.

**Source:** *The FBI.*

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

## Former Bank Director and Principal Shareholder Sentenced

On October 14, 2015, a former director and principal shareholder of Southwest Community Bank, Springfield, Missouri, was sentenced to serve 78 months in federal prison without parole and was ordered to pay \$3,098,896 in restitution to the victims of his fraud schemes. On April 3, 2015, he pleaded guilty to bank fraud and bankruptcy fraud charges. Southwest Community Bank failed on May 14, 2010.

Beginning on or about May 9, 2005, and continuing through August 14, 2012, this individual misused his position as director and principal shareholder of the bank to obtain approximately \$65,396,132 in loans for about 35 entities in which he had an ownership interest. To obtain these loans, he knowingly submitted fraudulent loan applications containing false statements, fraudulent appraisals, and fictitious or severely misrepresented collateral. As of February 28, 2013, approximately \$14,622,863 of the known debt attributable to the defendant and the entities he owned and controlled had been charged off by the creditor financial institutions. The former director and shareholder and his wife also were majority shareholders in Glasgow Savings Bank in Glasgow, Missouri, which failed on July 13, 2012. Prior to Glasgow Savings Bank's failure, it was one of the oldest operating banks west of the Mississippi River.

**Source:** FDIC DRR.

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

## Former Vice President of Lending Pleads Guilty

On December 14, 2015, the former vice president of lending for Chicago Community Bank, Chicago, Illinois, pleaded guilty to one count of bank fraud, one count of making a false report in bank records, and one count of willful misapplication of bank funds.

The investigation showed and the former vice president admitted that he started manipulating the lending process for various customers of the bank as early as 2004 and continued to manipulate the process until 2009. During this time frame, he regularly accessed the approved lines of credit of certain customers in order to make both principal and interest payments on other unrelated loans. He did this without the knowledge of the customers, but he specifically targeted the lines of credit belonging to customers who knew him well and trusted him. The former vice president executed his scheme by taking cash disbursements from the chosen line of credit and using the cash to make principal and interest payments towards other loans and lines of credit. He admitted that he knew that what he was doing was illegal and against bank policy. As a result of his scheme to defraud, the bank lost at least \$4 million.

**Source:** U.S. Attorney's Office for the Northern District of Illinois.

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

### Former Assistant Controller Sentenced for Embezzlement

On November 13, 2015, the former assistant controller of The Equitable Bank, S.S.B. (TEB), Wauwatosa, Wisconsin, was sentenced to serve 6 months in prison to be followed by 24 months of supervised release and was ordered to pay restitution to TEB of \$216,350.

The former assistant controller, a 25-year employee of TEB, embezzled approximately \$216,350 between March 2009 and March 2013. She embezzled the money by electronically moving funds from a general ledger account used by the bank to hold funds from voided, stale dated checks awaiting escheatment to the State of Wisconsin as unclaimed property, to her own personal checking account at TEB, held jointly with her husband. She then moved the funds by depositing a check to a personal account she held at BMO Harris Bank. From her account at BMO Harris, she used the funds to pay personal expenses (such as tax payments, the purchase of a car, and the loan payoff of her son's car loan), or transferred it internally to her personal savings account.

**Source:** FDIC RMS.

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

### Former Teller Sentenced for Theft

On January 4, 2016, a former employee at The Farmers Bank, Woodland Mills, Tennessee, pleaded guilty to theft, was sentenced to serve 96 months in prison, and was ordered to pay restitution of \$191,769.

The employee served as the vault teller at the bank from September 24, 2002 to July 31, 2015, and was responsible for balancing the cash vault and placing currency orders. The theft was discovered on July 24, 2015, during a cash count that was part of the final phase of the bank's acquisition by another institution. The cash count revealed that vault cash was short \$237,000, and bank officials were unable to reconcile the cash shortage. The former teller ultimately admitted to embezzling the funds from September 2007 through July 2015, by making deposits from her teller drawer to her family's deposit accounts and creating fictitious cash-in tickets to balance the vault.

**Source:** FDIC RMS.

**Responsible Agencies:** This investigation was conducted by the FDIC OIG and the Tennessee Bureau of Investigation. The matter was prosecuted by the Obion County District Attorney's Office.

### Iowa Banker and Co-Conspirators Sentenced

On November 24, 2015, the former senior vice president of Iowa Trust and Savings Bank, Emmetsburg, Iowa, was sentenced to serve 14 months in prison to be followed by 5 years of supervised release. He was also ordered to pay \$207,209 in restitution. In addition, two bank customers were sentenced. One was sentenced to serve 12 months in prison to be followed by 3 years of supervised release and ordered to pay \$58,049 in restitution. The other was sentenced to 3 years of supervised release and ordered to pay \$27,460 in restitution.

According to the charges, from March 2003 until March 2010, the bank customers, with the assistance of the former senior vice president, fraudulently acquired 20 nominee loans totaling approximately \$1,377,994. A number of the loans were acquired by filling out applications without the knowledge or consent of the borrowers and forging their signatures. The money was used for personal expenses, business operating expenses, and classified debt at the bank.

**Source:** FDIC RMS.

**Responsible Agencies:** This is a joint investigation conducted by the FDIC OIG, SBA OIG, Iowa Division of Criminal Investigation, and the FBI. This case is being prosecuted by the U.S. Attorney's Office for the Northern District of Iowa.

## Former Bank Vice President and Branch Manager Sentenced

On February 3, 2016, the former vice president and branch manager of Kansas State Bank, Manhattan, Kansas, was sentenced to serve 27 months in prison to be followed by 2 years of supervised release and was ordered to pay \$277,000 in restitution in connection with her guilty plea for embezzlement.

From May 2012 until June 2014, the former vice president and branch manager misused her position to embezzle approximately \$277,000 from the bank. She was able to accomplish this by diverting funds from the bank's general ledger and forcing daily balancing of the account through fraudulent entries. The money gained from the embezzlement was used to augment her personal lifestyle.

**Source:** FDIC RMS.

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

## Three Sentenced in Bank Fraud Affecting Frontier Bank, LaGrange, Georgia

On February 8, 2016, a licensed real estate agent and owner of Coweta Eagle Construction; another licensed real estate agent; and a borrower were sentenced for their roles in a bank fraud scheme impacting Frontier Bank, LaGrange, Georgia. The real estate agents were each sentenced to 12 months of home detention to be followed by 5 years of supervised release; the agent owning Coweta Eagle Construction was ordered to pay restitution of \$361,900, and the other agent was ordered to pay restitution of \$362,420. The borrower was sentenced to 9 months of home detention to be followed by 5 years of supervised release and was ordered to pay restitution of \$347,160. The restitution orders are joint and several.

