

OIG

APRIL 1

2015

SEPTEMBER 30

2015

OFFICE OF INSPECTOR GENERAL
SEMIANNUAL REPORT TO THE CONGRESS

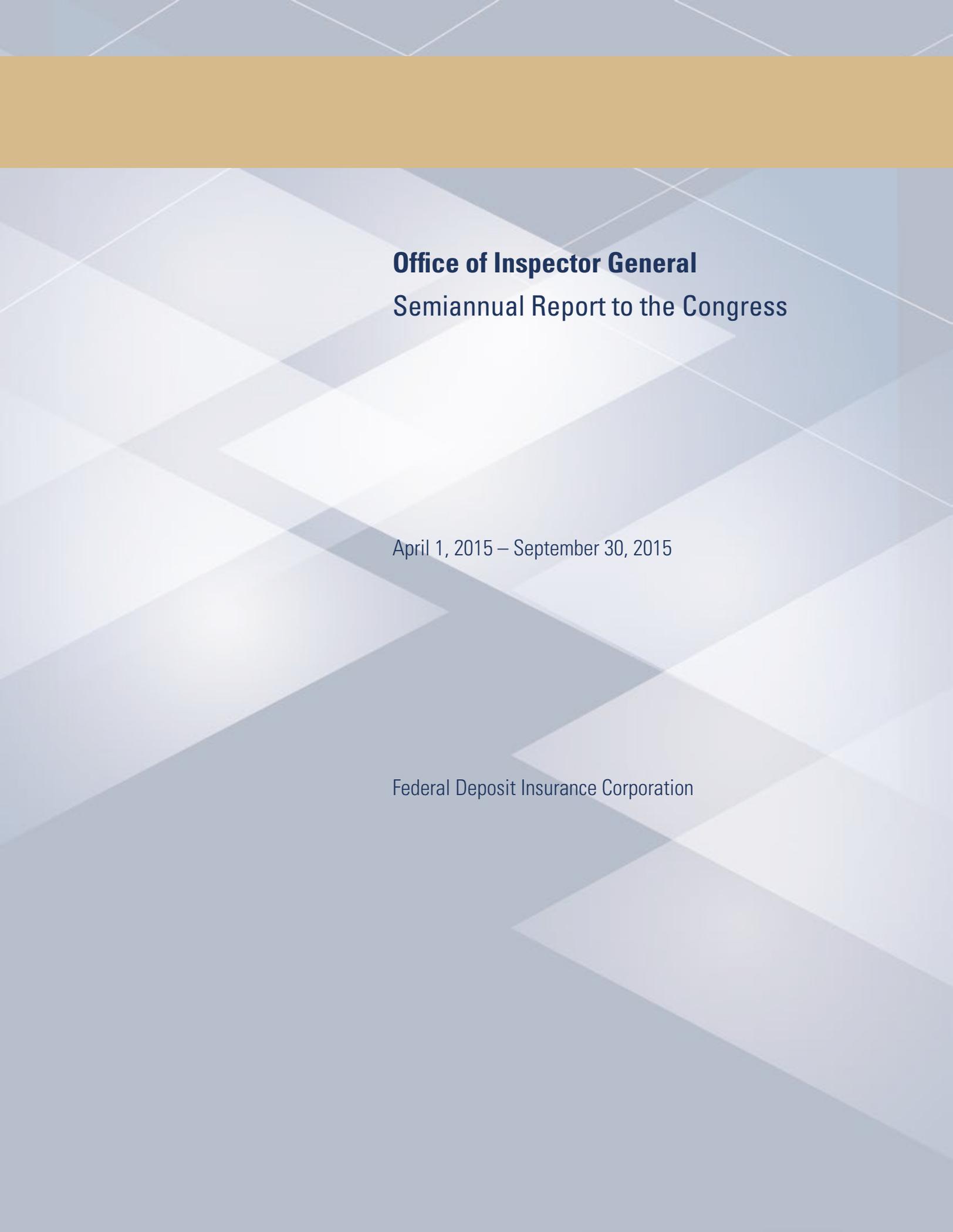


FDIC

FEDERAL DEPOSIT INSURANCE CORPORATION

The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the Congress to maintain stability and confidence in the nation's banking system by insuring deposits, examining and supervising financial institutions, and managing receiverships. Approximately 6,500 individuals carry out the FDIC mission throughout the country. According to most current FDIC data, the FDIC insured more than \$6.35 trillion in deposits in 6,348 institutions, of which the FDIC supervised 4,037. As a result of institution failures during the financial crisis, the balance of the Deposit Insurance Fund turned negative during the third quarter of 2009 and hit a low of negative \$20.9 billion by the end of that year. The FDIC subsequently adopted a Restoration Plan, and with various assessments imposed over the past few years, along with improved conditions in the industry, the Deposit Insurance Fund balance has steadily increased to a positive \$70.1 billion as of September 30, 2015. Receiverships under FDIC control as of September 30, 2015, totaled 470, with about \$5.5 billion in assets.





Office of Inspector General
Semiannual Report to the Congress

April 1, 2015 – September 30, 2015

Federal Deposit Insurance Corporation



I am pleased to present the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General's (OIG) semiannual report for the period April 1, through September 30, 2015. 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 9 audit and evaluation reports covering a variety of significant issues and made 20 recommendations for improvements. Our investigations resulted in 130 indictments or informations, 109 convictions, 59 arrests, and potential monetary benefits in excess of \$577 million. Several examples of our accomplishments from the reporting period follow and are discussed in more detail in our report.

- We completed a comprehensive review of the FDIC's role in Operation Choke Point and the Corporation's supervisory approach to institutions that conducted business with merchants associated with high-risk activities. This body

of work was prompted by a request from 35 Members of the Congress and a related request from the FDIC Chairman. We determined that the FDIC's role in Operation Choke Point was inconsequential. We also determined that particular individuals did not pursue their own personal, political, or moral agendas aimed at forcing lawfully operating businesses on a high-risk list out of the banking sector. However, we identified another matter involving the FDIC's actions regarding refund anticipation loans that warranted further review, and that work was ongoing as of the end of the reporting period. We made three recommendations in the report related to clarifying policy and guidance for providing and terminating banking services; assessing the revised policy and guidance after a reasonable time for implementation; and clarifying, as appropriate, supervisory policy and guidance to ensure that moral suasion is adequately addressed.

Importantly, we conducted a related investigation prompted by concerns on the part of the Congress that the Deputy General Counsel had provided false testimony in connection with Operation Choke Point. We concluded that the Deputy General Counsel did not knowingly or willfully provide the Congress with materially false, fictitious or fraudulent testimony.

- We also issued the results of three material loss reviews during the reporting period—a bit surprising at a time when failures are on the decline. One of those involved the failure of Doral Bank of Puerto Rico—causing losses to the DIF estimated at \$698 million. Another of the reviews involved the failure of a minority depository institution, where we determined that the bank failed primarily because its Board and management did not properly manage the risks associated with the bank's growth strategy that was centered on higher-risk commercial real estate loans, including acquisition, development, and construction, church and religious organizations, and gas and convenience store loans. Our third material loss review examined the failure of a relatively small bank in Illinois, and in that case, the institution failed primarily because of lax oversight by its Board and a dominant chief executive officer who implemented a risky business strategy.
- Our Office of Investigations, in partnership with U.S. Attorneys and law enforcement colleagues throughout the country, successfully brought to justice numerous former bank officials and other bank-affiliated parties who had used their positions of trust to undermine the integrity of the banking system. Of special note, in a case we highlighted in our last semiannual report, the former chief operating officer and chief credit officer of United Commercial Bank, San Francisco, California, was sentenced to serve 97 months in prison for his role in a securities fraud scheme and other corporate fraud offenses stemming from the failure of that bank. He had earlier been found guilty of conspiring with others within the bank to falsify key bank records to conceal millions of dollars in losses and falsely inflate the bank's financial statements.

- In another important case, the nature of which was somewhat unusual for our office, a West Virginia bank, the Bank of Mingo, was charged with violating the Bank Secrecy Act (BSA) over a period of more than 3 years. The Bank of Mingo admitted that its failure to file currency transaction reports was not only in breach of its own BSA/Anti-Money Laundering Program but also a violation of the BSA and corresponding regulations.
- In connection with another complex fraud case, we are reporting multiple actions involving Park Avenue Bank, New York, New York, including stiff sentences and restitution imposed on a businessman, an investment advisor, the bank's former senior vice president, and the bank's former president and chief executive officer, all of whom were complicit in a fraud that contributed to the bank's failure. Sentences for these individuals range from 21 months to 12 years in prison and ordered restitution exceeds \$220 million.
- Finally, and of extreme importance, during the reporting period we took steps to enhance our understanding and involvement in the IT security and cyber arena on multiple fronts. Our efforts include establishing an OIG Cyber Threat Working Group, increasing our involvement with the FBI's Cyber Task Force in Washington DC, and assigning one of our agents to serve as our representative on the National Cyber Investigative Joint Task Force, a group focusing on cyber threat investigations across the federal, state, local, and international law enforcement, intelligence, counterintelligence, and military communities. Our goal is to leverage the expertise and experience of our own staff, subject matter experts in other parts of the FDIC, and investigative entities external to the Corporation to more fully understand cyber threats, respond as needed, and share information as we seek to protect the FDIC's and the nation's critical infrastructure.

Our former Inspector General resigned to become the Department of Defense Inspector General on September 27, 2013. I have been honored to lead our office since that time. Jay N. Lerner from the Department of Justice OIG has been nominated to serve as the next FDIC Inspector General, and his confirmation hearing was held before the Senate Banking Committee on September 29, 2015.

In closing, I would like to acknowledge the support and cooperation of FDIC officials throughout the country as we have conducted our work during the past 6 months. On behalf of the office, I underscore our commitment to all of 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 carry out our independent oversight role, strive to help the FDIC accomplish its mission, and work in the best interest of the American people.



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

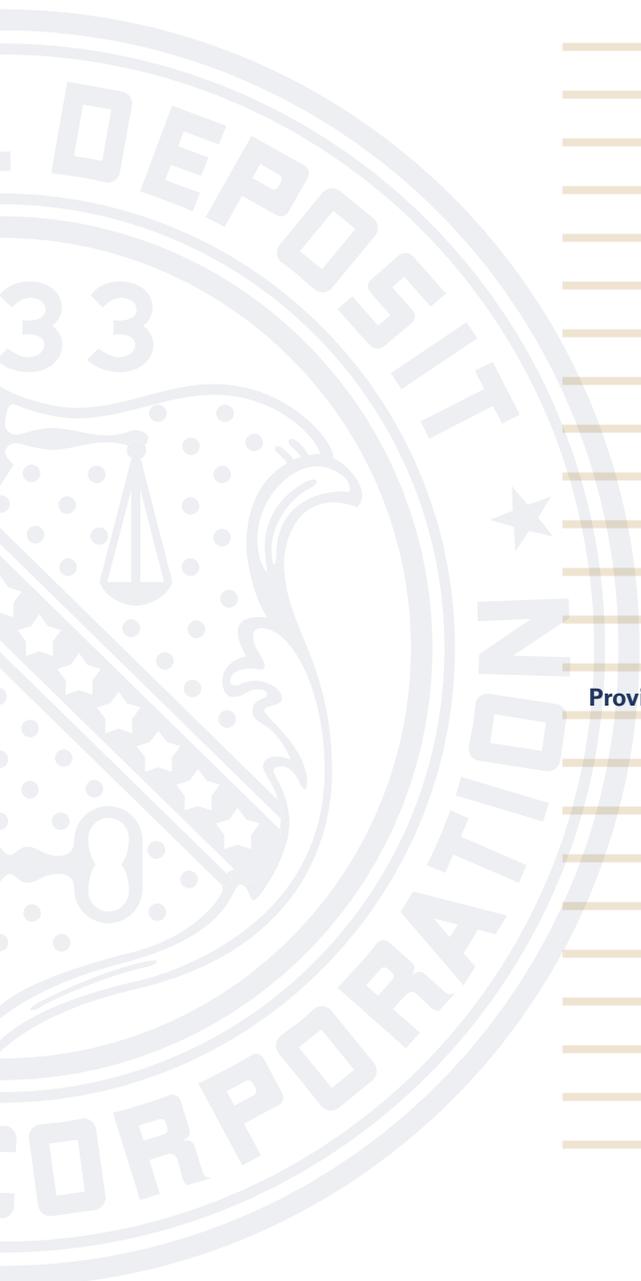
Table of Contents

Acting Inspector General’s Statement	ii
Acronyms and Abbreviations	2
Highlights and Outcomes	4
Strategic Goal Areas	
Goal 1: Supervision	
Assist the FDIC to Ensure the Nation’s Banks Operate Safely and Soundly	11
Goal 2: Insurance	
Help the FDIC Maintain the Viability of the Insurance Fund	44
Goal 3: Consumer Protection	
Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy	46
Goal 4: Receivership Management	
Help Ensure that the FDIC Efficiently and Effectively Resolves Failing Banks and Manages Receiverships	51
Goal 5: Resources Management	
Promote Sound Governance and Effective Stewardship and Security of Human, Financial, Information Technology, and Physical Resources	57
Goal 6: OIG Resources Management	
Build and Sustain a High-Quality OIG Staff, Effective Operations, OIG Independence, and Mutually Beneficial Working Relationships	68
Reporting Requirements	78
Appendix 1	
Information Required by the Inspector General Act of 1978, as amended	79
Appendix 2	
Information on Failure Review Activity	83
Appendix 3	
Peer Review Activity	84
Congratulations and Farewell	86

Acronyms and Abbreviations



BSA	Bank Secrecy Act
CBA	centrally billed account
CCB	Capitol City Bank & Trust Company
CEO	chief executive officer
CFPB	Consumer Financial Protection Bureau
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CRE	commercial real estate
CTR	currency transaction report
CY-4	Washington Field Office Cyber Squad-4
DFC	Doral Financial Corporation
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
EAR	Equipment Acquisition Resources, Inc.
ECU	Electronic Crimes Unit
FBI	Federal Bureau of Investigation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Modernization Act of 2014
FRB	Board of Governors of the Federal Reserve System
FY	fiscal year
GPRA	Government Performance and Results Act of 1993
GSA	General Services Administration



- HSLC** The Home Savings and Loan Company of Youngstown, Ohio
- IBA** individually billed account
- ICAM** Identity, Credential, and Access Management
- IRS** Internal Revenue Service
- IRS-CI** Internal Revenue Service Criminal Investigation Division
- IT** information technology
- MDI** minority depository institution
- NARA** National Archives and Records Administration
- NCIJTF** National Cyber Investigative Joint Task Force
- OCFI** Office of Complex Financial Institutions
- OCFIPR** Office of the Commissioner of Financial Institutions of Puerto Rico
- OIG** Office of Inspector General
- OMB** Office of Management and Budget
- PIV** personal identity verification
- Providence P&C** Providence Property and Casualty Insurance Company
- RAL** refund anticipation loan
- RMS** Division of Risk Management Supervision
- SAR** suspicious activity report
- SBA** Small Business Administration
- SEC** U.S. Securities and Exchange Commission
- SIGTARP** Special Inspector General for the Troubled Asset Relief Program
- SLA** shared loss agreement
- UCB** United Commercial Bank
- VBI** Valley Bank, Moline, Illinois

The OIG conducts its work in five strategic goal areas that are linked to the FDIC's mission, programs, and activities, and one that focuses on the OIG's internal business and management processes. A summary of our completed work during the reporting period, along with references to selected ongoing assignments, is presented below, by goal area. We have revised our goals and related performance indicators as we plan for fiscal year (FY) 2016 and 2017. In the interim, for FY 2015, we are highlighting our work within the framework of the goal areas that follow.

Strategic Goal 1: Supervision

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

Our work in helping to ensure that the nation's banks operate safely and soundly takes the form of audits, investigations, evaluations, and extensive communication and coordination with FDIC divisions and offices, law enforcement agencies, other financial regulatory OIGs, and banking industry officials. In support of this goal, during the reporting period, and at the request of 35 Members of the Congress, we issued a comprehensive report on the FDIC's role in Operation Choke Point and the Corporation's supervisory approach to institutions that conducted business with merchants associated with high-risk activities. We determined that the FDIC's role in Operation Choke Point was inconsequential. We also determined that particular individuals did not pursue their own personal, political, or moral agendas aimed at forcing lawfully operating businesses on a high-risk list out of the banking sector. However, we identified another matter involving the FDIC's actions regarding refund anticipation loans that warranted further review, and that work is ongoing. We made three recommendations in the report related to clarifying policy and guidance for providing and terminating banking services; assessing the revised policy and guidance after a reasonable time for implementation; and clarifying, as appropriate, supervisory policy and guidance to ensure that moral suasion is adequately addressed. Importantly, with respect to the related Congressional concern regarding the testimony of the FDIC Deputy General Counsel, we concluded that the Deputy General Counsel did not knowingly or willfully provide the Congress with materially false, fictitious or fraudulent testimony. We also issued three material loss review reports during the period, including a material loss review of Doral Bank, San Juan, Puerto Rico, whose failure caused losses to the Deposit Insurance Fund of approximately \$698 million. We made two recommendations in that report relating to ensuring compliance with Federal Deposit Insurance Act examination frequency requirements and revising policy guidance to document responsibilities of regional accountants relating to analyzing complex accounting transactions and escalating such matters within the Division of Risk Management Supervision (RMS).