According to the indictment, on or about September 29, 2006, a developer formed Karis Park, LLC. Karis Park, LLC was created for the purpose of developing a subdivision known as Karis Park, a condominium project, retail outlet, and common areas located on approximately 33 acres on Lake Martin near Dadeville, Alabama.

In order to purchase the Karis Park property, the developer recruited and obtained commitments to purchase a certain number of lake lots at Karis Park. Prior to acquiring the Karis Park property, the developer solicited the two real estate agents and the borrower to purchase two lake lots each in the Karis Park residential development. In exchange for their agreements to purchase the lake lots, the developer promised to give them each a free lot.

In October 2006, the three signed and provided loan applications to the developer to submit to Frontier Bank for the purpose of applying for loans to purchase the lots. Each of their loan applications contained false and fraudulent misrepresentations regarding their financial status. Based on these fraudulent applications, the three were approved by Frontier Bank for two loans each in the amount of \$860,000 to purchase lots at Karis Park. At closing, \$600,000 of each Frontier loan was applied towards the developer's purchase of the Karis Park property and \$260,000 was held in a line of credit available for construction of a home on each lot.

Also at the request of the developer, the three assisted on the construction and development of Karis Park. In the end, the Karis Park development suffered cost overruns, mismanagement, and poor construction to the extent that many of the homes were never completed or sold. Ultimately, the fraudulent loans were foreclosed, and Frontier Bank suffered hundreds of thousands of dollars in financial losses. Frontier failed on March 8, 2013.

**Source:** FDIC DRR.

**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 Northern District of Alabama.

## Former FDIC Attorney Sentenced for Bank Fraud

A former FDIC attorney was sentenced on February 19, 2016 to 12 months and one day in prison, followed by 2 years of supervised release, for defrauding Wells Fargo Bank in connection with the sham short sale of her home to her live-in boyfriend. She was also ordered to pay \$288,497 in restitution and to forfeit the proceeds of her offense.

The former attorney pleaded guilty on November 17, 2015 to committing bank fraud. The defendant was a senior attorney at the FDIC until September 2014. In 2007, she purchased a home in Nokesville, Virginia, for \$850,000, with mortgages totaling \$807,500 from Wells Fargo Bank. In 2013, she engineered the short sale of her Nokesville home to her boyfriend, who had been living with her at the property for several years.

In order to induce Wells Fargo Bank to approve the short sale and relieve the defendant of her mortgage obligations, she falsely represented to her lender that the sale of the property was an arm's-length transaction to someone with whom she had no close personal relationship. She also falsely certified that she was moving out of the property and claimed she was suffering a financial hardship due to the then-federal pay freeze. In reality, as the defendant has admitted, she had no intention of moving out of the property, despite accepting \$3,000 in relocation assistance in connection with a federal program designed to assist financially distressed short sellers. As a senior FDIC employee, the defendant also had not been subject to the federal pay freeze, and her base annual pay had steadily increased during the time she owned the home, to \$230,000 at the time of the short sale. As a result of the fraudulent short sale transaction, Wells Fargo Bank was required to write off nearly \$300,000 in losses.

**Source:** FHFA OIG.

**Responsible Agencies:** This was a joint investigation by the FDIC OIG and FHFA OIG. The case was prosecuted by the U.S. Attorney's Office for the Eastern District of Virginia.

## Electronic Crimes Unit Responds to Email and Other Schemes

The Electronic Crimes Unit (ECU) continues to work with agency personnel 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 in this international investment scam. During the reporting period, the ECU continued to coordinate with the FBI, Treasury Inspector General for Tax Administration, Department of the Treasury OIG, Internal Revenue Service, and Securities and Exchange Commission OIG on this multi-agency case.

## Strong Partnerships with Law Enforcement Colleagues

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

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

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



## Keeping Current with Criminal Activities Nationwide

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

<b>OIG Headquarters</b>	Financial Fraud Enforcement Task Force, National Bank Fraud Working Group — National Mortgage Fraud Working Sub-group.
<b>New York Region</b>	New York State Mortgage Fraud Working Group; Newark Suspicious Activity Report (SAR) Review Task Force; Philadelphia SAR Review Team; El Dorado Task Force - New York/New Jersey HIDTA; Philadelphia Financial Exploitation Prevention Task Force; Maryland Mortgage Fraud Task Force; Philadelphia Mortgage Fraud Working Group; Pittsburgh SAR Review Team.
<b>Atlanta Region</b>	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.
<b>Kansas City Region</b>	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.
<b>Chicago Region</b>	Dayton, Ohio, Area Financial Crimes Task Force; Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Detroit SAR Review Team; Financial Investigative Team, Milwaukee, Wisconsin; Milwaukee Mortgage Fraud Task Force; Madison, Wisconsin, SAR Review Team; Indiana Bank Fraud Working Group; FBI Louisville Financial Crime Task Force; U.S. Secret Service Louisville Electronic Crimes Task Force; Western District of Kentucky SAR Review Team.
<b>San Francisco Region</b>	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.
<b>Dallas Region</b>	SAR Review Team for Northern District of Mississippi; SAR Review Team for Southern District of Mississippi; Oklahoma City Financial Crimes SAR Review Working Group; Austin SAR Review Working Group.
<b>Electronic Crimes Unit</b>	Washington Metro Electronic Crimes Task Force; Botnet Threat Task Force; High Technology Crime Investigation Association; Cyberfraud Working Group; Council of the Inspectors General on Integrity and Efficiency Information Technology Subcommittee; National Cyber Investigative Joint Task Force; FBI Washington Field Office Cyber Task Force.

# Goal 3: Effective Communications

## Communicate effectively with internal and external stakeholders

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

Importantly, we keep OIG staff informed of office priorities and key activities. We do so through regular meetings among staff and management, bi-weekly updates from senior management meetings, and issuance of OIG newsletters. We also 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 also at Audit Committee meetings where recently issued audit and evaluation reports are discussed. Other contacts occur throughout the year as OIG officials confer with division and office leaders and attend and participate in internal FDIC conferences and other forums.