1933

With respect to investigative work, as a result of cooperative efforts with U.S. Attorneys throughout the country, numerous individuals were prosecuted for financial institution fraud, and we also successfully pursued a number of mortgage fraud schemes. Our efforts in support of bank fraud, mortgage fraud, and other financial services working groups also supported this goal. Particularly noteworthy results from our casework include the pleas and sentencing of a number of former senior bank officials and bank customers involved in fraudulent activities that undermined the institutions and, in some cases, contributed to the institutions' failures. For example, the Chief Executive Officer of United Commercial Bank, based in San Francisco, California, was sentenced to 97 months in prison for conspiring with others within the bank to falsify key bank records to conceal millions of dollars in losses and falsely inflate the bank's financial statements. In another important case, the Bank of Mingo was charged with violating the Bank Secrecy Act (BSA) and admitted that it failed to file suspicious activity reports and currency transaction reports, which constituted a breach of its own BSA/Anti-Money Laundering Program and the BSA itself. In another case, we are reporting multiple actions related to a complex fraud involving Park Avenue Bank, New York, New York, including stiff sentences and fines imposed on a businessman, an investment advisor, the bank's former senior vice president, and the bank's former president and chief executive officer, all of whom were complicit in a fraud that contributed to the bank's failure.

The Office of Investigations also continued its close coordination and outreach with RMS, the Division of Resolutions and Receiverships, and the Legal Division by way of attending quarterly meetings, regional training forums, and regularly scheduled meetings with RMS and the Legal Division to review suspicious activity reports and identify cases of mutual interest. We have coordinated regularly on enforcement action matters with the Legal Division and RMS, an activity that continues to be mutually beneficial. (See pages 11-43.)

Strategic Goal 2: Insurance

Help the FDIC Maintain the Viability of the Insurance Fund

We did not conduct specific assignments to address this goal area during the reporting period. However, our audit and evaluation work in support of goal 1 fully supports this goal, as does the investigative work highlighted above. In both cases, our work can serve to strengthen the FDIC's supervisory program and help prevent or lessen future failures. Further, the deterrent aspect of investigations and the ordered restitution may help to mitigate an institution's losses and losses to the Deposit Insurance Fund. (See pages 44-45.)

Strategic Goal 3: Consumer Protection

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

In support of this goal area, we completed work with OIG counterparts on an evaluation assignment to assess the extent to which the prudential regulators and the Consumer Financial Protection Bureau were coordinating their supervisory activities and avoiding duplication of regulatory oversight responsibilities. Our joint report concluded that the Consumer Financial Protection Bureau and prudential regulators were generally coordinating their regulatory oversight activities for federal consumer financial laws consistent with the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) and the provisions of a memorandum of understanding governing coordinating activities. However, we also cited opportunities for improved coordination among the parties involved.

Our Office of Investigations also supports consumer protection through its work. Investigators continue to pursue cases of misrepresentation of FDIC insurance or affiliation where unscrupulous individuals attempt to convince others to invest in financial products allegedly insured by or endorsed by the FDIC. Our Electronic Crimes Unit also responds to instances where fraudulent emails purportedly affiliated with the FDIC are used to entice consumers to divulge personal information and/or make monetary payments. Working with the Corporation's Chief Information Officer Organization, our investigators seek to protect consumers by dismantling such schemes. In further support of consumer protection, the OIG also continued to respond to a number of inquiries from the public, received both through our Hotline and through other channels. We addressed about 225 such inquiries during the past 6-month period. (See pages 46-50.)

Strategic Goal 4: Receivership Management

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

We completed two assignments involving the FDIC's receivership management activities. In one, we reported on the FDIC's controls over cash flows from receivership-related federal income tax refunds, and in that report we made five recommendations and identified \$4.6 million in funds put to better use. In a second assignment, we reviewed the risks associated with terminations of shared loss agreements and made a recommendation for a policy to help ensure program understanding, process compliance, and consistent treatment of early termination transactions.

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

From an investigative standpoint, our Electronic Crimes Unit continued to support investigative activities related to closed banks by providing computer forensic assistance in ongoing fraud investigations. Of note in that regard during the reporting period was the Electronic Crimes Unit's assistance related to the failure of Doral Bank, where forensic support is helping to establish accountability for various actions taken that proved detrimental to the bank's safety and soundness. (See pages 51-56.)

Strategic Goal 5: Resources Management

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

In support of this goal area, during the reporting period, we issued the results of two reviews of FDIC internal programs. In the first, we assessed the status of the FDIC's Identity, Credential, and Access Management (ICAM) Program and identified issues that needed to be addressed to clarify the long-term direction of the program. Overall, despite a relatively significant investment in corporate resources involved, the ICAM program was not subject to sufficient and consistently robust governance, which resulted in limited success. Our second review in this area examined the FDIC's controls over its Travel Card Program, wherein we did not identify any material weaknesses within the scope of controls we assessed. We did, however, make five recommendations, primarily involving enhancements to policies, procedures, and guidelines to clarify program requirements and formally establish practices to strengthen controls and safeguards. At the end of the reporting period, we were completing our annual work under the Federal Information Security Modernization Act of 2014. We were also conducting risk assessments of the contracting and financial management operations of the Corporation, in the interest of identifying any vulnerabilities that we may want to address in future work.

From an investigative standpoint, we completed a case involving UPS delivery practices and related charges to federal agencies, including the FDIC. This case helped resolve False Claims allegations and led to UPS agreeing to pay \$25 million. Assistance from the FDIC's Division of Administration was instrumental in the success of this case.

We promoted integrity in FDIC internal operations through ongoing OIG Hotline and other referrals and coordination with the FDIC's Divisions and Offices, including corporate labor and employee relations staff and ethics officials, as warranted. (See pages 57-67.)

Strategic Goal 6: OIG Resources Management

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

To ensure effective and efficient management of OIG resources, we continued to focus on a number of internal initiatives. We submitted to the FDIC Chairman a proposed budget of \$36 million for FY 2017 (an increase over the budgets of the past 4 fiscal years), and received the Chairman's approval. We closely monitored staffing and in the interest of succession planning, took steps to ensure that our office is positioned to handle anticipated attrition through a number of completed and planned hiring efforts. We tracked OIG spending, particularly costs involved in travel and procurements. We continued to develop a better system to capture data on our investigative cases and took steps to implement enhanced capabilities of TeamMate for our audit and evaluations staff. On an office-wide level, we continued to re-examine and update our policies and procedures and enhance our records management and disposition activities.

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

We encouraged individual growth through professional development by supporting individuals in our office involved in professional organizations, pursuing professional certifications, or attending graduate schools of banking. We continued our mentoring program for 2015 to further develop a strong cadre of OIG resources. We supported OIG staff members taking FDIC leadership training courses. We brought on a detailee from another FDIC division and supported one of our own staff on a detail to another FDIC division. We also employed interns on a part-time basis to promote the interns' professional development and assist us in our work.

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

In the area of risk management, we increased our involvement in multiple government-wide task forces established to understand, identify, and thwart current and emerging cyber threats. In connection with SAS 99 and the annual audit of the FDIC's financial statements, we shared our perspectives on the risk of fraud at the FDIC with the U.S. Government Accountability Office. We also assessed our internal control environment in preparation for the OIG's annual assurance statement to the FDIC Chairman. We monitored the Corporation's progress meeting annual performance goals and attended meetings of various corporate committees to further monitor risks at the Corporation and tailor OIG work accordingly. We shared OIG perspectives on risk areas with senior FDIC leadership. In keeping with the Reports Consolidation Act of 2000, we monitored those areas that we had identified as management and performance challenges facing the Corporation for inclusion in its annual report and conducted and planned assignments in a number of those areas. (See pages 68-76.)

Significant Outcomes

April 1, 2015–September 30, 2015

Audit and Evaluation Reports Issued	9
Questioned Costs or Funds Put to Better Use	\$4,586,022
Nonmonetary Recommendations	20
Investigations Opened	82
Investigations Closed	74
OIG Subpoenas Issued	19
Judicial Actions:	
Indictments/Informations	130
Convictions	109
Arrests	59
OIG Investigations Resulted in:	
Fines of	\$ 1,110,690
Restitution of	492,807,166
Asset Forfeitures of	83,186,942
Total	\$ 577,104,798
Cases Referred to the Department of Justice (U.S. Attorney)	78
Proposed Legislation and Regulations Reviewed	7
Responses to Requests Under the Freedom of Information/Privacy Acts	6

Strategic Goal 1: Supervision

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

The Corporation's supervision program promotes the safety and soundness of FDIC-supervised insured depository institutions. The FDIC is the primary federal regulator for 4,037 FDIC-insured, state-chartered institutions that are not members of the Board of Governors of the Federal Reserve System (FRB)—generally referred to as “state non-member” institutions. As insurer, the Corporation also has back-up examination authority to protect the interests of the Deposit Insurance Fund (DIF) for 2,311 national banks, state-chartered banks that are members of the FRB, and savings associations regulated by the Office of the Comptroller of the Currency.

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

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

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

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

In July 2015, RMS established an Operational Risk group. This group initially will have responsibility for IT policy, IT examinations, cybersecurity, and critical infrastructure protection programs.

The OIG's audits and evaluations address various aspects of the Corporation's supervision and examination activities, and, through their investigations of financial institution fraud, the OIG's investigators also play a critical role in helping to ensure the nation's banks operate safely and soundly. The OIG's Office of Investigations works closely with FDIC management in RMS, the Division of Resolutions and Receiverships (DRR), and the Legal Division to identify and investigate financial institution crime, especially various types of bank fraud. OIG investigative efforts are concentrated on those cases of most significance or potential impact to the FDIC and its programs. The goal, in part, is to bring a halt to the fraudulent conduct under investigation, protect the FDIC and other victims from further harm, and assist the FDIC in recovery of its losses. Pursuing appropriate criminal penalties not only serves to punish the offender but can also deter others from participating in similar crimes. 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 BSA/Anti-Money Laundering Section to address areas of concern, and we communicate regularly with the Department of Justice's Asset Forfeiture and Money Laundering Section. Our current inventory of BSA/anti-money laundering cases includes four cases.

The OIG's investigations of financial institution fraud historically constitute about 90 percent of the OIG's investigation caseload. The OIG is also committed to continuing its involvement in interagency forums addressing fraud. Such groups include national and regional bank fraud, check fraud, mortgage fraud, anti-phishing, and suspicious activity review working groups. Most recently, the OIG has expanded its involvement in several cyber security-related working groups, namely the National Cyber Investigative Joint Task Force and the Federal Bureau of Investigation's (FBI) Washington Field Office Cyber Task Force. Additionally, when possible, the OIG engages in industry and other professional outreach efforts to keep financial institutions and others informed of fraud-related issues and to educate them on the role of the OIG in combating financial institution fraud.

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

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

OIG Work in Support of Goal 1

In support of this overarching goal of helping ensure the safety and soundness of the nation's banks, we issued the results of a comprehensive review of the FDIC's role in a Department of Justice (DOJ) initiative known as Operation Choke Point and the FDIC's supervisory approach to institutions conducting business with merchants associated with high-risk activities. We also completed three material loss reviews during the period, including that of Doral Bank, San Juan, Puerto Rico, whose failure caused losses to the DIF estimated at \$698.4 million. As reported in our last semiannual report, we also continued activities related to our on-going risk assessment of the FDIC's activities related to implementation of the Dodd-Frank Act. The results of these efforts are described below.

Our office continued the legislatively mandated review of all failed FDIC-regulated institutions causing losses to the DIF of less than the threshold outlined in the Dodd-Frank Act to determine whether circumstances surrounding the failures would warrant further review. Our failed bank review activity is presented in Appendix II.

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

Ongoing Dodd-Frank Act Risk Assessment and Monitoring Effort

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

During the reporting period, we continued to observe the FDIC's Complex Financial Institutions Coordination Group meetings, monitored Dodd-Frank Act issues and media coverage, and briefed the FDIC Chairman and Vice Chairman to share our perspectives and hear their views on areas where the OIG can add the most value going forward. As part of our planning for FY 2016, we identified potential assignments related to the FDIC's living will reviews and pricing models for large banks.

In the coming weeks, we anticipate communicating to FDIC management periodic summaries of any issues or risks for management consideration and intend to begin more structured work in select areas.

The FDIC's Role in Operation Choke Point and Supervisory Approach to Institutions that Conducted Business with Merchants Associated with High-Risk Activities

In a letter dated October 23, 2014, thirty-five Members of Congress requested that the FDIC OIG investigate the involvement of the FDIC and its staff in the creation and/or execution of the DOJ initiative known as Operation Choke Point. In the letter, Members expressed concern that the FDIC was working with DOJ in connection with Operation Choke Point to pressure financial institutions to decline banking services to certain categories of lawfully operating merchants that had been associated with high-risk activities. The letter also indicated that it was the Members' belief that FDIC officials had abused their authority by advancing a political or moral agenda to force certain lawful businesses out of the financial services space.

On December 17, 2014, the FDIC Chairman requested that, as part of our planned and ongoing work in this area, we conduct a fact-finding review of the actions of one former and four current senior FDIC officials. The Chairman's request was prompted by concerns raised by a Congressman in a letter dated December 10, 2014 that stated the five officials had allowed their personal and political views to interfere with the important work of the FDIC and that the officials had misled the American people through their emails and in meetings with, and testimony before, the Congress.

We conducted an audit to (1) describe the FDIC's role in the DOJ initiative known as Operation Choke Point and (2) assess the FDIC's supervisory approach to financial institutions that conducted business with merchants associated with high-risk activities for consistency with relevant statutes and regulations. As part of the audit, we reviewed a non-statistical sample of 23 FDIC-supervised financial institutions to assess the FDIC's supervisory approach for addressing identified concerns. We also determined the extent to which the five referenced officials were involved with Operation Choke Point and whether their actions involving the institutions we reviewed were based on personal, political, or moral agendas aimed at forcing lawfully operating businesses out of the banking sector.

Separately, the OIG's Office of Investigations conducted work to determine whether one of the five individuals had misled the American people in testimony before the Congress.

Background: In November 2012, attorneys within DOJ's Civil Division proposed an internal initiative intended to protect consumers from fraud perpetrated by fraudulent merchants, financial institutions, and financial intermediaries known as third-party payment processors. The initiative, which DOJ named Operation Choke Point, focused on the relationship between third-party payment processors and financial institutions because these relationships were the means by which fraudulent merchants were able to access the banking system to commit consumer fraud. In carrying out its work in connection with Operation Choke Point, DOJ issued 60 administrative subpoenas from February 2013 through August 2013 to entities for which the Department determined it had evidence of potential consumer fraud. According to DOJ employees that we spoke with during the audit, 20 of the subpoenas were issued to FDIC-supervised financial institutions.

In August 2013, Members became concerned that the FDIC and DOJ were pressuring financial institutions and third-party payment processors to terminate business relationships with lawful lenders that provided short-term credit options to underserved consumers. Since that time, Members also expressed concern that financial institutions were declining basic banking services, such as deposit accounts and loans, to entire categories of merchants that had been associated with high-risk activities. Members asserted that the FDIC and DOJ were using a "high-risk list" of merchant categories that was published in an informational article contained in the FDIC's summer 2011 edition of the Supervisory Insights Journal, together with certain FDIC supervisory guidance, to target institutions for increased scrutiny.

The FDIC has defined higher-risk activities as those that have been understood by industry and financial regulators as being subject to complex or varying legal and regulatory environments (such as activities that may be legal only in certain states); being prohibited for certain consumers (such as minors); being subject to varying state and federal licensing and reporting regimes; or tending to display a higher incidence of consumer complaints, returns, or chargebacks. In the context of this audit, merchants associated with high-risk or higher-risk activities include (among others) payday lenders, pawnbrokers, firearms and ammunition manufacturers and retailers, and tobacco retailers.

Results: We reported that the FDIC's involvement in Operation Choke Point was limited to a few FDIC staff communicating with DOJ employees regarding aspects of the initiative's implementation. These communications with DOJ generally related to the Corporation's responsibility to understand and consider the implications of potential illegal activity involving FDIC-supervised financial institutions. Overall, we consider the FDIC's involvement in Operation Choke Point to have been inconsequential to the overall direction and outcome of the initiative.

We further determined that the FDIC's supervisory approach to financial institutions that conducted business with merchants on the high-risk list was within the Corporation's broad authorities granted under the FDI Act and other relevant statutes and regulations. However, the manner in which the supervisory approach was carried-out was not always consistent with the FDIC's written policy and guidance.

We found no evidence that the FDIC used the high-risk list to target financial institutions. However, references to specific merchant types in the summer 2011 edition of the FDIC's *Supervisory Insights* journal and in supervisory guidance created a perception among some bank executives that we spoke with that the FDIC discouraged institutions from conducting business with those merchants. This perception was most prevalent with respect to payday lenders.

With the exception of payday lenders, we found no instances among the financial institutions we reviewed where the FDIC pressured an institution to decline banking services to a merchant on the high-risk list. Further, bank executives that we spoke with indicated that, except for payday lenders, they had not experienced regulatory pressure to terminate an existing customer relationship with a merchant on the high-risk list, including a firearms, ammunition, or tobacco retailer. The FDIC has had concerns regarding payday lending by financial institutions that precede Operation Choke Point by many years. These concerns led to supervisory guidance and actions that caused FDIC-supervised institutions to stop offering payday loans.

Payday Lending and Related Activities: We found that a number of FDIC officials also had concerns about Automated Clearing House (ACH) payment processing by financial institutions for payday lenders. These concerns were based on the premise that such services facilitate payday lending. The heightened level of concern for payday lending by financial institutions and related ACH processing was reflected in the negative tenor of internal email communications among senior FDIC staff and others that we reviewed. In some cases, these communications involved instances in which FDIC personnel contacted institutions and used moral suasion to discourage them from adopting payday lending products or providing ACH processing for payday lenders. The FDIC does not have a formal definition of moral suasion in its policies. However, examiners commonly use moral suasion in an attempt to influence risk management practices at financial institutions before perceived problems rise to a level that necessitates an informal or formal enforcement action.