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

The OIG fully supports and participates in IG community activities through the Council of the Inspectors General on Integrity and Efficiency (CIGIE). We coordinate closely with representatives from the other financial regulatory OIGs. In this regard, the Dodd-Frank Act created the Financial Stability Oversight Council and further established 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 GAO to coordinate work, provide OIG perspectives on risk, and minimize duplication of effort. Similarly we coordinate with the OMB on budgeting and other matters requiring OIG attention. As noted earlier in this report, we also work closely with representatives of the DOJ, including the FBI and U.S. Attorneys' Offices, to coordinate our criminal investigative work and pursue matters of mutual interest.

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

## OIG Work in Support of Goal 3

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

### *FDIC Board and Management:*

- Communicated with the Chairman, Vice Chairman, other FDIC Board Members, the Chief Financial Officer, and other senior FDIC officials through the Acting Inspector General's regularly scheduled meetings with them and through other forums.
- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
- Kept RMS, DRR, the Legal Division, and other FDIC program offices informed of the status and results of our investigative work impacting their respective offices. This was accomplished by notifying FDIC program offices in headquarters and the regional offices of recent actions in OIG cases and providing Office of Investigations' quarterly reports to RMS, DRR, and the Legal Division, outlining activity and results in our cases involving closed and open banks. Coordinated closely with the Legal Division on matters pertaining to enforcement actions and professional liability cases.
- Coordinated with the FDIC Vice Chairman, in his capacity as Chairman of the FDIC Audit Committee, to provide status briefings and present the results of completed audits, evaluations, and related matters for his and other Committee members' consideration.
- Coordinated with DOJ and U.S. Attorneys' Offices throughout the country in the issuance of press releases announcing results of cases with FDIC OIG involvement and routinely informed the FDIC's Office of Communications and Chairman's Office of such releases.
- Attended FDIC Board Meetings, IT/Cyber Security Oversight Group meetings, Complex Financial Institutions Coordination Group meetings, corporate planning and budget meetings, and other senior-level management meetings to monitor or discuss emerging risks at the Corporation and tailor OIG work accordingly.
- 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, Office of Management and Budget A-123, and other key legislation, and communicated our views in the OIG's annual assurance letter.
- Provided the OIG's view of the management and performance challenge areas that we identified at the FDIC, in accordance with the Reports Consolidation Act of 2000 as we conducted audits, evaluations, and investigations: Carrying Out Dodd-Frank Act Responsibilities, Maintaining Strong IT Security and Governance Practices, Maintaining Effective Supervision and Preserving Community Banking, Carrying Out Current and Future Resolution and Receivership Responsibilities, Ensuring the Continued Strength of the Deposit Insurance Fund, Promoting Consumer Protections and Economic Inclusion, Implementing Workforce Changes and Budget Reductions, and Ensuring Effective Enterprise Risk Management Practices.

### *The Congress:*

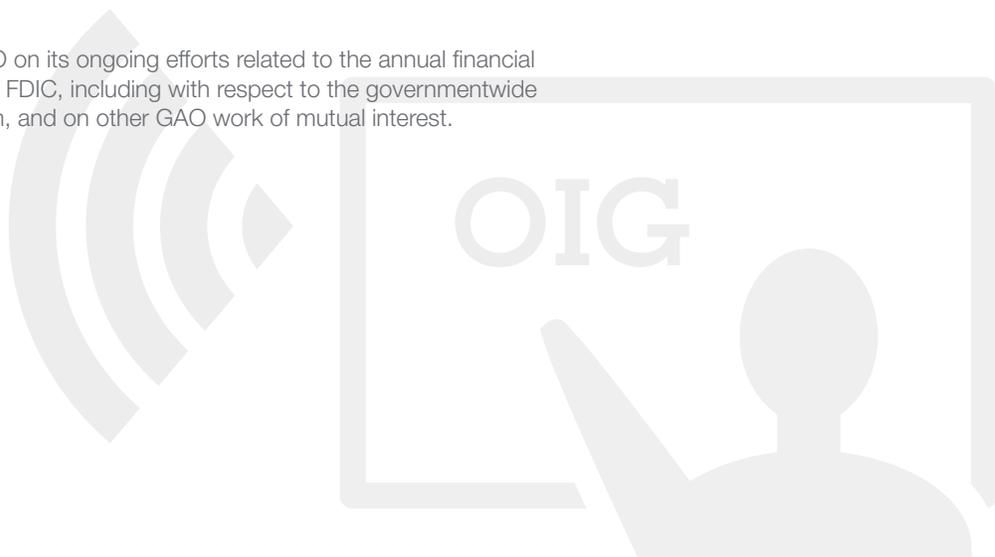
- Maintained congressional working relationships by communicating with various Committee staff on issues of interest to them; providing them our semiannual report to the Congress; notifying interested congressional parties regarding the OIG's completed audit and evaluation work; attending or monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the Corporation's Office of Legislative Affairs on issues of mutual interest.
- More specifically, we briefed and/or responded to interested Congressional parties regarding our refund anticipation loan-related work; ongoing work related to involvement by FDIC non-career officials in the Freedom of Information Act response process; the status of open, unimplemented recommendations; closed audits, evaluations, and investigations that were not made available to the public; and referrals to DOJ and resulting prosecutions.

### *The IG Community:*

- Supported the Inspector General community by attending monthly CIGIE meetings; participating on the CIGIE Audit Committee and the Professional Development Committee (and leading its Human Resources Roundtable); attending Assistant Inspectors General for Investigations, Council of Counsels to the IGs, and other meetings; responding to multiple requests for information on IG community issues of common concern; and commenting on various legislative matters through CIGIE's Legislative Committee.
- Provided an OIG staff member to serve a 1-year detail at CIGIE to provide IT assistance to the Council.
- Communicated with representatives of the OIGs of the federal banking regulators and others to discuss audit, evaluation, and investigative matters of mutual interest and leverage knowledge and resources.
- Participated on CIGFO, as established by the Dodd-Frank Act, and coordinated with the IGs on that council. Joined others on a CIGFO audit team in issuing a report on the Financial Stability Oversight Council's monitoring of interest rate risk to the financial system and provided the FDIC OIG's input to the CIGFO annual report for 2016.

### *The Government Accountability Office:*

- Provided the GAO 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.
- Coordinated with GAO on its ongoing efforts related to the annual financial statement audit of the FDIC, including with respect to the governmentwide financial report system, and on other GAO work of mutual interest.



### *The Public:*

- Continued using our QUEST inquiry intake process, as a supplement to our Hotline, 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. Responded to 167 such inquiries during the past 6-month period.
- Participated in numerous outreach efforts, including providing fraud training for the Federal Financial Institutions Examination Council; sharing information on tracing the movement of funds in financial investigations with contract asset forfeiture investigators from the Bureau of Alcohol, Tobacco, and Firearms; presenting information on insider threats at the annual Southwest Bank Secrecy Act and Financial Crimes Forum in Oklahoma City; speaking to students in a Master's of Accounting forensic accounting course at Northern Illinois University; and presenting information to the Kankakee County, Illinois, Chiefs of Police Association, to provide general information regarding the OIG and share perspectives on issues of mutual concern and importance to the financial services industry.
- Hosted international counterparts from the Deposit Insurance Corporation of Japan who were conducting research comparing the Japanese and U.S. legal systems and their respective approaches for pursuing professional liability cases involving failed banks. Also responded to questions from the Korea Deposit Insurance Corporation regarding the OIG's audit function.
- Developed media training for Office of Investigations' Special Agents in Charge from our regional offices, in the interest of facilitating their future communications with the media related to the completed investigations they conduct in partnership with the Department of Justice.

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

# Goal 4: Enhanced Understanding of Emerging Issues

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

The FDIC OIG keeps current on emerging issues and threats to the FDIC, our own office, and insured depository institutions. A priority area of focus for the OIG is the evolving issue of cyber security. To enhance the OIG's knowledge and understanding of current and emerging cyber threats to our office, the FDIC, the financial services industry at-large, and other federal entities and operations, we have increased our participation in government-wide task forces and law enforcement working groups, and actively expanded our monitoring and awareness of cyber-related matters. The OIG's Cyber Event Group is designed to identify key resources to ensure the OIG's continuous coverage and readiness to address potentially urgent cyber events affecting the FDIC or other federal entities. Further discussion of our efforts in the cyber-security realm is presented below.

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

## **OIG Work in Support of Goal 4**

### **FDIC OIG Increases Efforts to Address Cyber Threats**

The OIG is tackling threats to the FDIC's IT environment on multiple fronts. During the reporting period, we assigned one of our senior managers to serve as a Senior Cyber Security Liaison Officer. In that role, he is monitoring cyber-related activities and potential threats both internal and external to the FDIC and disseminating information to mitigate potential risk or harm to the FDIC, the OIG, and insured depository institutions. Additionally, our OIG Cyber Event Group continues to ensure OIG readiness to address cyber threats to the FDIC and share information with interested parties internal and external to the FDIC. We also continue our coordination with the Division of Information Technology and the Chief Information Officer Organization with respect to detecting and preventing insider threats to the abundance of sensitive information and personally identifiable information held by the Corporation. Together we are seeking to proactively prevent any release by FDIC insiders — accidental or deliberate — of such sensitive information beyond the walls of the FDIC's secure environment — through electronic means such as emailing sensitive information to personal email accounts, downloading such information to removable media devices, or otherwise allowing such information to be disclosed without authorization.

Over the past reporting period, the OIG has also increased its participation in two key cyber-related task forces, in the interest of enhancing our understanding and awareness of current and emerging cyber issues and sharing our own expertise with others seeking to combat cyber threats. These task forces and our involvement are described below.

### **FBI Cyber Task Force**

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

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

The FDIC OIG ECU continued its participation in the Washington Field Office Cyber Squad-4 (CY-4). There are 19 other federal, state, and local law enforcement agencies participating in CY-4, which has a total of 56 members. Through participation in CY-4, the ECU assists with new and ongoing FBI and partner cyber investigations by conducting interviews, victim notifications, forensic evidence review, and search warrants. The ECU agents also have access to many FBI informational systems and cyber notifications allowing them to search for relevant data on subjects and entities already under investigation or intrusions at FDIC-insured banks.

### **National Cyber Investigative Joint Task Force**

The National Cyber Investigative Joint Task Force (NCIJTF) is a multi-agency cyber center that serves as the national focal point for coordinating, integrating, and sharing information related to cyber threat investigations. The task force performs its role through the cooperation and collaboration of its co-located 19 partner agencies, its 4 affiliate member agencies, and its on-site representatives from both international partners and state and local law enforcement organizations. Members have access to a unique, comprehensive view of the nation's cyber threat while working together in a collaborative environment in which they maintain the authorities and responsibilities of their home agencies.

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

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

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

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

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

In addition, the NCIJTF continues to manage and evolve long-standing capabilities, such as its flexible and robust analytical platform that ingests and integrates increasing amounts of information from its partnering agencies. This provides a unique and holistic view of our nation's cyber threat and its vulnerabilities that the NCIJTF shares with cyber stakeholders. As the NCIJTF expands its platform and its capabilities, it helps to mature the analytical, investigative, and network defense capabilities of the U.S. government as well.

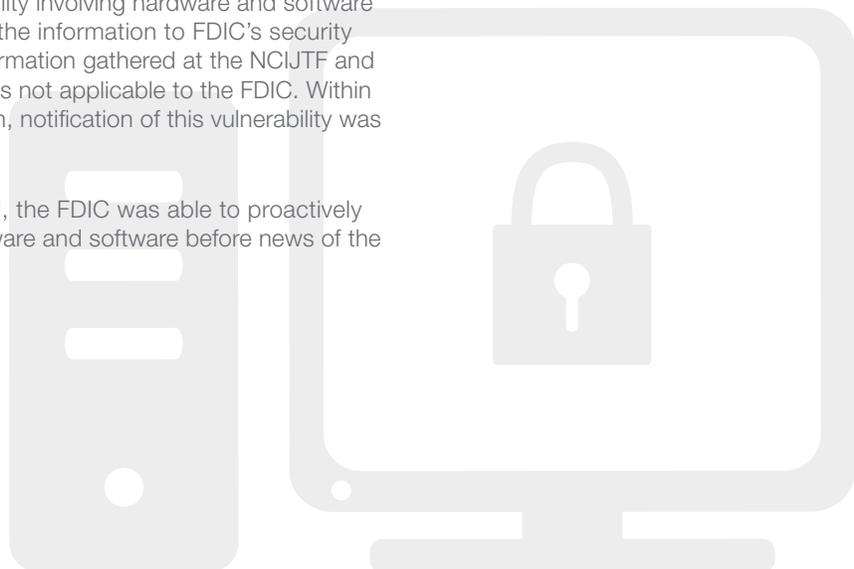
The NCIJTF collaborates directly with colleagues from a group of international U.S. partners. Representatives from Canada, Great Britain, Australia, and New Zealand work with NCIJTF assignees to identify mutual challenges and to develop common solutions in the cyber realm.