We noted two instances in which the FDIC discouraged institutions from providing ACH processing to payday lenders in written communications to the institutions. In both instances, the FDIC's principal stated concern was the reputation risk to the institutions due to their potential or existing relationship with a payday lender. The FDIC does not centrally track its written communications to financial institutions that involve ACH processing concerns. Accordingly, we were unable to determine how often such communications occur. However, our discussions with FDIC executives and our review of regional office status reports identified only three institutions where FDIC officials raised concerns regarding ACH processing practices for payday lenders.

Role of Certain FDIC Officials: We concluded that the five officials referenced above did not play a role in the development or implementation of Operation Choke Point. We also concluded that the individuals did not pursue their own personal, political, or moral agendas aimed at forcing lawfully operating businesses on the high-risk list out of the banking sector. As it pertains to payday lending and related activities, we concluded that the officials acted consistent with a widely-held understanding that the highest levels of the FDIC disfavored these types of banking services. We did, however, identify certain internal email communications and one written communication to an institution involving three of the five individuals that were not consistent with the FDIC's written policy and guidance pertaining to payday lending and related activities.

Refund Anticipation Loans: Our report includes an observation on the FDIC's supervisory approach to financial institutions that offered a credit product known as a refund anticipation loan (RAL). The FDIC considers RALs to carry a significant degree of risk to financial institutions, including third-party, reputation, compliance, and legal risks. Of particular concern to the FDIC is whether an institution can ensure proper underwriting and compliance with consumer protection requirements, particularly when RALs are brokered by large numbers of third-party tax return preparers (sometimes called electronic refund originators) in conjunction with the filing of a taxpayer's income tax return. Although RALs were not on the high-risk list, we observed that the FDIC's supervisory approach to institutions that offered this type of credit product involved circumstances that were similar to those that prompted the Congressional request to our office.

We identified three FDIC-supervised institutions that offered RALs. These institutions began offering RALs in 1987, 1988, and 2007, respectively. At various times from 2004 through 2009, FDIC examiners criticized the risk management practices pertaining to RALs at two of these institutions during compliance and risk management examinations. In late 2009 and early 2010, the FDIC sent letters to all three institutions expressing concerns about RALs and requesting that the institutions submit plans for discontinuing this type of lending. In early 2011, after efforts to convince these institutions to discontinue offering RALs were unsuccessful and supervisory concerns remained, the tenor of the FDIC's supervisory approach became aggressive. In one case, the FDIC took the highly unusual step of conducting a simultaneous, unannounced review of 250 electronic refund originators in 36 states involving hundreds of FDIC examiners in order to develop the evidence needed to compel the institution to stop offering RALs. In another case, a former FDIC supervisory attorney used a confrontational approach to pressure an institution's Board to terminate its RAL offerings. By April 2012, all three institutions had stopped offering RALs.

The FDIC drafted a policy statement in 2010 that defined the FDIC's supervisory concerns and expectations for institutions offering RALs. However, the policy statement was never finalized. In our view, establishing such a policy would have been prudent to ensure institutions understood the risks associated with RALs and provide transparent supervisory guidance and expectations for institutions already (or contemplating) offering RALs.

We concluded that the supervisory actions taken with respect to the three institutions that offered RALs fell within the Corporation's broad statutory authorities because the Corporation is permitted to require a financial institution to discontinue a practice if safety and soundness or consumer protection concerns warrant doing so. However, our report noted that the execution of these actions by FDIC management and staff warranted further review and the OIG is conducting additional work in this area. Further, in light of the concerns described in this report regarding the use of moral suasion with financial institutions, we pointed out that the FDIC should determine whether moral suasion is adequately defined in FDIC policy and guidance 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.

Recommendations: We made three recommendations to FDIC management to (1) review and clarify, as appropriate, existing policy and guidance pertaining to the provision and termination of banking services; (2) assess the effectiveness of the FDIC's supervisory policy and approach after a reasonable period of time is allowed for implementation; and (3) coordinate with the FDIC's Legal Division to review and clarify, as appropriate, supervisory policy and guidance to ensure that moral suasion is adequately addressed.

Management concurred with the report's recommendations and described planned and completed corrective actions that were responsive. Our report notes, however, that in reiterating our findings and providing perspective surrounding them, management did not discuss the potential impact that statements and actions by FDIC executives can have on those responsible for carrying out the FDIC's supervisory policies and approach. As described in our report, our interviews and review of documents showed that perceptions regarding the views of senior FDIC executives about institutions involved in payday lending and RALs influenced the supervisory approach to handling risks at those institutions. In several instances, the approach was not consistent with written FDIC policy and guidance.

Consequently, as it has committed to do, we believe it is prudent for FDIC senior leadership to reiterate its revised policies on a sustained basis to ensure they become engrained in the organization's supervisory culture. Given the significance of these issues, we will, at an appropriate time, follow up on the FDIC's actions to ensure they address the underlying concerns that support our recommendations.

Results of Investigative Inquiry Regarding FDIC Deputy General Counsel

Based on concerns expressed by the Congress and a letter from the FDIC Chairman, dated December 17, 2014, the OIG conducted an extensive criminal inquiry into whether Deputy General Counsel, Richard J. Osterman, knowingly or willfully provided materially false, fictitious or fraudulent testimony to the Congress, specifically to the Committee on Financial Services, U.S. House of Representatives on April 8, 2014, or to the House Financial Services Subcommittee on Oversight and Investigations on July 15, 2014. On those dates, Mr. Osterman testified in his then-capacity as Acting General Counsel of the FDIC on certain matters related to Operation Choke Point.

The OIG concluded that Mr. Osterman did not develop knowledge in conflict with his testimonies either contemporaneous with events or during his preparation to testify before the Congress on the occasions referenced above. Therefore, the OIG concluded that Mr. Osterman did not knowingly or willfully provide the Congress with materially false, fictitious or fraudulent testimony.

Doral Bank Material Loss Review

The Office of the Commissioner of Financial Institutions of Puerto Rico (OCFIPR) closed Doral Bank (Doral), San Juan, Puerto Rico, on February 27, 2015, and named the FDIC receiver. On March 6, 2015, the FDIC notified the OIG that total assets at closing were \$5.6 billion and that the loss to the DIF was \$748.9 million. As of July 31, 2015, the estimated loss had decreased to \$698.4 million. We conducted a material loss review, the scope of which covered examinations performed and supervisory actions taken from 2005 until Doral failed in 2015.

Doral was originally established as a mutually owned federal savings bank in 1981. In September 1993, the bank was acquired and recapitalized by the Doral Financial Corporation (DFC), a financial holding company. In October 1997, the bank switched its charter from a federal savings bank to become a state non-member bank regulated by the FDIC. The conversion was part of DFC's strategy to increase the size and market share of Doral. Through its other subsidiaries, DFC also engaged in the origination, sale, and servicing of mortgage loans. At the time of the charter conversion, the bank had assets of \$340 million and primarily originated and retained single-family mortgages. Doral's total assets increased significantly, peaking at \$11.2 billion in December 2004. Although the bank continued to focus on residential mortgage lending, its commercial real estate loan portfolio grew during this period.

In April 2005, DFC announced the need to restate its financial statements for the years 2000 through 2004 due to irregularities in its mortgage business. Although the restatement had only a minor impact on Doral, DFC's financial condition was weakened considerably, and the FDIC no longer considered DFC a source of strength for Doral. A number of significant management changes took place at DFC and the bank in 2006 due, in part, to concerns related to the restatement. Also during 2006, DFC entered into a consolidated agreement with the Secretary of the Department of Treasury of Puerto Rico (also referred to as the Hacienda) to address the overpayment of income taxes during the restatement period. The result of this and prior agreements was the creation of a deferred tax asset on various DFC entities' financial statements. Notably, the 2006 agreement became the basis of a new agreement made between the DFC and the Hacienda in 2012. As discussed later, issues surrounding the regulatory treatment of the later agreement emerged as factors impacting Doral's capital position in the period 2012 to 2014. In 2007, to strengthen the holding company's financial position, DFC's new executive leadership led efforts to raise \$610 million in capital, which resulted in the significant recapitalization of the holding company.

Like other insured depository institutions operating in Puerto Rico, Doral relied heavily on wholesale funding, and the business activities and credit exposure of both DFC and Doral were concentrated in Puerto Rico. Accordingly, significant to understanding the history of Doral is to understand economic conditions in Puerto Rico over the past decade.

Puerto Rico's current recession started in 2006, nearly 2 years before the U.S. downturn and has continued well past the official end of the U.S. recession. Further, the government is in the midst of a prolonged fiscal crisis. The economic conditions in Puerto Rico had a severe impact on Doral's loan portfolio.

Cause of Failure: Poor asset quality was the underlying cause of Doral's failure. Puerto Rico's severe and prolonged economic decline coupled with weak underwriting and risk management practices were significant factors in the deterioration of Doral's loan portfolio. Management's strategies for handling its troubled loan portfolio were based on overly optimistic assumptions in light of actual economic conditions and proved to be ineffective over time. In addition, Doral's flawed allowance for loan and lease losses methodology masked the extent of deterioration in its loan portfolio. Further, the Board's oversight of management was inadequate, given the bank's size, financial condition, and challenges.

Negative earnings resulting from losses associated with the loan portfolio progressively eroded capital. Doral's holding company served as a source of strength for a period of time, but the amount and quality of DFC's capital proved to be insufficient. In addition, in 2014, the FDIC determined that the \$286 million in prepaid tax assets on Doral's books, much of which had been down-streamed by DFC to the bank, should not have been included in regulatory capital until collected by the bank from the Hacienda. As a result, the bank did not comply with capital requirements under an existing formal enforcement action with the FDIC. Further, Doral was no longer statutorily able to enhance liquidity by accepting, renewing, or rolling over any brokered deposits. Because Doral was not in a sound financial condition to continue operations, OCFIPR closed Doral and appointed the FDIC as receiver on February 27, 2015.

The FDIC's Supervision of Doral: Between 2005 and 2014, the FDIC and OCFIPR conducted joint safety and soundness examinations of Doral, and the FDIC performed limited scope reviews in 2011 and 2014. As Doral's condition deteriorated, the FDIC and OCFIPR issued a number of progressively stronger supervisory actions. Following the 2011 examination, RMS officials placed Doral on a targeted examination schedule. Additionally, beginning in 2006, the FDIC's New York Regional Office recognized the need to closely monitor economic and banking conditions in Puerto Rico, leading to the development of an annual supervisory strategy. The analysis of economic data and annual risk profile and trends informed institution-specific supervisory strategies, including one for Doral.

Our report raised no concerns with the FDIC's overall level of supervisory attention given to Doral or the supervisory strategy. However, we had to consult with FDIC officials to determine whether the FDIC complied with FDI Act examination frequency requirements when Doral was placed on a targeted examination schedule, which provides for a more continuous onsite presence. Guidance related to RMS' large state nonmember onsite supervision program that describes continuous examination methodologies (i.e., visitations and limited scope reviews conducted throughout the year) does not address dates to be used for purposes of monitoring the FDI Act examination frequency requirements. *The Risk Management Manual of Examination Policies* explicitly states that because limited scope examinations or visitations are not full scope examinations, those do not satisfy the examination frequency requirements. Clarifying guidance on how using a targeted examination schedule impacts compliance with examination frequency requirements would help ensure consistency in this supervisory approach.

Generally, the FDIC's assessment of Doral's condition and assignment of component and composite ratings was consistent with supervisory guidance and reflected the increasing deterioration in the loan portfolio, deficient earnings, and the threat to capital. For example, asset quality and earnings were progressively downgraded beginning in 2007. Further, management ratings assigned in 2005 through 2009 appropriately reflected management's (1) lack of responsibility for the high-risk lending strategy undertaken before 2005 and economic conditions in Puerto Rico; (2) responsiveness to supervisory concerns at that time; and (3) ability to successfully raise capital.

That said, with the benefit of hindsight, downgrading the management component rating in 2009, further downgrading the management rating and the composite rating in 2010, and imposing stronger enforcement actions following both examinations may have been prudent. In these examinations, we believe greater skepticism of management's capability to develop and implement effective plans to address the significant deterioration in Doral's loan portfolio and deficient earnings may have been warranted. We recognize that doing so may not have changed the eventual outcome. However, given Doral's overall risk profile, such actions, particularly in 2010, would have been more consistent with the FDIC's forward-looking approach that was being emphasized at the time and the forward-looking supervision program adopted in 2011 that focuses on risks when assigning ratings. Additionally, such actions may have garnered needed Board attention at a critical time in Doral's history.

Further, the FDIC could have been more critical and proactive in its evaluation of the regulatory capital treatment of the Hacienda tax asset in 2012, when the FDIC first became aware of DFC's plans to down-stream the asset to Doral to serve as regulatory capital. We determined Doral would likely have been *Undercapitalized* a few months earlier assuming that Doral would not have taken any different actions that impacted capital. More significantly perhaps, had the FDIC determined the asset was not eligible for regulatory capital in 2012, Doral may have accelerated its capital-raising efforts. FDIC officials did coordinate with Federal Reserve counterparts and OCFIPR on the matter, but RMS lacks a formal process for escalating complex and/or unique accounting topics internally to ensure such matters are vetted by the appropriate subject matter experts within the division. With respect to Prompt Corrective Action, based on the supervisory actions taken, the FDIC properly implemented applicable Prompt Corrective Action provisions of section 38 in a timely manner.

We made two recommendations in the report. The first was intended to enhance the effectiveness of supervisory controls for ensuring the FDIC's compliance with the FDI Act examination frequency requirements when a bank is on a targeted examination schedule. The second recommendation involved issuing or revising policy guidance to document the requirements and responsibilities of Regional Accountants related to conducting analysis for complex and/or unique accounting transactions, including when such matters should be escalated within RMS. FDIC management concurred and its proposed actions are responsive to the recommendations.

Capitol City Bank Material Loss Review

On February 13, 2015, the Georgia Department of Banking and Finance (DBF) closed Capitol City Bank & Trust Company, Atlanta, Georgia (CCB), and the FDIC was appointed receiver. The FDIC's Division of Finance notified the FDIC's OIG on March 6, 2015, that the estimated loss to the DIF for the failure was \$88.9 million. We engaged KPMG LLP to conduct a material loss review of CCB.

CCB was a state nonmember minority depository institution (MDI) that was chartered and became insured in 1994. Its Board of Directors (Board) and management historically pursued a traditional community banking model focused on serving the African American community in the Atlanta, Georgia, metropolitan area. CCB was wholly owned by Capitol City Bancshares, Inc., a one-bank holding company. In the years leading up to the bank's failure, the holding company had a minimal amount of liquidity and was highly leveraged and, as a result, could no longer provide financial support to CCB.

MDIs often promote the economic viability of minority and under-served communities. The FDIC has long recognized the importance of MDIs and has historically taken steps to preserve and encourage minority ownership of insured financial institutions. The FDIC also recognizes that MDIs face many challenges, including the need to compete with larger financial institutions for both business and a talented work force. Additionally, it may be difficult for MDIs to diversify their geographical and credit risk exposure due to their commitment to serve local communities and ethnic populations.

CCB played a unique role in promoting the economic viability of minority and under-served communities, particularly the African American communities in the metropolitan Atlanta area and in Albany, Georgia; Augusta, Georgia; and Savannah, Georgia. All of CCB's offices, which consisted of seven branches and a main office, were also located in or near a low- or moderate-income census tract. CCB's assets were centered in its loan portfolio, which had large concentrations of commercial real estate (CRE) loans, including loans to church and religious organizations.

Cause of Failure: We determined that CCB failed primarily because its Board and management did not properly manage the risks associated with the bank's growth strategy that was centered on higher-risk CRE loans, which included acquisition, development, and construction, church and religious organizations, and gas and convenience store loans. Specifically, CCB's Board and management did not establish appropriate risk management practices, such as applying prudent credit underwriting and administration practices, ensuring adequate internal controls were in place, and maintaining key personnel and proper staffing levels as the bank grew. The president and chief executive officer (CEO) served as a dominant official, exerting significant authority over the lending function as well as the Board. Under the leadership of the CEO, the bank significantly increased its CRE portfolio and did not adequately respond to examiners' repeat recommendations to improve the bank's overall condition, particularly in the lending area.

Deficient loan underwriting and credit administration practices, such as over-reliance on collateral, lack of borrower financial information, and continued loan renewals negatively impacted the CRE loan portfolio. Additionally, the bank's appraisal practices were less than ideal since the bank did not often obtain updated appraisals, and the bank's appraisal reviews did not identify concerns noted by examiners.

Such practices resulted in inaccurate calculations of the Allowance for Loan and Lease Losses and had the effect of delaying the timely recognition of loan exposure and losses as well as overstating earnings and capital. As a result, when economic and real estate market conditions deteriorated during the financial crisis, beginning in late 2007, CCB's loan portfolio was heavily impacted.

The FDIC's Supervision of CCB: Our report noted that the FDIC, in coordination with the Georgia Department of Banking and Finance, provided ongoing supervisory oversight of CCB through regular on-site examinations, visitations, and various offsite monitoring. In addition, the FDIC provided technical assistance to the bank in certain areas, consistent with the requirements of the FDIC's MDI Program. Through its supervisory efforts, the FDIC identified risks in the bank's operations as early as 2005 and brought these risks to the attention of the institution's Board and management through examination reports and visitation documentation, correspondence, and informal and formal enforcement actions. Such risks included the presence of a high-risk loan portfolio in an operating environment that lacked key controls and risk management practices, particularly in the lending area.