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

As a member of the NCIJTF, the FDIC OIG is able to provide insight into the financial industry by acting as a subject matter expert. In addition, the FDIC OIG has been able to coordinate with other federal regulators within the financial industry, including the Securities and Exchange Commission OIG and Office of the Comptroller of Currency.

The OIG's participation and information sharing has paid off. For example, during the reporting period, as a member of the NCIJTF, the OIG's ECU received information regarding a possible vulnerability involving hardware and software used by the FDIC. The ECU transmitted the information to FDIC's security personnel. They were able to use the information gathered at the NCIJTF and made a determination the vulnerability was not applicable to the FDIC. Within days of the ECU providing this information, notification of this vulnerability was available publicly.

Thus, through coordination with the ECU, the FDIC was able to proactively ensure the security of the agency's hardware and software before news of the vulnerability was publicly available.



## Dodd-Frank Act Risk Assessment and Related Work

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

We have subsequently identified areas where we believe we can add value and have initiated assignments in those. To name a few, we are auditing the FDIC's controls for safeguarding sensitive information in resolution plans, and we are conducting evaluations of the FDIC's resolution plan review process and its monitoring of systemically important financial institutions.

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

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

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

The OIG views the above requirements to be highly significant to our office and the Corporation. We are planning for such an eventuality by meeting and researching issues relating to scope, frequency, reporting, and funding, and we will coordinate with corporate officials as needed in carrying out this work should the need arise.



# Goal 5: Operational Efficiency and Workforce Excellence

## Maximize OIG operational efficiency and workforce excellence

While the OIG's audit, evaluation, and investigation work is focused principally on the FDIC's programs and operations, we also hold ourselves to high standards of performance and conduct. We seek to recruit and retain a high-quality staff, and promote employee engagement at all levels of the organization. A major challenge for the OIG over the past few years was ensuring that we had the resources needed to effectively and efficiently carry out the OIG mission at the FDIC, given a sharp increase in the OIG's statutorily mandated work brought about by numerous financial institution failures, the FDIC's substantial resolution and receivership responsibilities, and its new resolution authorities under the Dodd-Frank Act. We now have a bit more discretion in planning our work and have been able to focus attention on certain corporate activities that we have not reviewed for some time. Still, however, we are facing future attrition in our OIG workforce and are currently operating below our authorized staffing level. As a result, we are closely monitoring our staffing and taking steps to ensure we are positioned to sustain quality work to address risk areas 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 seek to ensure effective and efficient use of human, financial, IT, and procurement resources in conducting OIG audits, evaluations, investigations, and other support activities, and have a disciplined budget process to see to that end. In all of our operations, we want to leverage the capabilities of the technological tools at our disposal. That said, we are acutely aware of information security vulnerabilities and take steps to secure and safeguard the information that we possess.

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

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

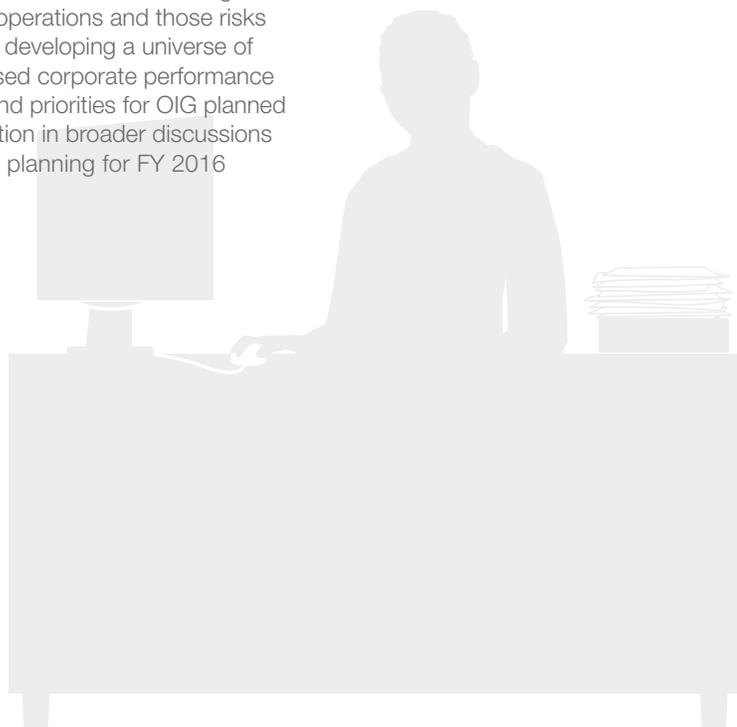
The OIG supports the GPRA Modernization Act of 2010, signed into law on January 4, 2011, and is committed to applying its principles of strategic planning and performance measurement and reporting to our operations. Importantly, the OIG has re-examined the strategic and performance goals and related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

## OIG Work in Support of Goal 5

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

- Carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. Positions filled during the reporting period included several human resources professionals, an Associate Counsel, and two managers for our Office of Audits and Evaluations.
- 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. OIG staff are enrolled in the banking schools at Southwestern Graduate School of Banking, Southern Methodist University, Dallas; Graduate School of Banking, University of Wisconsin, Madison, Wisconsin; Colorado Graduate School of Banking, University of Colorado, Boulder, Colorado; and the American Bankers Association Commercial Lending School, Southwestern Methodist University, Dallas, Texas.
- Employed interns on a part-time basis and a detailee from another federal agency in the OIG to provide assistance on priority issues, including with regard to cyber security.
- Enrolled OIG staff in several different FDIC leadership development programs to enhance their leadership capabilities and supported an OIG staff member selected to participate in the Partnership for Public Service's Financial Leaders Program.
- Hosted a small group of college students for a 3-day information session to explain the role of the FDIC OIG and acquaint them with public service as they pursue possible career paths.
- Provided one of the members of the OIG's Counsel's Office to serve as a Special Assistant U.S. Attorney for multiple cases and trials involving bank fraud. This opportunity allows the Associate Counsel to apply legal skills as part of the prosecutorial teams in advance of and during the trials.
- Reviewed the OIG's performance management and awards programs to foster an understanding of their use and help ensure fairness and consistency in their application.
- Continued efforts to develop and test 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.
- Formed a project team to address issues relating to the OIG's IT environment, with special attention to ensuring effective back-up and recovery processes.

- 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.
- Reviewed and updated a number of OIG internal policies related to audit, evaluation, investigation, and management operations of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the office and made substantial progress converting and transferring such policies to a new automated policies and procedures repository for use by all OIG staff.
- Oversaw contracts to qualified firms to provide audit, evaluation, and other services to the OIG to provide support and enhance the quality of our work and the breadth of our expertise as we conduct audits, evaluations, and other functions and closely monitored contractor performance.
- Continued to monitor, track, and control OIG spending, particularly as it relates to OIG travel-related expenses, use of procurement cards, and petty cash expenditures.
- 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*.
- Relied on OIG Counsel's Office to provide legal advice and counsel to teams conducting audits, evaluations, and special inquiries, and to support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.
- Coordinated with Treasury OIG as that office conducted an investigative peer review of our office as part of the CIGIE 3-year investigative peer review cycle and assisted the Railroad Retirement Board OIG as it prepares for the peer review of the system of quality control for our audit organization.
- Undertook risk-based OIG planning efforts for audits, evaluations, and investigations for FY 2016 and beyond, taking into consideration the goals of, and risks to, FDIC corporate programs and operations and those risks more specific to the OIG. Devoted resources to developing a universe of FDIC programs, activities, and risk areas and used corporate performance goals as further input for identifying risk areas and priorities for OIG planned coverage for the FY. Incorporated such information in broader discussions related to both OIG strategic and performance planning for FY 2016 and 2017.

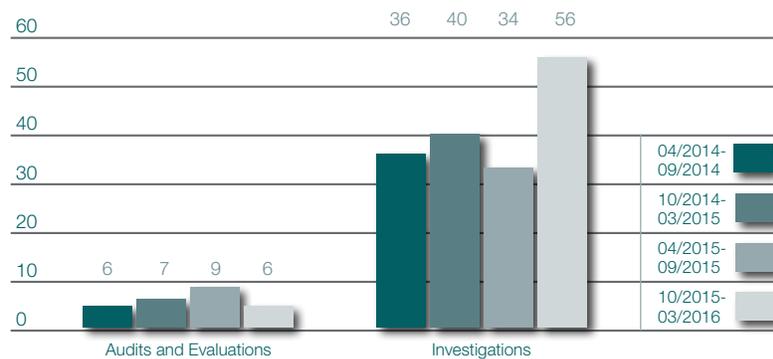


## Cumulative Results (2-year period)

### Nonmonetary Recommendations

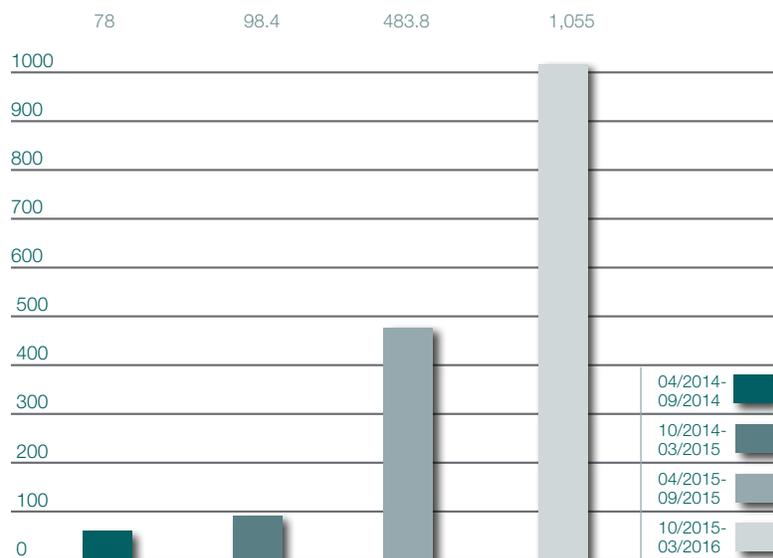
April 2014 – September 2014	27
October 2014 – March 2015	35
April 2015 – September 2015	20
October 2015 – March 2016	12

### Products Issued\* and Investigations Closed



\*Also issued: *Report of Inquiry into the FDIC's Supervisory Approach to Refund Anticipation Loans and the Involvement of FDIC Leadership and Personnel.* (Report No. OIG-16-001)

### 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
<b>Section 4(a)(2)</b> Review of legislation and regulations	48
<b>Section 5(a)(1)</b> Significant problems, abuses, and deficiencies	9-20
<b>Section 5(a)(2)</b> Recommendations with respect to significant problems, abuses, and deficiencies	9-20
<b>Section 5(a)(3)</b> Recommendations described in previous semiannual reports on which corrective action has not been completed	49-50
<b>Section 5(a)(4)</b> Matters referred to prosecutive authorities	8
<b>Section 5(a)(5) and 6(b)(2)</b> Summary of instances where requested information was refused	53
<b>Section 5(a)(6)</b> Listing of audit reports	51
<b>Section 5(a)(7)</b> Summary of particularly significant reports	9-20
<b>Section 5(a)(8):</b> Statistical table showing the total number of audit reports and the total dollar value of questioned costs	52
<b>Section 5(a)(9)</b> Statistical table showing the total number of audit reports and the total dollar value of recommendations that funds be put to better use	52
<b>Section 5(a)(10)</b> Audit recommendations more than 6 months old for which no management decision has been made	53
<b>Section 5(a)(11)</b> Significant revised management decisions during the current reporting period	53
<b>Section 5(a)(12)</b> Significant management decisions with which the OIG disagreed	53

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 enacted law and/or proposed Congressional legislation, including the following as of the end of the reporting period:

- Public Law No. 114-113, the Consolidated Appropriations Act, 2016:
  - Counsel's Office (CO) conducted an informal review of the Act to determine whether any provisions have direct impact on the OIG;
  - A detailed analysis was underway for impact of the Act on the FDIC and on the OIG;
  - A detailed analysis of section 406 of the Cybersecurity Act of 2015, which is Division N of the Consolidated Appropriations Act, which requires a review by federal OIGs regarding agency information security practices, was also underway; and
  - CO also analyzed and provided comments to the Legislation Committee of the Council of the Inspectors General on Integrity and Efficiency, on S. 754, the Cybersecurity Information Sharing Act, on which Division N was based.
- Public Law No. 113-101, the *Digital Accountability and Transparency Act (DATA Act)*: CO monitored developments regarding implementation of the Act's review requirements for federal Offices of Inspector General in general and the FDIC OIG in particular. These developments included:
  - correspondence from the Council of the Inspectors General on Integrity and Efficiency regarding the due dates of OIG review requirements;
  - IG community guidance regarding "readiness audits"; and
  - FDIC and Office of Management and Budget (OMB) views regarding the legal applicability of the DATA Act and related OMB and Department of the Treasury guidance and standards.
- H.R. 4781, the *FDIC Accountability Act of 2016*: CO reviewed this bill and made inquiries regarding appropriations offsets that would be required under the bill and the types of FDIC expenses that would be subject to future appropriations acts that would affect the FDIC.
- H.R. 653, the *FOIA Accountability Act of 2016*, and S.337, the *FOIA Improvement Act of 2016*: CO reviewed both bills, which deal with the Freedom of Information Act (FOIA), to identify provisions that would affect the FDIC OIG directly.
- Executive Order 13714, *Strengthening the Senior Executive Service (SES)*, and the Office of Personnel Management's guidance document, *Strengthening the Senior Executive Service: Implementing the Executive Onboarding Requirement*: CO obtained the FDIC Legal Division's opinion and input and will prepare an analysis for the OIG.
- Executive Order 13719, *Establishment of Federal Privacy Council*: CO considered this Executive Order, which establishes a Federal Privacy Council and requires OMB to issue guidance on the role of a Senior Agency Official for Privacy, and is awaiting OMB's guidance.

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

This table shows the corrective actions management has agreed to implement but has not completed, along with any associated monetary amounts. In some cases, these corrective actions are different from the initial recommendations made in our reports. However, the OIG has agreed that the planned actions meet the intent of the initial recommendations. The information in this table is based on (1) information supplied by FDIC’s Corporate Management Control (CMC), Division of Finance, and (2) the OIG’s determination of closed recommendations. Recommendations are closed when (a) CMC notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, after the OIG confirms that corrective actions have been completed and are responsive. CMC has categorized the status of these recommendations as follows:

### Management Action in Process: (seven recommendations from three reports)

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

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

Report Number, Title & Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
<b>Management Action in Process</b>		
EVAL-15-003 <b>The FDIC’s Supervisory Approach to Cyberattack Risks</b> March 18, 2015	1	Consider and study the IT information security best practices, industry standards and frameworks, and other related guidance and incorporate into the IT-Risk Management Program those features that would strengthen the IT examination program to more specifically address cyber threats and other emerging risks.
	2	Continue to work with the Federal Financial Institutions Examination Council to update the IT Handbook, including eliminating duplication and redundancy contained in the booklets.

**Management Action in Process (continued)**

AUD-15-008	1	Review and clarify, as appropriate, existing policy and guidance pertaining to the provision and termination of banking services to ensure it adequately addresses banking products other than deposit accounts, such as credit products.
<b>FDIC's Role in Operation Choke Point and Supervisory Approach to Institutions that Conducted Business with Merchants Associated with High-Risk Activities</b>		
September 16, 2015	2	Assess the effectiveness of the FDIC's supervisory policy and approach with respect to the issues and risks discussed in this report after a reasonable period of time is allowed for implementation.
	3	Review and clarify, as appropriate, existing supervisory policy and guidance to ensure it adequately defines moral suasion in terms of the types and circumstances under which it is used to address supervisory concerns, whether it is subject to sufficient scrutiny and oversight, and whether meaningful remedies exist should moral suasion be misused.
AUD-15-011	1	Prepare a business case that defines the FDIC's goals and approach for implementing the ICAM program.
<b>The FDIC's Identity, Credential, and Access Management Program (ICAM)</b>		
September 30, 2015	2	Based on the business case developed:  (a) Establish and revise, as appropriate, the roles and responsibilities (including decision-making and accountability) of key parties involved in implementing and overseeing the ICAM program; and  (b) Prepare or update, as appropriate, all ICAM governance documentation to reflect the revised project and governance structure.

**Table II: Audit and Evaluation Reports Issued by Subject Area**

<u>Audit/Evaluation Report</u>		<u>Questioned Costs</u>		<u>Funds Put to Better Use</u>
<b>Number and Date</b>	<b>Title</b>	<b>Total</b>	<b>Unsupported</b>	
<b>Supervision</b>				
EVAL-16-004 March 18, 2016	<i>Interest Rate Risk Management Case Study</i>		N/A	
<b>Receivership Management</b>				
EVAL-16-001 February 11, 2016	<i>The FDIC's Efforts to Ensure Professional Liability Claims Are Cost Effective</i>		N/A	
<b>Resources Management</b>				
AUD-16-001 October 28, 2015	<i>The FDIC's Information Security Program - 2015</i>		N/A	
EVAL-16-002 February 16, 2016	<i>Case Study of a Computer Security Incident Involving a Technology Service Provider</i>		N/A	
AUD-16-002 February 29, 2016	<i>The FDIC's Data Submissions through the Governmentwide Financial Report System as of September 30, 2015</i>		N/A	
EVAL-16-003 March 8, 2016	<i>The FDIC's Freedom of Information Act Response Process</i>		N/A	
<b>Totals for the Period</b>		<b>\$0</b>	<b>\$0</b>	<b>\$0</b>

**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
<b>Subtotals of A &amp; B</b>	<b>0</b>	<b>\$0</b>	<b>\$0</b>
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
<b>Subtotals of A &amp; B</b>	<b>0</b>	<b>\$0</b>
C. For which a management decision was made during the reporting period.	0	\$0
(i) dollar value of recommendations that were agreed to by management.	0	\$0
- based on proposed management action.	0	\$0
- based on proposed legislative action.	0	\$0
(ii) dollar value of recommendations that were not agreed to by management.	0	\$0
D. For which no management decision has been made by the end of the reporting period.	0	\$0
Reports for which no management decision was made within 6 months of issuance.	0	\$0