The FDIC and the Georgia Department of Banking and Finance generally provided supervision in accordance with examination policies and guidelines. In retrospect, however, an elevated level of supervisory scrutiny and/or stronger enforcement action may have been warranted to emphasize the inherent risk and exposure that resulted from the bank's growth strategy and, in later years, management's inability to fully address weaknesses and recommendations or comply with supervisory enforcement actions.

With respect to Prompt Corrective Action, the FDIC properly implemented the applicable provisions of section 38.

We made no recommendations in this report.

Valley Bank Material Loss Review

On June 20, 2014, the Illinois Department of Financial and Professional Regulation closed Valley Bank, Moline, Illinois (VBI), and the FDIC was appointed receiver. The FDIC's Division of Finance notified the FDIC OIG on July 9, 2014 that the estimated loss to the DIF was \$51.4 million. We engaged KPMG LLP to conduct a material loss review.

VBI was a state-chartered nonmember bank that was established on January 31, 2002 when the State Bank of Latham, Latham, Illinois, merged with the Valley State Bank, Eldridge, Iowa. The combined institution adopted a new name—Valley Bank. VBI's assets were centered in its loan portfolio, which contained significant concentrations of CRE loans, including acquisition, development, and construction loans. In the years preceding its failure, VBI also developed a considerable exposure to troubled businesses in the media sector, including television and broadcast operations. In addition, the bank maintained an investment portfolio consisting of mortgage-backed securities, collateralized mortgage obligations, municipal securities, and other investments. At the time of its failure, VBI maintained 15 offices, all of which were located in Iowa, except for the bank's main office, which was located in Moline, Illinois.

VBI was wholly-owned by River Valley Bancorp, Inc. (River Valley), a multi-bank holding company located in Davenport, Iowa. River Valley also owned substantially all of the outstanding stock of Valley Bank, Fort Lauderdale, Florida (VBF). VBI's chairman of the board of directors (Board) and president and CEO also served as the president, CEO, and board chairman of River Valley as well as the president, CEO, and vice chairman of Valley Bank, Fort Lauderdale, Florida's Board. This individual, who we refer to herein as the CEO, exercised significant control over the strategic and operational direction of the entire River Valley organization.

Cause of Failure: VBI failed primarily because of lax oversight by its Board and a dominant CEO that implemented a risky business strategy. Under the leadership of the CEO, VBI pursued an aggressive growth strategy centered in CRE loans, including speculative acquisition, development, and construction loans that made the bank vulnerable to a sustained downturn in the real estate market. In 2008, after deterioration in VBI's CRE portfolio had been identified, the bank acquired a failing thrift institution that had a considerable amount of distressed CRE loans. Adding to VBI's exposure to the real estate market was a significant investment in Private Label Mortgage Backed Securities that the bank acquired without conducting a proper pre-purchase analysis. Although these securities had an investment grade at the time of their purchase, they had risky characteristics and lost significant value when the real estate market deteriorated.

As losses associated with VBI's CRE and acquisition, development, and construction loans and Private Label Mortgage Backed Securities increased, VBI's CEO made a number of poor business decisions in an attempt to return the bank to profitability. For example, the CEO continued to extend credit to certain business customers after they were unable to repay their existing obligations, which had the effect of masking the true financial condition of VBI's loan portfolio, and ultimately increased the losses incurred by the bank. Weak internal controls, particularly in the lending function, also contributed to VBI's problems. Specifically, examiners identified numerous errors in VBI's financial books and records, inappropriate insider transactions, conflicts of interest involving certain directors and officers, and repeat apparent violations of laws and regulations and contraventions of policy. Notably, VBI's Board did not effectively challenge the CEO regarding the bank's risky business strategy and lending practices or hold the CEO accountable for the bank's weak internal controls and unsatisfactory financial performance.

Between 2010 and the first quarter of 2014, VBI reported combined net losses of approximately \$51.3 million and provision expenses for loan and lease losses of approximately \$70.4 million. These losses and provision expenses eliminated the bank's earnings and impaired its capital. The Illinois Department of Financial and Professional Regulation closed VBI on June 20, 2014 because the bank did not have sufficient capital to continue safe and sound operations and had no viable means of raising additional capital.

The FDIC's Supervision of VBI: The FDIC, in coordination with the Illinois Department of Financial and Professional Regulation, provided ongoing supervisory oversight through regular on-site examinations, visitations, and targeted reviews. Through its supervisory efforts, the FDIC identified risks in the bank's operations and brought these risks to the attention of the institution's Board and management through examination reports and visitation documentation, correspondence, and informal and formal enforcement actions. Such risks included the Board and management's high tolerance for risk, the dominance of the CEO, VBI's significant exposure to CRE and acquisition, development, and construction loans, and the bank's weak internal controls, poor lending practices, and deteriorating financial condition. We note that the FDIC has the authority to review the business activities of failed financial institutions, including the activities of bank officials, for possible regulatory action.

The CEO served in positions of high trust and responsibility at VBI and its affiliates despite having a criminal conviction and a troubled career history. As detailed in the report, such service violated section 19 of the FDI Act, which prohibits individuals convicted of certain criminal offenses from participating in the affairs of an insured depository institution without the prior written consent of the FDIC. Although the FDIC had a process in place to mitigate the risk of individuals serving in violation of section 19, the process was not effective in identifying instances of section 19 violations at VBI and its affiliates, resulting in an increased risk to the safety and soundness of the banks. In addition, the FDIC evaluated and favorably resolved two notices required by section 32 of the FDI Act that permitted the CEO to expand his role and authority within the River Valley organization. However, it did not appear that the FDIC's documentation and analysis regarding these notices was sufficient to support the favorable resolutions. Further, in one instance, the FDIC did not pursue obtaining a notice required by section 32 for the CEO's expanded role at Valley Bank, Fort Lauderdale, Florida.

We noted that the FDIC should have taken stronger supervisory action at the February 2011 and April 2012 examinations when it was apparent that prior supervisory efforts to address the CEO's risky business decisions and the bank's deteriorating financial condition were unsuccessful. Such an approach may have instilled urgency in VBI's Board to address management's poor performance, mitigating the losses incurred by the bank and, to some extent, the DIF.

With respect to Prompt Corrective Action, KPMG LLP determined that the FDIC implemented supervisory actions that were generally consistent with relevant provisions of section 38.

We made three recommendations that were intended to enhance the effectiveness of the FDIC's supervisory controls for ensuring bank compliance with the prohibitions of section 19, addressing risks associated with dominant bank officials, and ensuring information pertaining to key supervisory decisions is recorded in systems of record. Management concurred with those recommendations and described responsive actions.

OIG Investigations Address Financial Institution Fraud

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

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

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

Former United Commercial Bank Chief Operating Officer and Chief Credit Officer Sentenced to 97 Months in Prison

On September 1, 2015, the former chief operating officer and chief credit officer of United Commercial Bank (UCB)/UCB Holdings, Inc., was sentenced to serve 97 months in prison for his role in a securities fraud scheme and other corporate fraud offenses stemming from the failure of UCB, San Francisco, California. Restitution will be determined at a later date. The sentencing brings to a close one of the most significant prosecutions to arise out of the 2008 financial crisis.

According to evidence presented at trial, the former bank executive conspired with others and deceived UCB's auditors by manipulating the bank's books and records in a manner that misrepresented and concealed the bank's true financial condition and performance and caused the bank to issue materially false and misleading financial statements for the third quarter of 2008 (10Q and Call Report), year-end 2008 (10K and Call Report), and first quarter of 2009 (Call Report). He 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, the former chief operating officer and chief credit officer knew the loan loss allowance package, along with the quarterly call reports, 10Q(s), and 10K(s), for the third quarter 2008 and the year end 2008 were false and misleading.

Other former officers were involved in falsifying bank records. On December 9, 2014, UCB's chief financial officer, pleaded guilty to one count of conspiracy to make a materially false and misleading statement to an accountant. On October 7, 2014, the bank's senior vice president pleaded guilty to charges of conspiracy to commit false bank entries, reports, and transactions related to his preparation of false and misleading reports. Both former officers await sentencing.

Source: *In May 2009, UCB Holdings, Inc., 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 of Directors reported the results of the internal investigation to DOJ.*

Responsible Agencies: *This is a joint investigation by the FDIC OIG, FBI, FRB and the Consumer Financial Protection Bureau OIG, and Special Inspector General for the Troubled Asset Relief Program (SIGTARP). The case is being prosecuted by the United States Attorney's Office for the Northern District of California.*

Bank of Mingo, Williamson, West Virginia, Charged with Violating the Bank Secrecy Act

Beginning in at least the early 2000s, two individuals operated a series of employee-leasing companies that provided contract labor to coal mines and coal-mining related operations in southern West Virginia. They both maintained business accounts at Bank of Mingo. From at least 2005 through approximately April 2012, both of the men, each in his own respect and through various employees or others, routinely withdrew cash from a line of credit established at Bank of Mingo to make payroll. The withdrawals consisted of separate transactions, in amounts less than \$10,000, for the purpose of avoiding the Bank of Mingo's currency transaction report (CTR) filing requirement. In June 2005, as required by the BSA/Anti-Money Laundering Program, the Williamson branch manager of Bank of Mingo conducted a "Know Your Customer" investigation to ascertain the individuals' intended purpose for this banking pattern. At that meeting, the two claimed that the reason they orchestrated the cash withdrawals was because their mine service business had crews working in several different geographical areas. Each of the withdrawals was intended for a different crew and the fact that all of the amounts were less than \$10,000 was coincidental. Further, the two men claimed that all of the cash payments were documented in a payment log and provided to their accountant at the end of the year so the appropriate tax forms could be prepared. The Williamson Branch Manager accepted this explanation and conducted no further investigation to corroborate the statements made by the two men, and their conduct continued without interruption.

By November 2007, the two men had formed Aracoma Contracting, LLC (Aracoma) as part of the employee leasing business. They placed Aracoma in the name of a nominee owner. The Bank of Mingo failed to obtain sufficient information to determine if Aracoma was placed in the name of a nominee or, more importantly, the reason for doing so. Once the two men formed Aracoma, the Williamson branch manager approved a \$50,000 line of credit, which was used by both men for payroll. The men were told by the Williamson branch manager to prepare the line of credit "request for advance" for each of the anticipated cash withdrawals for that day identifying which Aracoma employee would make that particular withdrawal and the amount. Further, the Williamson branch manager instructed the men to prepare a "cash denomination sheet" to be submitted with each request for advance so the tellers could pre-count the cash. An Aracoma employee would transmit, via facsimile to the Williamson Branch, the line of credit requests for advance and corresponding cash denomination sheets. Either the Williamson branch manager or the assistant branch manager would approve the requests for advance. Then, a teller would prepare a cashier's check in the name of the identified Aracoma employee, along with the pre-counted cash. Later, the Aracoma employees, sometimes together, would arrive at the Williamson Branch. The employees would then endorse the cashiers' checks and receive the pre-counted cash.

Aracoma employees were not required to deposit the cashier's check into an Aracoma checking account and then make the withdrawal from that account. In order to track branch banking cash activities, the bank maintained at each branch a "cash log" for all cash transactions during the day over the amount of \$3,000. The teller would enter in the cash log the name of the employee withdrawing the cash and the Bank of Mingo account on which the cashier's check was drawn. By conducting the cash withdrawal transactions in this manner, there was nothing on the cash log to indicate more than \$10,000 had been drawn from the line of credit on the same banking day. The cash log was reviewed the following day by the BSA officer to determine what, if any, CTRs should be filed.

As a matter of general practice, the BSA officer reviewed the cash log and did not file a CTR because the cash log entries only referenced the individual Aracoma employee. However, as clearly stated in the Bank of Mingo BSA/Anti-Money Laundering Program, the BSA officer should have aggregated the separate Aracoma banking activities under one account, but did not do so. As a result of this failure, Bank of Mingo did not file CTRs on the cash withdrawals.

On June 15, 2015, the U.S. Attorney's Office announced the filing of an information against the Bank of Mingo. The bank was charged with violating the BSA from January 2009 through April 2012 by failing to develop, implement, and maintain an effective anti-money laundering program.

Bank of Mingo admitted that from January 2009 through April 2012, it should have filed CTRs and suspicious activity reports related to cash withdrawals from the line of credit involving at least \$2.2 million. Bank of Mingo admits that its failure to file CTRs was not only in breach of its own BSA/Anti-Money Laundering Program, but also a violation of the BSA and the regulations promulgated under that Act. Bank of Mingo acknowledged that it was legally responsible for the Williamson branch manager's willful failure to file CTRs related to Aracoma. Finally, Bank of Mingo admitted that had it complied with its obligations under the BSA, and the regulations prescribed under it by the Secretary for the Department of Treasury, CTRs and suspicious activity reports would have been filed on the Aracoma structuring activity. For its part, Aracoma pleaded guilty to conspiring to structure currency transactions.

The United States Attorney also filed a motion with the District Court requesting that all proceedings in the case, including trial, be deferred for a period of 12 months from the filing of the information. As stated in the motion, the U.S. Attorney and Bank of Mingo have signed an agreement, which includes a "Stipulation of Facts" wherein the bank admits the conduct with which it is charged. The deferment will allow the bank to demonstrate its acceptance of responsibility and to take remedial measures to correct its past, wrongful conduct. The bank agreed to cooperate with the United States and to forfeit \$2.2 million.

***Source:** The FBI and the U.S. Attorney's Office for the Southern District of West Virginia.*

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

Multiple Actions in Case Involving Fraud at Park Avenue Bank, New York, New York

A Kentucky businessman controlled numerous entities located throughout the United States. As such, he controlled the companies and their finances, using them to orchestrate a \$53 million fraud on the Internal Revenue Service (IRS) as well as other illegal schemes. However, rather than exercise control of these companies openly, he concealed his control by installing other individuals to oversee the companies' day-to-day functions and to serve as the companies' titular owners, directors, or officers. He also maintained a corrupt relationship with Park Avenue Bank and two of its executives, the president and CEO, and the senior vice president.

Tax Crimes: From 2008 to 2010, the businessman controlled O2HR, a professional employer organization located in Tampa, Florida. Like other such companies, O2HR was paid to manage the payroll, tax, and workers' compensation insurance obligations of its client companies. However, instead of paying \$53 million in taxes that O2HR's clients owed the IRS, and instead of paying \$5 million to Providence Property and Casualty Insurance Company (Providence P&C) – an Oklahoma-based insurance company – for workers' compensation coverage expenses for O2HR clients, the businessman stole the money that his client companies had paid O2HR for those purposes. Among other things, he diverted millions of dollars from O2HR to fund his investments in unrelated business ventures, and to pay his family members' personal expenses. The expenses included mortgages on his homes, rent payments for his children's apartments, staff and equipment for his farm, designer clothing, jewelry, and luxury cars.

Conspiracy to Commit Bank Bribery, Defraud Bank Regulators, and Fraudulently Purchase an Oklahoma Insurance Company: From 2007 up to and including 2010, the businessman engaged in a massive multi-faceted conspiracy, in which he schemed to (i) bribe executives of Park Avenue Bank, (ii) defraud bank regulators and the board and shareholders of a publicly-traded company and (iii) fraudulently purchase an Oklahoma insurance company. As described in more detail below, he paid bribes totaling hundreds of thousands of dollars in cash and other items to the senior vice president and president and CEO, in exchange for their favorable treatment at Park Avenue Bank.

As part of the corrupt relationship between the businessman and the bank executives, the three and others conspired to defraud various entities and regulators during the relevant time period. Specifically, the three conspired to falsely bolster Park Avenue Bank's capital by orchestrating a series of fraudulent transactions to make it appear that Park Avenue Bank had received an outside infusion of \$6.5 million and engaged in a series of further fraudulent actions to conceal from bank regulators the true source of the funds.

The three and others also conspired to defraud Oklahoma insurance regulators and others by making material misrepresentations and omissions regarding the source of \$37.5 million used to purchase Providence P&C, an Oklahoma insurance company that provided workers' compensation insurance for O2HR's clients, and to whom O2HR owed a significant debt.

Bribery of Park Avenue Bank Executives: From 2007 to 2009, the businessman paid the two bank executives at least \$400,000 in exchange for which they: (1) provided him with fraudulent letters of credit obligating Park Avenue Bank to pay an investor in one of his businesses \$1.75 million if he failed to pay the investor back himself; (2) allowed the businessman's controlled entities to accrue \$9 million in overdrafts; (3) facilitated intra-bank transfers in furtherance of the businessman's frauds; and (4) fraudulently caused Park Avenue Bank to issue at least \$4.5 million in loans to the businessman's controlled entities.

Fraud on Bank Regulators and a Publicly-Traded Company: From 2008 to 2009, the three co-conspirators engaged in a scheme to prevent Park Avenue Bank from being designated as “undercapitalized” by regulators – a designation that would prohibit the bank from engaging in certain types of banking transactions, and that would subject the bank to a range of potential enforcement actions by regulators. Specifically, they engaged in a series of deceptive, “round-trip” financial transactions to make it appear that the former president and CEO had infused the bank with \$6.5 million in new capital when, in actuality, the \$6.5 million was part of the bank’s pre-existing capital. The three men funneled the \$6.5 million from the bank through accounts controlled by the businessman to the former president and CEO. This was done to make it appear as though the former president and CEO was helping to stabilize the bank’s capitalization problem, so the bank could continue engaging in certain banking transactions that it would otherwise have been prohibited from doing, and to put the bank in a better posture to receive \$11 million from the Troubled Asset Relief Program.

To conceal their unlawful financial maneuvering, the businessman created, or directed the creation of, documents falsely suggesting that the former president and CEO had earned the \$6.5 million through a bogus transaction involving another company that the former president and CEO owned. The three men further concealed their scheme by stealing \$2.3 million from General Employment Enterprises, Inc., a publicly-traded temporary staffing company, in order to pay Park Avenue Bank back for monies used in connection with the \$6.5 million transaction.

Fraud on Insurance Regulators and the Investment Firm: From July 2008 to November 2009, the three men and an executive at an investment bank and financial services company headquartered in New York, New York, conspired to (i) defraud Oklahoma insurance regulators into allowing the former president and CEO to purchase the assets of Providence P&C – the Oklahoma insurance company that was owed \$5 million by O2HR and (ii) defraud the Investment firm into providing a \$30 million loan to finance the purchase.

Specifically, the businessman and the former president and CEO devised a scheme in which the latter would purchase Providence P&C’s assets by obtaining a \$30 million loan from the investment firm, which used Providence P&C’s own assets as collateral for the loan. However, because Oklahoma insurance regulators had to approve any sale of Providence P&C, and because Oklahoma law forbade the use of Providence P&C’s assets as collateral for such a loan, the four co-conspirators made, and conspired to make, a number of material misstatements and material omissions to the investment firm and Oklahoma insurance regulators concerning the true nature of the financing for the former president and CEO’s purchase of Providence P&C.

Among other things, the investment advisor directed the former president and CEO to sign a letter that provided false information regarding the collateral that would be used for the loan, and the businessman and two former bank executives conspired to falsely represent to Oklahoma insurance regulators that Park Avenue Bank – not the investment firm – was funding the purchase of Providence P&C. After deceiving Oklahoma regulators into approving the sale of Providence P&C, the businessman took \$4 million dollars of the company’s assets, which he used to continue the scheme to defraud O2HR’s clients. Ultimately, in November 2009, the insurance company became insolvent and was placed in receivership after the businessman and two former bank executives had pilfered its remaining assets.

Chronology of Actions

On March 15, 2010, the former president and CEO was arrested based on a criminal complaint; the complaint alleged that he was involved in bank fraud, mail fraud, and false statements while at Park Avenue Bank.

On September 27, 2012, a 13-count sealed indictment was filed in the Southern District of New York against the investment advisor, the former vice president of Park Avenue Bank, and the businessman—the ring leader of the entire fraud. The charges included wire fraud, tax evasion, fraud on bank regulators, and conspiracy to commit wire fraud, bank fraud, bank bribery, and fraud on bank regulators.

On June 5, 2015, the businessman was sentenced to serve 12 years in prison to be followed by 3 years of supervised release. He was also ordered to forfeit \$10.8 million to the United States and pay a total of more than \$108 million in restitution.

On July 15, 2015, the investment advisor was sentenced in the Southern District of New York to 21 months in prison followed by 2 years of supervised release. He was also ordered to forfeit \$200,000 to the United States and pay a total of more than \$10 million in restitution.

On August 19, 2015, the former senior vice president was sentenced to one year in prison followed by 2 years of supervised release. He was also ordered to forfeit \$5 million to the United States and pay a total of \$49 million in restitution.

On August 20, 2015, the former president and CEO was sentenced in the Southern District of New York to 30 months in prison followed by 2 years of supervised release. He was also ordered to forfeit \$11 million to the United States and pay a total of \$54 million in restitution.

Source: FDIC RMS.

Responsible Agencies: This is a joint investigation by the FDIC OIG, FBI, SIGTARP, Department of Homeland Security Investigations, New York State Department of Financial Services, and IRS-CI. The case is being prosecuted by the U.S. Attorney’s Office for the Southern District of New York’s Complex Frauds and Cybercrime Unit.

Former Developer Sentenced to 18 Years in Prison

On June 25, 2015, a developer who was a co-conspirator in a complex scheme was sentenced to serve 18 years in prison to be followed by 3 years of supervised release and was ordered to pay \$18,384,584 in restitution. On October 17, 2013, he had been found guilty on 13 counts of bank fraud, conspiracy, misapplication of bank funds, wire fraud, and money laundering for his role in a lot loan/builder bailout fraud scheme, which fraudulently obtained loans from banks, including the Bank of Asheville, Asheville, North Carolina, and Pisgah Community Bank, Asheville, North Carolina, to fund the ailing Seven Falls Golf and River Club Development (Seven Falls) in Hendersonville, North Carolina.

As reported in earlier semiannual reports, Seven Falls was a proposed residential development that the developer owned in Henderson County, North Carolina. He purchased the property in 2006 with a \$25 million loan from the National Bank of South Carolina and, after selling approximately 70 lots in 2007 for an average price of \$450,000, he began running out of money and needed a new source of funds. The developer had numerous outstanding loans from the Bank of Asheville and he was near his statutory lending limit with both banks. He, along with co-conspirators, developed the Lot Loan Program whereby they recruited straw borrowers to purchase lots, with funding from both the Bank of Asheville and Pisgah Community Bank, the proceeds of which were turned over to the conspirators. The aggregate fraud significantly contributed to the failure of the Bank of Asheville on January 21, 2011, and the failure of Pisgah Community Bank on May 10, 2013.

Source: This investigation was initiated based on information provided by RMS and the North Carolina Commissioner of Banks.

Responsible Agencies: This is a joint investigation by the FDIC OIG, FBI, and IRS-CI. The case is being prosecuted by the U.S. Attorney's Office for the Western District of North Carolina.

La Jolla Bank Manager Conspired with Senior Bank Officials to Issue Hundreds of Millions of Dollars in Bad Loans

On September 25, 2015, a former bank manager was charged and pleaded guilty to conspiracy to misapply bank funds while managing the Small Business Administration (SBA) lending department at La Jolla Bank, La Jolla, California, from 2005 until 2009. She is scheduled to be sentenced on November 30, 2015.

According to the Information, in 2005, La Jolla Bank opened its SBA department under the direction of the former manager. She did not have authority to lend bank funds, but instead reviewed borrowers' applications and recommended that loans be approved and funds disbursed. The former manager required approval from either La Jolla Bank's CEO or the chief credit officer before funds were disbursed. The CEO, chief credit officer, and other bank employees offered favorable terms and treatment to certain high-volume borrowers they referred to as "Friends of the Bank." The CEO and chief credit officer encouraged the former bank manager to offer the same favorable terms and treatment to SBA borrowers.

From 2005 until 2009, the three employees and others caused the bank to issue loans under favorable terms to unqualified or underqualified Friends of the Bank and SBA borrowers knowing that these disbursements served no benefit to La Jolla Bank. They and others supported the disbursement of bank funds by supplying or knowingly accepting false and fraudulent information in the borrowers' loan applications, and would knowingly overlook negative aspects of the borrowers' creditworthiness. The three and others demanded and accepted personal payments from the borrowers in return for loans issued by the bank. As part of the conspiracy, the co-conspirators arranged for the bank's SBA department to issue at least \$55.8 million in loans to largely unqualified or underqualified SBA borrowers. They and others used the loan disbursements to inflate the bank's performance measures which, in turn, increased their own compensation. In order to prevent these risky loans from going into default and exposing the true poor performance of the bank's receivables, the three co-conspirators and others caused the bank to issue additional loans, including extensions of lines of credit, to enable the borrowers to make loan payments. Many of these loans defaulted, and losses within the SBA department, in particular, were approximately \$19.8 million, which contributed to the failure of the bank.

The conspirators also took steps to cover up the scheme. In 2009, as the bank was failing, regulators began to investigate La Jolla Bank's poor performance. In order to conceal the mismanagement and self-dealing from the regulators, senior bank officials directed the former bank manager and other co-conspirators to destroy fraudulent financial statements and Friends of the Bank designations contained within the bank's files, according to the former bank manager's plea agreement.

To date, three other defendants have been charged in this case.

***Source:** This investigation was initiated based on information uncovered during another on-going investigation.*

***Responsible Agencies:** This is a joint investigation by the FDIC OIG, FBI, Federal Housing Finance Agency OIG, SBA OIG, and Treasury Inspector General for Tax Administration. The case is being prosecuted by the U.S. Attorney's Office for the Southern District of California, San Diego.*

Former Bank Executive Pleads Guilty

On July 22, 2015, the former vice president of lending at the Bank of Oswego, Lake Oswego, Oregon, pleaded guilty to conspiracy to commit wire fraud and making false entries in bank records.

According to a second superseding Indictment, the former vice president; his brother, a former financial adviser at Morgan Stanley; and others defrauded investors and Morgan Stanley clients by making them think their funds were being used for certain investments when, in fact, they were not, or caused funds to be withdrawn from Morgan Stanley accounts without the authorization of the owner.

The former bank officer also admitted that while he was a vice president of lending at the Bank of Oswego, he and other senior executives conspired and participated in a scheme to defraud whereby they caused, directed, or created false entries in the official records of the bank, submitted false Call Reports, and provided the bank's Board of Directors with false or misleading monthly reports. As a part of the scheme, false documents and statements were made regarding the bank's financial affairs, its other real estate owned sales/purchases, and its cash account usage. As part of his plea agreement, the former vice president of lending stipulated to a consent agreement with the FDIC imposing a prohibition from banking.

Source: FDIC RMS and FBI, Portland Division.

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

Former Bank Employee Sentenced for Embezzlement

On June 25, 2015, a former bank employee—a customer service manager—was sentenced to serve 24 months in federal prison to be followed by 3 years of supervised release for her convictions on embezzlement by a bank employee and embezzlement from Indian tribal organizations. She was also ordered to pay \$217,125 in restitution to Bank of the West, San Francisco, California.

The former bank manager made unauthorized withdrawals totaling \$217,125 from the accounts of six Bank of the West customers over a 31-month period. The affected customers were businesses and individuals, including an 83-year old woman and local Indian tribes. The former manager began withdrawing funds from customers' accounts as if the customers were making in-branch cash withdrawals, except the required personal identification numbers were not supplied. As her embezzlement activity continued and as customers became aware of funds missing from their accounts and contacted the bank about the missing funds, the former manager replaced the missing funds by transferring funds from different customers' accounts to cover the earlier withdrawals. When interviewed by the bank's corporate security staff, the former manager confessed to taking \$55,000 from one victim's account but denied any additional unauthorized activity. She was terminated by the bank on July 28, 2014. The investigation later revealed that the total unauthorized withdrawals were approximately \$217,125.

Source: FDIC Legal Division.

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

Former Bank Employee Victimized Elderly Bank Customer

A retired employee of The Home Savings and Loan Company of Youngstown, Ohio (HSLC), Youngstown, Ohio, was sentenced to 41 months in prison for her role in a bank fraud. HSLC initiated a review of 20 demand deposit accounts held by two bank customers. Their investigation showed that between March 1, 2007, and November 4, 2013, the former bank employee made numerous HSLC official checks payable to herself by debiting customer accounts without authorization. The former employee's chosen victim was an elderly woman who had been a client she worked with frequently while she was employed at HSLC. The former employee also used the trust built through a long professional relationship to obtain a power of attorney for the elderly victim which she later used to perpetuate the fraud in this case. As a result of the scheme, the former employee obtained approximately \$860,000 from the elderly customer's accounts.

On January 15, 2015, the former employee was indicted by a federal grand jury, Northern District of Ohio, Youngstown, Ohio, for bank fraud. On April 1, 2015, she pleaded guilty to bank fraud charges, and on July 8, 2015, she was sentenced to 41 months of incarceration, 3 years of supervised release, and was ordered to pay \$860,000 in restitution.

Source: FDIC RMS.

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

Bank Customer Sentenced to 60 Months in Prison

A bank customer made materially false statements to obtain three separate loans from Municipal Trust and Savings Bank, Bourbonnais, Illinois. One loan was to obtain his personal residence and was in the amount of approximately \$157,000. A second loan was to obtain "rental" property and was in the amount of approximately \$100,000 (in 2012 a state search warrant was executed at this property and over \$3 million of marijuana was seized). The third loan was to obtain a Yukon Denali and was in the amount of approximately \$32,000. On each of these applications, the individual indicated that he had substantial amounts of legal source income. However, the investigation discovered that the bank customer's true source of income was from drug proceeds and not from the sources listed on the loan applications.

On September 9, 2014, the bank customer was charged with possession of marijuana with intent to distribute, three counts of filing false tax returns, and one count of bank fraud. On January 29, 2015, he pleaded guilty to all charges and was immediately remanded to the custody of the Bureau of Prisons. On July 24, 2015, the bank customer was sentenced to 60 months in prison, 4 years of supervised release, and ordered to pay restitution to the IRS in the amount of \$52,158.

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

Responsible Agencies: This is a joint investigation by the FDIC OIG, IRS-CI, and Kankakee Area Metropolitan Enforcement Group. The case was prosecuted by the U.S. Attorney's Office for the Central District of Illinois.

Two Executives Involved in \$190 Million Equipment Financing Fraud Scheme That Caused \$100 Million Loss to Lenders

A co-owner of a bankrupt Illinois company (Equipment Acquisition Resources, Inc., or EAR) that sold refurbished semiconductor-making machinery and the owner of a Pennsylvania company (Machine Tools Direct, Inc.) that sold machine tools engaged in a scheme to fraudulently obtain approximately \$190 million from banks and financing companies and, eventually, caused those lenders to lose at least \$100 million.

From 2005 to October 2009, the co-owner of EAR obtained loans from multiple banks to purchase manufacturing equipment. EAR pledged the same manufacturing equipment as collateral on multiple loans to different financial institutions. Another co-owner of EAR allegedly concealed the multiple pledging from the financial institutions by changing the serial numbers on the manufacturing equipment.

The owner of Machine Tools, Direct, Inc., worked with the EAR co-owners to arrange sham sale transactions between EAR and Machine Tools, Direct, Inc. The three represented to financial institutions and finance companies that the two companies were separate companies engaged in arm's length transactions but, in fact, no such transactions occurred. It is estimated that the total amount of fraudulent activity from this scheme is \$190 million and may have caused a loss to financial institutions of approximately \$112 million.

On February 27, 2014, one of the co-owners of EAR and the owner of Machine Tools, Direct, Inc., were both indicted and charged with mail fraud, wire fraud, and bank fraud. The other EAR co-owner was not charged due to his death several months before the indictment.

On January 7, 2015, the charged EAR co-owner pleaded guilty to one count of wire fraud. On July 22, 2015, he was sentenced to 60 months of incarceration, 3 years of supervised release, and ordered to pay restitution of \$97 million.

A status hearing for owner of Machine Tools, Direct, Inc., was scheduled for October 13, 2015.

Source: This investigation was initiated based on information provided by the FBI regarding Fifth Third Bank, Cincinnati, Ohio.

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

Former Bank Director and Principal Shareholder Pleads Guilty

On April 3, 2015, a former director and principal shareholder of Southwest Community Bank, Springfield, Missouri, pleaded guilty to bank fraud and bankruptcy fraud charges. Southwest Community Bank failed on May 14, 2010. Under the terms of his plea agreement, the former director will be sentenced to 6 years and 6 months in federal prison without parole and must pay \$3,098,896 in restitution to the victims of his fraud schemes.

Beginning on or about May 9, 2005, and continuing through August 14, 2012, the former bank director misused his position to obtain approximately \$65,396,132 in loans from multiple banks for approximately 35 entities in which he had an ownership interest. He engaged in the schemes even after he was under indictment and while incarcerated. 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 also acknowledged that he substantially jeopardized the soundness of Southwest Community Bank and directly contributed to the failure of that bank.

Source: FDIC DRR.

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

Two Developers and Their Wives Plead Guilty in Bank Fraud Case

On May 27, 2015, two developers of the Indian Ridge Resort, Branson, Missouri, and their wives pleaded guilty for their roles in a real estate fraud scheme. Previously, the group was charged with bank fraud, conspiracy to commit bank fraud, money laundering, and conspiracy to commit money laundering. Two of the banks involved—Columbian Bank and Trust (CBT), Overland Park, Kansas, and New Frontier Bank, Greeley, Colorado—were both FDIC-supervised institutions prior to their failure.

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

Following the failure of CBT, a review of the 28 notes held by the bank reflected that all 28 notes were between 75 percent and 100 percent drawn with no supporting performance. By utilizing “shell” companies and submitting fraudulent loan draw requests to the associated financial institutions, the defendants falsely obtained the various borrowers’ loan proceeds. In her plea, one of the wives admitted she knew invoices submitted to the bank included overhead and profit in the line item costs in violation of the terms of the loan agreement. The other wife owned a company called Colorado Modular Home Finders Service, LLC. In her plea she admitted she helped to conceal the developers’ felonies by allowing her company to be used to withdraw home deposits from Columbian Bank and Trust.

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

The two men each pleaded guilty to conspiracy to commit bank fraud and conspiracy to commit money laundering. Their wives each pleaded guilty one count of concealing a felony (misprision).

Source: FDIC DRR.

Responsible Agencies: This is a joint investigation by the FDIC OIG, U.S. Secret Service, and IRS-CI. The case is being prosecuted by the U.S. Attorney's Office for the District of Kansas.

Fugitive Bank Customers Sentenced

On June 5, 2015, a bank customer was sentenced to serve 5 years in prison to be followed by 3 years of supervised release in connection with his guilty plea to conspiracy to commit bank fraud and willfully filing a false tax return. He was also ordered to pay restitution of \$10,759,722 to the FDIC as Receiver for WestSound Bank, Bremerton, Washington, and \$370,541 to the IRS. His wife also pleaded guilty to willfully filing a false tax return. She was sentenced to serve 5 months in prison to be followed by 1 year of supervised release. She was also ordered to pay restitution of \$370,541 (joint and several).

Between April 2005 and August 2007, WestSound Bank originated over 150 loans for borrowers introduced by the bank customer, almost all of whom were immigrants from Eastern Europe who attended church with the bank customer or knew his family in Moldova.