### **Table V: Status of OIG Recommendations Without Management Decisions**

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

### **Table VI: Significant Revised Management Decisions**

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

### **Table VII: Significant Management Decisions with Which the OIG Disagreed**

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

### **Table VIII: Instances Where Information Was Refused**

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

# Appendix 2

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

### FDIC OIG Review Activity for the Period October 1, 2015 through March 31, 2016

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

Institution Name	Closing Date	Estimated Loss to DIF (Dollars in Millions)	Grounds Identified by the State Bank Supervisor for Appointing the FDIC as Receiver	Unusual Circumstances Warranting In-depth Review?
<b>Reviews Completed</b>				
Edgebrook Bank (Chicago, Illinois)	5/8/15	\$16.8	The bank was conducting its business in an unsafe and unsound manner.	No
Highland Community Bank (Chicago, Illinois)	1/23/15	\$5.8	The bank was conducting its business in an unsafe and unsound manner.	No
Northern Star Bank (Mankato, Minnesota)	12/19/14	\$5.9	The bank was in an unsafe and unsound condition to transact banking business; it was unsafe and inexpedient for the bank to continue its business; the bank's ability to meet its financial obligations was questionable.	No
Eastside Commercial Bank (Conyers, Georgia)	7/18/14	\$33.9	The bank was critically undercapitalized for Prompt Corrective Action purposes.	No
The Freedom State Bank (Freedom, Oklahoma)	6/27/14	\$5.8	The institution failed to maintain adequate capital and was engaging in unsafe and unsound banking practices.	No

**FDIC OIG Review Activity for the Period  
October 1, 2015 through March 31, 2016**

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

Institution Name	Closing Date	Estimated Loss to DIF (Dollars in Millions)	Grounds Identified by the State Bank Supervisor for Appointing the FDIC as Receiver	Unusual Circumstances Warranting In-depth Review?
<b>Reviews Completed (continued)</b>				
The Bank of Georgia (Peachtree City, Georgia)	10/2/15	\$23.2	The financial condition of the bank did not permit it to meet certain requirements of a June 30, 2009 Consent Order, including requirements to maintain minimum capital levels. In addition, the bank was Critically Undercapitalized for purposes of Prompt Corrective Action, presenting a significant safety and soundness risk.	No
<b>Reviews Ongoing</b>				
North Milwaukee State Bank (Milwaukee, Wisconsin)	3/11/16	\$9.6		

# 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

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

- The U.S. 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.

#### 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.

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 considered 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](http://www.fdicig.gov).

Our Office of Audits and Evaluations is currently preparing to be peer reviewed by the Railroad Retirement Board OIG, an engagement that will commence soon.

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

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

As is customary, we also issued a Letter of Comment, dated April 30, 2014, that set forth findings and recommendations that were not considered to be of sufficient significance to affect our opinion expressed in the system review report. We made 14 recommendations. NARA OIG agreed with 11 of the 14 recommendations, partially agreed with one recommendation, and did not agree with the remaining two recommendations. NARA's planned actions adequately addressed the 11 recommendations with which NARA agreed. With respect to the remaining three, NARA's response included a rationale for its decision not to fully address those recommendations. Estimated completion dates for corrective actions ranged from June 30, 2014 to September 30, 2014. In an earlier semiannual report, we noted that NARA OIG advised us that it had completed actions on all but two of the agreed-upon recommendations and planned full implementation of the two outstanding recommendations by March 31, 2015. In updating the status for the last reporting period, NARA OIG informed us that it had revised the planned implementation date from March 31, 2015 to September 30, 2016. That status has not changed. NARA OIG posted the peer review report (system review report) on its Web site at [www.archives.gov/oig/](http://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. For our office, applicable Attorney General Guidelines include the *Attorney General Guidelines for Offices of Inspectors General with Statutory Law Enforcement Authority* (2003), *Attorney General Guidelines for Domestic Federal Bureau of Investigation Operations* (2008), and *Attorney General Guidelines Regarding the Use of Confidential Informants* (2002).

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

# Congratulations and Farewell

## Congratulations and farewell to members of the FDIC OIG who have recently retired:



**John Davidovich**

John retired from our office in early January 2016 following 25 years of work at the FDIC. John's career was multi-faceted, and at every turn, he excelled — first as an Assistant State's Attorney in DuPage County, Illinois; then as a Trial Attorney at the Department of Justice; as a Senior Attorney, Counsel, and Supervisory Counsel in the FDIC Legal Division; and most recently during his 6 years as the Counsel to the Inspector General. John was recognized as an Outstanding Assistant State's Attorney, and as a recipient of the FDIC General Counsel's Award and the Department of Justice's John Marshall Award for Interagency Cooperation in Support of Litigation.



**Jennifer Etheridge**

Jennifer retired after more than 39 years of federal service. Her career began in the summer of 1974 when she was a library assistant trainee at the D.C. Public Library. In 1975, she worked at the National Labor Relations Board as a summer aide. In 1977, she joined the Department of Commerce, Census Bureau, as a federal junior fellow and in 1981 she became a voucher examiner at the Department of Energy. By 1982, she had started work in the OIG at the U.S. Department of Agriculture as an accountant, where she was later promoted to an auditor position. In 1985, she joined the FDIC's Office of Corporate Audits and Internal Investigations, which later became the FDIC OIG. Over the years, Jennifer played a key role with respect to assignments covering financial, procurement, and administrative operations of the Corporation.



### **Joe Uricheck**

Joe retired after more than 32 years of federal service. He can boast an OIG career from beginning to end, having entered the government as an auditor in the OIG at the Veteran's Administration and leaving the government as an audit specialist in the FDIC OIG all these years later. Joe made multiple contributions to our office since joining the FDIC OIG in 1991. Joe also cared deeply about the OIG workplace and participated over the years in

Employee Groups to help communicate staff concerns to OIG management, in the interest of making our office a better place to work. Joe was also a Certified Public Accountant and a Certified Fraud Examiner, two professional certifications that served him and our office very well.



### **Nick "Ravi" Ravichandran**

Ravi retired after more than 30 years of federal service. His federal career began in 1985 when he joined the U.S. General Accounting Office (GAO) (now the Government Accountability Office) in Atlanta, Georgia, as an evaluator. In March 1987, he transferred to the GAO's headquarters in Washington, D.C. In September 1990, he joined the Resolution Trust Corporation (RTC) OIG, which merged with the FDIC OIG upon the RTC's sunset

in December 1995. His role at the RTC as a senior audit specialist involved coordinating the work of the RTC OIG auditors in certain field sites — a task that was instrumental in the RTC OIG's overall success. During his time at the FDIC, he served with distinction, including while serving for a time as a resolutions and closings manager in the Division of Resolutions and Receiverships in the FDIC's East Coast Temporary Satellite Office in Jacksonville, Florida.

Prior to retiring, Ravi assisted on a risk-based inventory and planning process for the Office of Audits and Evaluations. He played an important role on multiple audit teams over the years and also provided valuable input to Office of Audits and Evaluations' internal quality control reviews.





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

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

# 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](mailto: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.