The loans were for the construction of single-family residences, many of which were stated-income loans that required no income or asset verification. The bank customer assisted borrowers in inflating their bank account balances prior to their loan applications and provided false subcontractor bid documents in connection with at least 55 loans totaling more than \$35 million. The investigation also revealed fraudulent tax returns, over-stated incomes and assets, and the speculative intentions of many of the borrowers. The bank customer charged a development fee payable at closing on each loan for finding the lot, assisting with the loan application, and making referrals to subcontractors. His wife, a real estate agent, also received significant commissions related to the transactions.

Aware of the investigation, but before the indictment was returned, the couple fled the U.S. and went to Moldova where the husband retains citizenship. The two were out of the reach of U.S. law enforcement until December 2014, when the wife was returned to the U.S. based on an extradition warrant. She had been arrested in Moldova in September 2014 for having false Moldovan and Russian travel documents. The husband returned to the U.S. on February 23, 2015, to resolve the criminal charges.

Source: FDIC RMS.

Responsible Agencies: This is a joint investigation by the FDIC OIG, FBI, and IRS. The case is being prosecuted by the U.S. Attorney's Office, Western District of Washington.

Former Banker Sentenced for Filing a False Call Report

On April 9, 2015, the former executive vice president of Freedom State Bank, Freedom, Oklahoma, was sentenced to 15 months of incarceration and 1 year of supervised release. He was also ordered to pay \$1,557,808 in restitution. He had pleaded guilty to a one-count Information charging him with making a false statement by filing a materially false Consolidated Report of Condition and Income Report (Call Report) for December 31, 2013.

While employed at the bank, the former executive vice president engaged in a scheme to manipulate the books and records of the bank to conceal his misapplication of funds used to cover customer overdrafts in excess of \$2 million from 2009 through 2013. Freedom State Bank was closed by the Oklahoma State Banking Department on June 27, 2014, and the FDIC was appointed Receiver.

Source: FDIC RMS.

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

Businessman Sentenced to 87 Months in Prison

On August 12, 2015, the owner of Southern Rock and Southern Rock Equipment was sentenced to serve 87 months in prison and pay \$3,216,031 in restitution. He was also ordered to pay a \$500 special money assessment and another \$3.2 million money judgment. After a 4-day jury trial in October 2014, the businessman was found guilty of conspiracy to commit bank fraud and four counts of bank fraud in connection with a scheme to fraudulently obtain loans from First National Bank of Davis, Davis, Oklahoma. In December 2014, the former president of First National Bank of Davis was sentenced to serve 24 months in prison and ordered to pay restitution of \$14,698,660 to the FDIC in connection with his role in the scheme. First National Bank of Davis was regulated by the Office of the Comptroller of the Currency until it was determined to be insolvent, and the FDIC was appointed Receiver on March 11, 2011.

Between October 2009 and March 2011, the former bank president approved large under-collateralized loans in the name of unqualified straw borrowers in order to provide funds to the businessman. During this time, loans to the businessman exceeded the bank's legal lending limit. The two used the proceeds of the fraudulent loans to conceal a \$1.6 million overdraft and legal lending limit violation in connection with extensions of credit by the president to the businessman.

Source: FDIC DRR.

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

Strong Partnerships with Law Enforcement Colleagues

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

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

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



Keeping Current with Criminal Activities Nationwide

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

OIG Headquarters	Financial Fraud Enforcement Task Force, National Bank Fraud Working Group–National Mortgage Fraud Working Sub-group.
New York Region	New York State Mortgage Fraud Working Group; Newark Suspicious Activity Report (SAR) Review Task Force; Philadelphia SAR Review Team; El Dorado Task Force - New York/New Jersey HIDTA; Philadelphia Financial Exploitation Prevention Task Force; Maryland Mortgage Fraud Task Force; Philadelphia Mortgage Fraud Working Group; Pittsburgh SAR Review Team.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force; Southern District of Florida Mortgage Fraud Working Group; Northern District of Georgia Mortgage Fraud Task Force; Eastern District of North Carolina Bank Fraud Task Force; Northern District of Alabama Financial Fraud Working Group; Northern District of Georgia SAR Review Team; Middle District of Georgia SAR Review Team; South Carolina Financial Fraud Task Force.
Kansas City Region	St. Louis Mortgage Fraud Task Force; Kansas City Financial Crimes Task Force; Minnesota Inspector General Council meetings; Kansas City SAR Review Team; Springfield Area Financial Crimes Task Force; Nebraska SAR Review Team; Iowa Mortgage Fraud Working Group.
Chicago Region	Dayton, Ohio, Area Financial Crimes Task Force; Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Detroit SAR Review Team; Financial Investigative Team, Milwaukee, Wisconsin; Milwaukee Mortgage Fraud Task Force; Madison, Wisconsin, SAR Review Team; Indiana Bank Fraud Working Group.
San Francisco Region	FBI Seattle Mortgage Fraud Task Force, Fresno Mortgage Fraud Working Group for the Eastern District of California, Sacramento Mortgage Fraud Working Group for the Eastern District of California, Sacramento SAR Working Group, Los Angeles Mortgage Fraud Working Group for the Central District of California, Orange County Financial Crimes Task Force-Central District of California.
Dallas Region	SAR Review Team for Northern District of Mississippi, SAR Review Team for the Southern District of Mississippi, Oklahoma City Financial Crimes SAR Review Working Group, Austin SAR Review Working Group.
Electronic Crimes Unit	Washington Metro Electronic Crimes Task Force, Botnet Threat Task Force, High Technology Crime Investigation Association, Cyberfraud Working Group, Council of the Inspectors General on Integrity and Efficiency Information Technology Subcommittee, National Cyber Investigative Joint Task Force, FBI Washington Field Office Cyber Task Force.

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

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

In the aftermath of the financial crisis, FDIC-insured institutions continue to make gradual but steady progress. Continuing to replenish the DIF in a post-crisis environment is a critical activity for the FDIC. The DIF balance had dropped below negative \$20 billion during the worst time of the crisis. With various assessments over the past few years and improved conditions in the industry, the DIF balance has increased steadily. The DIF balance as of September 30, 2015 was \$70.1 billion.

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

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

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

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

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

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

OIG Work in Support of Goal 2

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

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

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

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

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

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

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

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

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

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

OIG Work in Support of Goal 3

During the reporting period, we completed work with financial regulatory OIG counterparts on an assignment to examine the progress that the prudential regulators and the CFPB have made in establishing coordination for the consumer protection responsibilities that the various parties carry out. We also continued efforts to protect consumers by way of our Electronic Crimes Unit's involvement in investigating email and other schemes that prey on the public.

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

Coordination of Responsibilities Among the Consumer Financial Protection Bureau and the Prudential Regulators—Limited Scope Review

During a March 20, 2013, hearing held by the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, a concern was raised regarding potential regulatory overlap between the CFPB and the FDIC. In subsequent conversations, the FDIC OIG notified the Subcommittee that it planned to coordinate with the OIGs of the other prudential regulators (FRB, the Office of the Comptroller of the Currency, and the National Credit Union Administration) to assess whether there are overlaps in how the CFPB and prudential regulators are carrying out their regulatory responsibilities. As such, the FDIC OIG and OIGs for the FRB and the CFPB, Department of the Treasury, and the National Credit Union Administration conducted a joint review.

The objective of our review was to assess the extent to which the CFPB and prudential regulators were coordinating their supervisory activities and avoiding duplication of regulatory oversight responsibilities.

We found that the CFPB and prudential regulators were generally coordinating their regulatory oversight activities for federal consumer financial laws, consistent with the Dodd-Frank Act and the provisions of a memorandum of understanding governing coordination activities. Nonetheless, we determined that there are opportunities for enhanced coordination. We did not identify regulatory duplication of oversight responsibilities. Officials from the CFPB and prudential regulators reported that they were generally satisfied with the level of communication and coordination occurring, which has continued to improve since the inception of the CFPB. These officials also identified challenges to coordinating certain supervisory activities and stated that they continue to discuss opportunities for improved coordination. None of the officials interviewed identified any instances where institutions received duplicative or conflicting supervisory guidance from the CFPB and a prudential regulator.

In accordance with the Dodd-Frank Act, the CFPB assumed exclusive responsibility for examining Very Large institutions (those with assets over \$10 billion) for compliance with federal consumer financial laws. Officials from the prudential regulators confirmed that their agencies were continuing to examine Very Large institutions for laws or areas of law for which they retained responsibility under the Dodd-Frank Act. The CFPB and prudential regulators entered into a memorandum of understanding in May 2012 which governs the CFPB and prudential regulators' coordination and information-sharing activities pertaining to Very Large institutions. The CFPB and prudential regulators shared examination schedules, conducted a limited number of simultaneous examinations,¹ and shared draft examination reports for comment and other appropriate supervisory materials.

¹ A simultaneous examination generally is one where material portions of the examinations by the prudential regulator and CFPB are conducted during a concurrent time period to facilitate coordination and information-sharing. Examination activities may be carried out on- or off-site by either regulator.

Based on our interviews, we concluded that the prudential regulators retained responsibility for examining Other institutions (those with assets of \$10 billion or less) for compliance with federal consumer financial laws, and the CFPB does not examine these institutions. Consistent with the framework established by the Dodd-Frank Act, the CFPB exercises limited oversight of these institutions.

We also found that the CFPB requested information from Very Large and Other institutions in support of its consumer protection and enforcement activities, as allowed by the Dodd-Frank Act. CFPB officials usually notified the prudential regulator in advance of such information requests. None of the officials interviewed were aware of any significant complaints from financial institutions pertaining to these requests. As an example of the feedback provided, officials at prudential regulators reported that some institutions questioned the CFPB's information requests because those institutions did not fully understand the CFPB's role and authority to collect such information. The Office of the Comptroller of the Currency noted several examples where other institutions received information requests from the CFPB and erroneously believed they would be examined by the CFPB.

We concluded that there are opportunities for improved coordination between the CFPB and prudential regulators. These opportunities include conducting additional simultaneous examinations, better communicating matters identified in draft supervisory letters among the regulators, establishing a framework to address the potential for conflicting supervisory determinations, developing a standard CFPB process for notifying the prudential regulators of federal consumer financial law violations by Other institutions, and timely notifying the prudential regulators of CFPB information requests to their regulated institutions. The CFPB and prudential regulators meet periodically to discuss these and other matters.

Electronic Crimes Unit Responds to Email and Other Schemes

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

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

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

The OIG's inquiry intake system supplements the OIG Hotline function. The Hotline continues to address allegations of fraud, waste, abuse, and possible criminal misconduct. However, over the past several years, our office has continued to receive a large number of public inquiries ranging from media inquiries to requests for additional information on failed institutions to pleas for assistance with mortgage foreclosures to questions regarding credit card companies and banking practices. These inquiries come by way of phone calls, emails, faxes, and other correspondence. The OIG makes every effort to acknowledge each inquiry and be responsive to the concerns raised. We coordinate closely with others in the Corporation through the FDIC's Public Service Provider working group and appreciate their assistance. We handle those matters within the OIG's jurisdiction and refer inquiries, as appropriate, to other FDIC offices and units or to external organizations. During the past 6-month period, we addressed approximately 225 such matters.

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

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

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

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

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

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

In a number of instances, through purchase and assumption agreements with acquiring institutions, the Corporation has entered into shared loss agreements (SLA). In fact, since loss sharing began during the most recent crisis in November 2008, the Corporation resolved 304 failures with accompanying SLAs; the initial covered balance was \$216.5 billion. As of September 30, 2015, 238 receiverships still had active SLAs, with a covered asset balance at that time of \$35.9 billion. Under these agreements, the FDIC agrees to absorb a portion of the loss—generally 80-95 percent—which may be experienced by the acquiring institution with regard to those assets, for a period of up to 10 years.

As another resolution strategy, the FDIC entered into 35 structured sales transactions involving 43,315 assets with a total unpaid principal balance of \$26.2 billion. Under these arrangements, the FDIC retains a participation interest in future net positive cash flows derived from third-party management of these assets. As of September 30, 2015, the unpaid principal balance was \$3.5 billion.

Other post-closing asset management activities continue to require FDIC attention. FDIC receiverships manage assets from failed institutions, mostly those that are not purchased by acquiring institutions through purchase and assumption agreements or involved in structured sales. As of September 30, 2015, DRR was managing 470 active receiverships with assets in liquidation totaling about \$5.5 billion. As receiver, the FDIC seeks to expeditiously wind up the affairs of the receiverships. Once the assets of a failed institution have been sold and the final distribution of any proceeds is made, the FDIC terminates the receivership.

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

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

While OIG audits and evaluations address various aspects of controls in resolution and receivership activities, OIG investigations benefit the Corporation in other ways. For example, in the case of bank closings where fraud is suspected, our Office of Investigations may send case agents and computer forensic special agents from the ECU to the institution. ECU agents use special investigative tools to provide computer forensic support to OIG investigations by obtaining, preserving, and later examining evidence from computers at the bank.

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

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

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

OIG Work in Support of Goal 4

During the reporting period, and as discussed further below, we completed audit work related to the FDIC's controls over receivership-related federal income tax refunds. We also completed an evaluation involving the risks associated with the early termination of SLAs. Ongoing efforts of our ECU as they relate to bank closings support this goal and are described below.

Controls Over Receivership-Related Federal Income Tax Refunds

As noted earlier, as the receiver of failed insured depository institutions, the FDIC is responsible for maximizing recoveries from the disposition of receivership assets and the pursuit of receivership claims. A significant source of recoveries for receiverships in recent years has been from federal income tax refund claims. Establishing controls to ensure that potential tax refunds are identified and claimed, and that reductions to tax refunds from audits by taxing authorities are minimized, is important for maximizing recoveries for receiverships.

In one of our completed audits this reporting period, we assessed the extent to which FDIC internal controls provide reasonable assurance that management information associated with federal income tax refund claims for receiverships is complete and accurate; responses to IRS inquiries are timely; IRS adjustments to tax refund claims are evaluated, accepted and/or appealed in accordance with relevant criteria; and tax refunds are properly recorded on the books and records of the receiverships.

As of March 31, 2015, DRR reported \$4.2 billion in tax refund claims related to failed financial institution receiverships. The tax refund claims have generally been submitted by either the FDIC, or if the situation warrants, by a failed financial institution's holding company on behalf of a consolidated group. Over 97 percent of the reported refund claims (\$4.09 billion) are for federal income taxes while the remaining 3 percent (\$138 million) are for state, territory, or local income taxes.

The receivership-related income tax refund claims are primarily the result of a one-time change in federal tax law that occurred in 2009. Specifically, Congress amended the federal income tax code by enacting Public Law 111-92, the *Worker, Homeownership, and Business Assistance Act of 2009*, which became law on November 6, 2009. The Act allowed most financial institutions and related holding companies a one-time irrevocable election to carry back 2008 or 2009 net operating losses to their prior tax returns for up to a maximum of 5 tax years, rather than the usual 2 tax years. The impact of this change was a large dollar amount of receivership income tax refund claims related to tax years 2003 through 2009. The tax refund windfall resulting from the Act has led to holding companies and related interests asserting legal ownership of all or a portion of the tax refunds. Of the \$4 billion disbursed from taxing authorities for receivership-related tax refunds, almost 66 percent or \$2.8 billion has been distributed to the FDIC, on behalf of receiverships, or to holding companies. The remaining \$1.2 billion is generally being held in escrow until legal ownership of the monies is determined.

In general, we found that the FDIC had properly recorded \$2.1 billion in receivership federal income tax refunds collected from the IRS, \$50.6 million in interest received on those refunds, and \$45.3 million in uncollected federal income tax refunds for the receiverships that we reviewed. We also found that the DRR Tax Department made significant improvements in its procedures, processes, and training and had initiated a multi-year tax research project to ensure that all recoverable tax refunds had been pursued. In addition, DRR had worked to enhance tax policy and guidelines in situations where ownership of the tax refund was in dispute with the holding company or where the IRS disallowed deductions for estimated selling costs. Notwithstanding these accomplishments, our audit identified further opportunities for DRR to improve controls and guidance. Specifically, we found that the FDIC could:

- Enhance guidance for recording, and maintaining the reliability of, tax refund claim-related information in the Tax Track system;
- Better track and document responses to IRS inquiries and more consistently record activities performed to evaluate and accept, or appeal, IRS tax audit adjustments; and
- Improve procedures for recording potential tax refund recoveries in the receivership records.

Limited DRR Tax Department staff resources were a contributing factor to our findings. In that regard, we brought that issue to management's attention in separate correspondence during the course of our audit as the FDIC continues to reduce resources in this area. We also made observations related to controls over sensitive tax and personally identifiable information maintained by DRR, automated tools used to prepare annual income tax returns, and obtaining IRS account transcripts and reported these matters separately to FDIC management.

We made five recommendations to address the concerns we identified. Our report also identified \$4.6 million in funds put to better use. Management concurred with the recommendations. With respect to the funds put to better use, DRR collected approximately \$140,000 during our audit, researched and determined that a significant portion was not recoverable, and agreed to develop approaches for resolving what remained outstanding.

Risks Associated with Early Terminations of SLAs

The FDIC endeavors to terminate those SLAs that result in estimated savings to the FDIC rather than waiting until the SLA's expiration date as defined in the agreements. However, in executing these transactions, the FDIC must ensure that early termination decisions are not counter to the FDIC's mandate to maximize the value of the receivership estate or harm the FDIC's reputation.

To assess this matter, we conducted an evaluation to determine whether the FDIC has established controls to mitigate risks associated with SLA early terminations and is complying with its early termination process.

When an institution fails, the FDIC may enter into SLAs to reduce the FDIC's immediate cash needs, provide continuity to failed bank customers, and move assets into the private sector. As noted earlier, under an SLA, the FDIC enters into an agreement with an assuming institution to absorb a portion of the loss on a specified asset pool to maximize asset recoveries and minimize the FDIC's losses. In 2010, the FDIC provided certain assuming institutions participating in SLAs with the option to terminate their SLAs early. In 2012, the FDIC created a pilot program to terminate SLAs before their natural expiration date and later expanded the program. The early termination program objective is to maximize receivership recoveries, as required by the FDIC's statutory mandate to maintain the viability of the DIF. Within the FDIC, DRR has overall responsibility for the SLA program.

The FDIC has established process controls that collectively mitigate the risk that early termination decisions are counter to the FDIC's mandate to maximize the value of the receivership estate or harm the FDIC's reputation. Specifically, the FDIC's process controls help to ensure that (1) program eligibility requirements are met, (2) the FDIC's underlying financial analysis for early termination is complete and accurate, (3) the assuming institution is in compliance with the SLA agreement, (4) the FDIC assesses risks to the DIF, and (5) a final review and approval of the decision to terminate is performed by the proper delegated authority within DRR. Further, as part of a 2015 DRR performance goal, DRR was developing a plan to further validate a worksheet it uses to identify the breakeven price the FDIC is willing to accept for an early termination.

The FDIC has limited guidance related to early terminations. Since its introduction, the program has evolved and expanded and involves multiple FDIC divisions and groups within DRR. As a result, the FDIC could benefit from an overarching policy that clearly defines the early termination program objectives and explains the responsibilities and authorities of the various organizations involved.

Based on our testing, we determined that the FDIC is properly assessing whether SLAs are eligible for early termination according to DRR's current guidance. To date, many assuming institutions have declined to terminate their SLAs early, but that trend may change as assuming institutions lose loss coverage under the SLAs and covered asset levels decline. For cases included in our sample, we found that the FDIC complied with key early termination process controls. Moreover, we confirmed that the completed transactions we reviewed were cost beneficial to the FDIC, consistent with the FDIC's early termination program objectives.

We made one recommendation for the Director, DRR, to establish a policy for the SLA early termination program that defines program objectives, explains the early termination process, and assigns roles and responsibilities of each FDIC division and DRR organizational unit involved in the program. Such a policy would help to ensure program understanding, process compliance, and consistent treatment of early termination transactions. DRR concurred with the recommendation and described a corrective action that was responsive.

Electronic Crimes Unit Supports Closed Bank Investigations

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

ECU Provides Forensic Analysis for Case Involving Doral Bank:

As discussed earlier in this report, Doral Bank was headquartered in San Juan, Puerto Rico, with additional offices in New York, New York, and Miami, Florida. Doral Bank was closed on February 27, 2015, and the FDIC was named Receiver. The forensic collection at Doral was conducted from February 27 – March 13, 2015 at all three locations. The FDIC OIG ECU coordinated with Doral Bank information technology personnel, DRR investigators and FDIC forensic contractors in all three locations to assist with the identification and forensic capture of relevant evidence related to the failure. Among other items, we collected personal computers; emails from local machines, network shares, and email servers; user documents; backup media; and copy machine hard disk drives and flash memory.

In total, over 32 terabytes of data was collected. The OIG has been issuing subpoenas for forensic data pertinent to the institution's failure.

The OIG has also coordinated with the U.S. Securities and Exchange Commission (SEC), as the SEC is conducting an investigation into Doral Bank and Doral Financial Corporation (bank holding company). The OIG has received 50 gigabytes of data from the SEC that is currently being analyzed.

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

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

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

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

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

The FDIC has long promoted diversity and inclusion initiatives in the workplace. Section 342 of the Dodd-Frank Act reiterates the importance of standards for assessing diversity policies and practices and developing procedures to ensure the fair inclusion and utilization of women and minorities in the FDIC's contractor workforce. The Dodd-Frank Act also points to the Office of Minority and Women Inclusion as being instrumental in diversity and inclusion initiatives within the FDIC working environment.

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

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

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

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

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

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

OIG Work in Support of Goal 5

During the reporting period, we completed two assignments in support of this goal area. We conducted a review the FDIC's Identity, Credential, and Access Management (ICAM) Program and another review of the Corporation's controls over its Travel Card Program. At the end of the reporting period, among other assignments, we were conducting work related to controls over outside counsel costs associated with professional liability claims and completing our annual review under the Federal Information Security Modernization Act of 2014. Completed reviews are summarized below.

The ICAM Program

Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors, issued on August 27, 2004, requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification. As a government corporation, the FDIC is not subject to HSPD-12. However, the FDIC has decided to voluntarily comply with the goals and objectives of the directive through the ICAM Program.

We conducted an audit to (1) determine the status of the ICAM Program, including progress and costs in relation to goals, budgets, and milestones and (2) identify significant issues or risks that need to be addressed to clarify the long-term direction of the program.

By way of background, HSPD-12 required the Secretary of Commerce to promulgate, in accordance with applicable law, a federal standard for secure and reliable forms of identification. Following the promulgation, the heads of executive departments and agencies were required, to the maximum extent practicable, to mandate the use of identification by federal employees and contractors that meet the standard in gaining physical access to federally controlled facilities and logical access to federally controlled information systems. Based upon this directive, the National Institute of Standards and Technology developed a standard that includes a description of the minimum requirements for a federal personal identity verification (PIV) card system.

The FDIC awarded a contract (referred to herein as the ICAM contract) in September 2011 to procure expertise and support for the planning and implementation of the ICAM Program. Under the terms of the contract, the ICAM Program consisted of two phases. The focus of Phase 1 was to issue PIV cards that provide physical access capabilities for FDIC employees and contractor personnel. The focus of Phase 2 was to implement logical access controls using PIV cards (i.e., multi-factor authentication for users of FDIC information systems). Although the FDIC's PIV cards are designed for both physical and logical access, the principal focus of the ICAM Program has been on developing and issuing PIV cards for physical access. The FDIC had not funded or prepared a budget for Phase 2 of the ICAM Program, and a task order had not been awarded under the ICAM contract for Phase 2 implementation.

With respect to the status of the ICAM Program, according to the terms of the ICAM contract, PIV cards should have been issued to all FDIC employees and contractor personnel by August 2014. However, at that time, a significant number of employees and contractor personnel had not received a PIV card. On August 31, 2014, the FDIC executed a contract modification to increase the cost ceiling of the ICAM contract from \$3.4 million to \$4.9 million. By the close of 2014, the FDIC had expended 90 percent of the ICAM Program's total budget.

As of May 1, 2015, only 4,490 of the 8,527 eligible FDIC employees and contractors had been issued PIV cards. On May 11, 2015, the ICAM Executive Committee, which has oversight responsibility for the ICAM Program, decided to "pause" the PIV card issuance process until it could adequately reassess the costs, benefits, and risks of using the General Services Administration's (GSA) USAccess program. At that time, the FDIC was about to proceed with issuing PIV cards to employees and contractor personnel in the FDIC's field offices. On July 3, 2015, the only remaining active task order on the ICAM contract expired. As a result, contractor work on the ICAM Program stopped. Responsibility for PIV card rollout activities going forward is being handled by FDIC personnel.

Our report noted significant issues and risks that needed to be addressed. Specifically, as of May 1, 2015, the FDIC had not made a decision about whether to move forward with Phase 2 of the ICAM program. According to officials in the Chief Information Officer Office and the Division of Information Technology, such a decision would not be made until the FDIC identified an enterprise-wide solution for implementing multi-factor authentication. The decision about whether to use the PIV cards for multi-factor authentication has implications for whether the goals described in the ICAM Project Charter, such as those pertaining to the management of Public Key Infrastructure certificates, can be achieved. Further, if the PIV cards are not used for logical access, they would only provide some marginal additional utility beyond that of the existing FDIC identification badges (i.e., facilitating access to other federal facilities).

Subsequent to the close of our audit field work, the FDIC decided to use USB tokens (rather than PIV cards) for multi-factor authentication. Now that this decision has been made, the FDIC needs to make two additional determinations that impact the long-term direction of the ICAM Program. Specifically, the FDIC needs to decide whether all employees and contractors should have PIV cards and, if so, how the Corporation will complete the issuance process. Secondly, the FDIC needs to decide how it will maintain PIV cards and FDIC identification badges going forward.

After these determinations are made, the FDIC should focus on:

- clearly defining the roles and responsibilities (including decision-making and accountability) of all parties involved in governing the ICAM Program;
- determining the types of cost, budget, performance, and risk reporting that would be effective in measuring whether the ICAM Program is meeting established goals and expectations; and
- updating project governance documentation, establishing clear ownership and accountability for ICAM Program processes, and making informed and timely decisions.

Like other agencies, the FDIC has been confronted with technical hurdles and challenges in implementing its ICAM Program. Other factors have also contributed to delays in fully implementing the ICAM Program. Most notably, responsibility for implementing various aspects of the program were divided among two FDIC divisions and there did not appear to be clear ownership or a shared vision of what should be accomplished and how. In addition, the ICAM Program was, to some extent, viewed more as an administrative process of issuing PIV cards, rather than the broader program described in the ICAM contract and other ICAM Program documentation. Consequently, despite the relatively significant investment in corporate resources involved, the ICAM Program was not subject to sufficient and consistently robust governance, which resulted in limited success. In our view, the FDIC's decision to pause the ICAM Program for purposes of making critical decisions regarding the program's direction was a prudent one.

The report contains two recommendations addressed to key individuals involved in the program to (1) prepare a business case that defines the goals and approach for implementing the ICAM Program and (2) establish appropriate governance measures over the ICAM Program. In a joint response, management officials concurred with both recommendations and described planned actions that were responsive.

The Travel Card Program

On October 5, 2012, the President signed into law the Government Charge Card Abuse Prevention Act of 2012 (Charge Card Act), Public Law 112-194, requiring all executive agencies to establish and maintain safeguards and internal controls for charge cards. While the FDIC Legal Division has determined that the FDIC is not subject to the Charge Card Act, the Corporation has decided to implement certain provisions it determined represent improved security and industry best practices. The statute also requires Inspectors General in the agencies covered by the Charge Card Act to conduct periodic audits or reviews of travel card programs to analyze risks of illegal, improper, or erroneous purchases and payments. Consistent with the spirit of the Charge Card Act, we conducted an audit of the FDIC's Travel Card Program.

Our audit assessed (1) the extent to which the FDIC's key internal controls align with 12 recognized safeguards and controls that we determined are key controls in mitigating the risk of fraud, misuse, and abuse in government-wide charge card programs and (2) whether the controls are being implemented. Eleven of the 12 safeguards and controls pertain to individually billed accounts (IBA), and the remaining control relates to centrally billed accounts (CBA).

Established in 1998, the GSA SmartPay2 Program provides services to more than 350 federal tribal agencies, organizations, and Native American tribal governments. Customer agencies access GSA SmartPay2 Program solutions by issuing task orders against the GSA SmartPay2 Master Contract from one of three contractor banks, namely, JP Morgan Chase (JP Morgan), Citibank, and US Bank. JP Morgan, the FDIC's travel card provider, issues Visa-branded travel cards to employees for use while on official travel.

Any employee who travels for the FDIC may participate in the Travel Card Program. To the extent permissible by law, FDIC employees are not required to use the travel card, but an employee must obtain GSA government rates for air travel, and in those circumstances FDIC employees must use their travel cards or a CBA. In addition, FDIC travelers are required to use the government travel card for train fares and car rentals if the vendors require its use in order to purchase government fare rail tickets and rent cars at the government car rental rate. FDIC employees are authorized to use the travel card to pay for transportation, lodging, and other travel-related expenses when on official business.

IBA travel cards are issued to employees and used to pay for official travel-related expenses, and the FDIC reimburses employees only for authorized and allowable travel expenses. The employee is responsible for making payment to JP Morgan. Full liability for all charges and fees rests with the individual cardholder and, under the terms of the SmartPay2 Master Contract, the FDIC accepts no liability for charges made to IBAs.

If an employee does not have an IBA travel card, the employee may request permission to use the CBA to purchase government airfare and rail tickets. CBA charges are paid directly by the FDIC to JP Morgan. Travelers without an IBA must use a personal charge card or cash for all other official travel expenses. Employees may not have an IBA for several reasons. They may be new employees who have not yet obtained their own travel cards, infrequent travelers, or cardholders whose accounts were suspended or cancelled due to delinquency or misuse.

Overall, our review did not identify any material weaknesses within the scope of controls and safeguards that we assessed. We determined that the FDIC has established a number of key controls intended to minimize the risk of fraud, misuse, and abuse in the Travel Card Program that were generally consistent with recognized safeguards and controls. For example, the FDIC has provided written policies and procedures for the appropriate use of the charge cards, established spending limits for each charge card account, and ensured that delinquent accounts are addressed and corrective actions are taken to prevent further occurrences. In addition, the FDIC is working to strengthen controls in the area of training and ensuring that the travel card of each employee who ceases to be employed by the agency is invalidated immediately upon separation.

In reviewing individual transactions, we found few policy exceptions, none of which appeared to be of the nature of those that have been the subject of Congressional concern. Moreover, in those cases where the FDIC had detected policy exceptions in the past, employees involved were subject to disciplinary action.

We initially found, however, that the FDIC's Travel Card Program could be strengthened to better align with certain recognized safeguards and controls and to further mitigate associated risks by:

- enhancing policies, procedures, or guidelines that address or clarify requirements for certifying cardholders' continued need and eligibility; training program officials, including officials with responsibility for overseeing the use of the travel card; reviewing Automated Teller Machine cash withdrawals for reasonableness and association with official travel; and performing periodic, program-level reviews of cardholder spending and Automated Teller Machine withdrawal limits to ensure they remain appropriate;
- making a greater use of available reports to detect prohibited transactions that may be indicative of potential fraud and misuse; and
- strengthening certain controls over the CBA program.

We found some transactions that related to on-line hotel reservation services, which could involve ancillary fees that are not reimbursable. We also determined that in situations where on-line hotel reservations are made, the traveler is precluded from using FDIC tax-exemption forms. Further, we learned about a web-based application, the VISA IntelliLink Compliance Management tool, which can be used to test Automated Teller Machine withdrawal transactions and other transactions to identify possible misuses.

While the structure of the FDIC's Travel Card Program limits financial risk to the Corporation, its mission is more successfully carried out when its employees maintain a reputation for integrity. Accordingly, as we generally found during our review, the FDIC must remain vigilant in its efforts to have cost-effective controls over this program, in part, to protect that reputation. During and after our audit fieldwork, the FDIC took actions to address our preliminary observations. We took these actions into consideration in presenting our findings and making recommendations.

We made five recommendations, and management concurred with all of them. Management also agreed to consider our observations related to on-line hotel reservation services and use of IntelliLink and implement changes as appropriate.

OID Investigates UPS Delivery Practices and UPS Agrees to Settle False Claims Allegations

The FDIC OIG joined other investigative colleagues in a unique case for us related to a False Claims Act lawsuit involving the United Parcel Service Inc. (UPS). We are especially appreciative of the FDIC's assistance—particularly from staff in the Division of Administration—as we gathered evidence in this case.

On May 18, 2015, UPS agreed to pay \$25 million to settle civil false claims act violations. The settlement resolves allegations that UPS submitted false claims to the federal government in connection with its delivery of Next Day Air overnight packages. The settlement also resolves allegations that UPS supplied federal customers with inaccurate delivery times and “exception codes” to deprive the customers of the ability to request “Guaranteed Service Refunds” for late overnight deliveries.

UPS is a package delivery company based in Atlanta, Georgia. UPS provides delivery services to hundreds of federal agencies through contracts with GSA and U.S. Transportation Command, which provides support to Department of Defense agencies. Under these contracts, UPS guaranteed delivery of packages by certain specified times the following day.

The settlement reached in May resolves allegations that from 2004 to 2014, UPS engaged in practices that concealed its failure to comply with its delivery guarantees, thereby depriving federal customers of the ability to request refunds for the late delivery of packages. In particular, the government alleged that UPS knowingly recorded inaccurate delivery times on packages to make it appear that the packages were delivered on time, applied inapplicable “exception codes” to excuse late delivery (such as “security delay,” “customer not in,” or “business closed”), and provided inaccurate “on-time” performance data under the federal contracts.

The civil settlement resolves a lawsuit filed under the whistleblower provision of the False Claims Act, which permits private parties to file suit on behalf of the United States for false claims and obtain a portion of the government's recovery. The civil lawsuit was filed in the Eastern District of Virginia by a former employee of UPS, who will receive \$3.75 million.

Source: DOJ, Washington, D.C.

Responsible Agencies: This is a joint investigation by the FDIC OIG, GSA OIG, Defense Criminal Investigative Service, Treasury Inspector General for Tax Administration, and Department of Treasury OIG, with assistance from the Department of Veterans Affairs OIG.

FDIC OIG Increases Efforts to Address Cyber Threats

The ECU is tackling threats to the FDIC's IT environment on multiple fronts. During the reporting period, we formalized a charter and corresponding processes for an OIG Cyber Event Group to better ensure OIG readiness to address cyber threats to the FDIC and share information with interested parties internal and external to the FDIC. We also continued our coordination with the Division of Information Technology and the Chief Information Officer Organization with respect to detecting and preventing insider threats to the abundance of sensitive information and personally identifiable information held by the Corporation. Together we are seeking to proactively prevent any release by FDIC insiders—accidental or deliberate—of such sensitive information beyond the walls of the FDIC's secure environment—through electronic means such as emailing sensitive information to personal email accounts or otherwise allowing such information to be disclosed.

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 began participation in the Washington Field Office Cyber Squad-4 earlier this year (CY-4). There are approximately 19 other federal, state, and local law enforcement agencies participating in CY-4. Through participation in CY-4, the ECU will assist 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 the Currency.

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

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

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

To carry out our responsibilities, the OIG must be professional, independent, objective, fact-based, nonpartisan, fair, and balanced in all its work. Also, the Inspector General and OIG staff must be free both in fact and in appearance from personal, external, and organizational impairments to their independence. As a member of the Council of the Inspectors General on Integrity and Efficiency (CIGIE), the OIG is mindful of the *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.

Strong working relationships are fundamental to our success. We place a high priority on maintaining positive working relationships with the FDIC Chairman, Vice Chairman, other FDIC Board members, and management officials. The OIG is a regular participant at FDIC Board meetings and at Audit Committee meetings where recently issued audit and evaluation reports are discussed. Other meetings occur throughout the year as OIG officials meet with division and office leaders and attend and participate in internal FDIC conferences and other forums.

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

The OIG fully supports and participates in CIGIE activities. We coordinate closely with representatives from the other the financial regulatory OIGs. In this regard, the Dodd-Frank Act created the Financial Stability Oversight Council and further established the Council of Inspectors General on Financial Oversight (CIGFO). This Council facilitates sharing of information among CIGFO member Inspectors General and discusses ongoing work of each member Inspector General as it relates to the broader financial sector and ways to improve financial oversight. CIGFO may also convene working groups to evaluate the effectiveness of internal operations of the Financial Stability Oversight Council.

Additionally, the OIG meets with representatives of the Government Accountability Office to coordinate work, provide OIG perspectives on risk, and minimize duplication of effort. We also work closely with representatives of the DOJ, including the FBI and U.S. Attorneys' Offices, to coordinate our criminal investigative work and pursue matters of mutual interest.

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

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

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

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

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

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

- 1** Provided the OIG's FY 2017 budget proposal to the FDIC Chairman, proposing a budget of \$36 million, to fund 137 authorized positions. The budget reflects a 4-percent increase over the budgets of the past 4 fiscal years.
- 2** Continued to monitor, track, and control OIG spending, particularly as it relates to OIG travel-related expenses, use of procurement cards, and petty cash expenditures.
- 3** Continued efforts to develop a new investigative case management system and worked to better track audit and evaluation assignment milestones and costs and to manage audit and evaluation records located in TeamMate or on shared drives or SharePoint sites.
- 4** Continued efforts to update the OIG's records and information management program and practices to ensure an efficient and effective means of collecting, storing, and retrieving needed information and documents. Took steps to increase awareness of the importance of records management in the OIG, including through communications to OIG staff in headquarters and field locations.
- 5** Continued using our inquiry intake system to capture and manage inquiries from the public, media, Congress, and the Corporation, in the interest of prompt and effective handling of such inquiries. Participated with the FDIC's group of Public Service Providers to share information on inquiries and complaints received, identify common trends, and determine how best to respond to public concerns.
- 6** Continued to refine our redesigned OIG Intranet site to provide a more useful, efficient work tool for all OIG staff and began a re-design of our external Website.
- 7** Carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. Positions filled during the reporting period included several new audit and evaluation managers.

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

- 1 Continued to implement the OIG's Quality Assurance Plan for October 2013–March 2016 to ensure quality in all audit and attestation engagement work and evaluations, in keeping with government auditing standards and *Quality Standards for Inspection and Evaluation*. As part of those efforts, issued the results of our quality control review of Generally Accepted Government Auditing Standards assignments for 2013/2014, in which staff made four internal recommendations related to OIG-performed audits and contractor-performed audits monitored by the FDIC OIG.
- 2 Oversaw contracts to qualified firms to provide audit and evaluation services to the OIG to enhance the quality of our work and the breadth of our expertise as we conduct audits and evaluations, and closely monitored contractor performance.
- 3 Participated in planning the FDIC's Annual Accounting and Auditing Conference to offer OIG staff and others continuing professional education in matters relating to the current economic environment, emerging risk areas, and changes to accounting and auditing standards and practices, in the interest of enhancing the quality of the audit and evaluation function and knowledge of current trends and approaches to auditing and accounting issues. Arranged for OIG special agents to present one of the OIG's high-profile cases at the conference.
- 4 Relied on OIG Counsel's Office to provide legal advice and counsel to teams conducting audits and evaluations, and to support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.
- 5 Conducted internal quality assurance reviews of the Office of Investigations field offices to ensure compliance with quality standards established by CIGIE and applicable Attorney General Guidelines. Coordinated with Treasury OIG who will conduct an investigative peer review as part of the CIGIE 3-year investigative peer review cycle.
- 6 Reviewed and updated a number of OIG internal policies related to audit, evaluation, investigation, and management operations of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the office and made substantial progress converting and transferring all such policies to a new automated policies and procedures repository for use by all OIG staff.
- 7 Monitored and participated in the Corporation's Plain Writing Act initiative to ensure quality products and OIG compliance with the intent of the Act, particularly with respect to the OIG's interface with the public on the OIG Website.

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

- 1** Continued to support members of the OIG pursuing professional training and certifications or attending graduate banking school programs to enhance the OIG staff members' expertise and knowledge. 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.
- 2** Employed interns on a part-time basis in the OIG to provide assistance to the OIG.
- 3** Selected an individual from the FDIC to serve in a temporary detail position in the immediate Office of the Inspector General as a learning and professional development opportunity and supported an FDIC OIG employee to serve on a detail with the FDIC's OCFI to foster his professional development.
- 4** Enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities.
- 5** Carried out the OIG's Mentoring Program for 2015, which paired mentors and mentorees as a means of developing and enriching both parties in the relationship and enhancing contributions of OIG staff to the mission of the OIG.
- 6** Provided one of the members of the OIG's Counsel's Office to serve as a Special Assistant U.S. Attorney for multiple cases and trials involving bank fraud. This opportunity allows the Associate Counsel to apply legal skills as part of the prosecutorial teams in advance of and during the trials.

Foster Good Client, Stakeholder, and Staff Relationships

- 1 Maintained congressional working relationships by communicating with various Committee staff on issues of interest to them; providing them our semiannual report to the Congress; notifying interested congressional parties regarding the OIG's completed audit and evaluation work; attending or monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the Corporation's Office of Legislative Affairs on issues of mutual interest.
- 2 Communicated with the Chairman, Vice Chairman, 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 means.
- 3 Participated in numerous outreach efforts with such external groups as the Federal Audit Executive Council, DOJ, and the American Bankers Association Commercial Lending School to provide general information regarding the OIG and share perspectives on issues of mutual concern and importance to the financial services industry.
- 4 Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
- 5 Kept RMS, DRR, the Legal Division, and other FDIC program offices informed of the status and results of our investigative work impacting their respective offices. This was accomplished by notifying FDIC program offices of recent actions in OIG cases and providing Office of Investigations' quarterly reports to RMS, DRR, 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.
- 6 Coordinated with the Chairman of the FDIC Audit Committee to provide status briefings and present the results of completed audits, evaluations, and related matters for his and other Committee members' consideration.
- 7 Continued to interact with international counterparts from the Deposit Insurance Corporation of Japan to share information on the mission of the FDIC OIG, our investigative function, and coordination with the DOJ.

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

- 8** Supported the Inspector General community by participating on the CIGIE Audit Committee; attending monthly CIGIE meetings; responding to requests for information; participating in Assistant Inspectors General for Investigations, Council of Counsels to the IGs, and other meetings; and commenting on various legislative matters through the Legislative Committee.
- 9** Communicated with representatives of the OIGs of the federal banking regulators and others to discuss audit, evaluation, and investigative matters of mutual interest and leverage knowledge and resources. Participated on CIGFO, as established by the Dodd-Frank Act, and coordinated with the IGs on that council. Joined others on a CIGFO audit team in issuing a report on the Financial Stability Oversight Council's oversight of interest rate risk and provided the FDIC OIG's input to the CIGFO's annual report for 2015.
- 10** Coordinated with the Government Accountability Office on its ongoing efforts related to the annual financial statement audit of the FDIC and on other Government Accountability Office work of mutual interest.
- 11** Coordinated with the FDIC's Public Service Provider group on matters regarding inquiries from the public and how best to respond to or refer such inquiries and related concerns.
- 12** Coordinated with 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.
- 13** Briefed and/or responded to interested Congressional parties regarding our Operation Choke Point-related work; on-going work related to involvement by FDIC non-career officials in the Freedom of Information Act response process; any instances where the FDIC may have denied timely and complete access to information that the Inspector General requested (of which there were none); and circumstances surrounding the departure of a senior FDIC official.
- 14** Coordinated with SIGTARP to provide information on FDIC OIG work related to any SIGTARP matters for inclusion in SIGTARP's quarterly reports to the Congress.

Enhance OIG Risk Management Activities

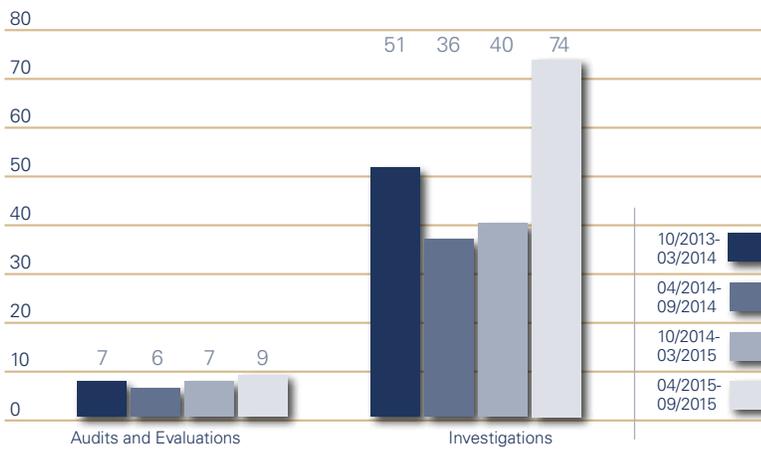
- 1** Undertook risk-based OIG planning efforts for audits, evaluations, and investigations for FY 2016 and beyond, taking into consideration the goals of, and risks to, FDIC corporate programs and operations and those risks more specific to the OIG. Devoted resources to developing a universe of FDIC 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.
- 2** Attended FDIC Board Meetings, IT/Cyber Security Oversight Group meetings, Complex Financial Institutions Coordination Group meetings, corporate planning and budget meetings, and other senior-level management meetings to monitor or discuss emerging risks at the Corporation and tailor OIG work accordingly.
- 3** Assessed OIG controls in support of the annual assurance letter to the FDIC Chairman, under which the OIG provides assurance that it has made a reasonable effort to meet the internal control requirements of the Federal Managers' Financial Integrity Act, Office of Management and Budget A-123, and other key legislation, in preparation for issuing the OIG's annual assurance letter.
- 4** Enhanced 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 by way of increased participation in government-wide task forces and law enforcement working groups. Also developed a charter for the OIG's Cyber Event Group to identify key resources and help ensure the OIG's continuous coverage and readiness to address potentially urgent cyber events affecting the FDIC or other federal entities.
- 5** Met with the Government Accountability Office to share our perspectives on the risk of fraud at the FDIC. We did so in response to the Government Accountability Office's responsibility under Statement of Auditing Standards No. 99, Consideration of Fraud in Financial Statement Audits.
- 6** Monitored the management and performance challenge areas that we identified at the FDIC, in accordance with the Reports Consolidation Act of 2000 as we conducted audits, evaluations, and investigations: Carrying Out Dodd-Frank Act Responsibilities, Maintaining Strong IT Security and Governance Practices, Maintaining Effective Supervisory Activities and Preserving Community Banking, Carrying Out Current and Future Resolution and Receivership Responsibilities, Ensuring the Continued Strength of the Insurance Fund, Promoting Consumer Protections and Economic Inclusion, Implementing Workforce Changes and Budget Reductions, and Ensuring Effective Enterprise Risk Management Practices.

Cumulative Results (2-year period)

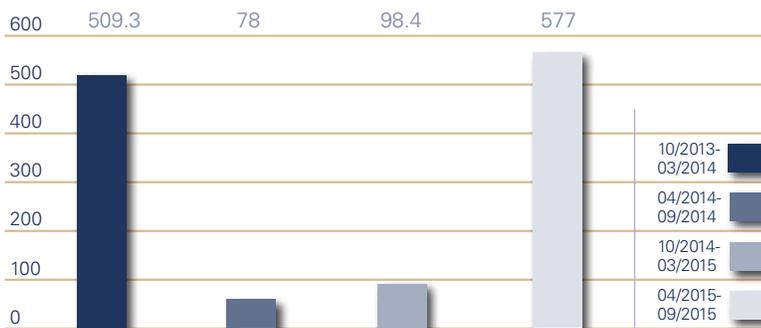
Nonmonetary Recommendations

October 2013 – March 2014	37
April 2014 – September 2014	27
October 2014 – March 2015	35
April 2015 – September 2015	20

Products Issued and Investigations Closed



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



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

Reporting Requirements		Page
Section 4(a)(2)	Review of legislation and regulations	79
Section 5(a)(1)	Significant problems, abuses, and deficiencies	11-67
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies	11-67
Section 5(a)(3)	Recommendations described in previous semiannual reports on which corrective action has not been completed	80
Section 5(a)(4)	Matters referred to prosecutive authorities	10
Section 5(a)(5) and 6(b)(2)	Summary of instances where requested information was refused	82
Section 5(a)(6)	Listing of audit reports	81
Section 5(a)(7)	Summary of particularly significant reports	11-67
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	82
Section 5(a)(9)	Statistical table showing the total number of audit reports and the total dollar value of recommendations that funds be put to better use	82
Section 5(a)(10)	Audit recommendations more than 6 months old for which no management decision has been made	82
Section 5(a)(11)	Significant revised management decisions during the current reporting period	82
Section 5(a)(12)	Significant management decisions with which the OIG disagreed	82

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

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

Review of Legislation and Regulations

The FDIC OIG's review of legislation and regulations during the past 6-month period involved continuing efforts to monitor and/or comment on enacted law and/or proposed Congressional legislation, including:

- The Federal Information Security Modernization Act of 2014 (Public Law 113-283): analyzed the Act's provisions regarding national security systems and provided information about such systems for consideration by the FDIC Legal Division.
- Office of Management and Budget's (OMB) draft 2015 Memorandum "Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements" and the related "FY 2016 CIO FISMA Metrics": provided comments to OMB.
- OMB's request for Agency Contingency Plans: provided a response to OMB.
- Digital Accountability and Transparency Act of 2014 (DATA Act), Public Law 113-101 and OMB's implementing guidance, OMB Memorandum M-15-12, "Increasing Transparency of Federal Spending by Making Federal Spending Data Accessible, Searchable, and Reliable.": communicated with the FDIC on whether the Act and guidance were legally binding on the FDIC. We considered any potential effects on the OIG's obligations under the Act.
- S. 579, the Inspector General Empowerment Act: reviewed the bill to determine whether to send comments thereon to CIGIE.
- The FDIC's proposed changes to the FDIC's Privacy Act System of Records Notices: provided the FDIC with comments regarding the Privacy Act System of Records Notices that are managed by the OIG or by other FDIC components that may have implications for the OIG.
- Office of Government Ethics Regulation at 5 CFR Part 2638, The Executive Branch Ethics Program: reviewed proposed changes to Part 2638 and attended an Office of Government Ethics-sponsored meeting regarding the proposed changes to that Part.

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 may be different from the initial recommendations made in the OIG reports. However, the OIG has agreed that the planned actions meet the intent of the initial recommendations. The information in this table is based on (1) information supplied by FDIC's Corporate Management Control, Division of Finance (CMC) 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: (two recommendations from one report)

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 and Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Any Associated Monetary Amounts
Management Action In Process		
EVAL-15-003 The FDIC's Supervisory Approach to Cyberattack Risks 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 Information Technology-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.*

* Implementation scheduled for a future date.

Table II
Audit and Evaluation Reports
Issued by Subject Area

Report Number and Date	Audit/Evaluation Report Title	Questioned Costs		Funds Put to Better Use
		Total	Unsupported	
Supervision				
AUD-15-005 August 12, 2015	Material Loss Review of Valley Bank, Moline, Illinois		N/A	
AUD-15-006 September 3, 2015	Material Loss Review of Capitol City Bank & Trust Company, Atlanta, Georgia		N/A	
AUD-15-007 September 3, 2015	Material Loss Review of Doral Bank, San Juan, Puerto Rico		N/A	
AUD-15-008 September 16, 2015	The FDIC's Role in Operation Choke Point and Supervisory Approach to Institutions that Conducted Business with Merchants Associated with High-Risk Activities		N/A	
Consumer Protection				
EVAL-15-004 June 1, 2015	Coordination of Responsibilities Among the Consumer Financial Protection Bureau and the Prudential Regulators – Limited Scope Review		N/A	
Receivership Management				
EVAL-15-005 August 26, 2015	Risks Associated with Early Termination of Shared-Loss Agreements		N/A	
AUD-15-009 September 21, 2015	Controls Over Receivership-Related Federal Income Tax Refunds		N/A	\$4,586,022
Resources Management				
AUD-15-010 September 30, 2015	The FDIC's Travel Card Program		N/A	
AUD-15-011 September 30, 2015	The FDIC's Identity, Credential, and Access Management Program		N/A	
Totals for the Period		\$0	\$0	\$4,586,022

**Table III
Audit and Evaluation Reports
Issued with Questioned Costs**

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

**Table IV
Audit and Evaluation Reports
Issued with Recommendations
for Better Use of Funds**

	Number	Dollar Value
A. For which no management decision has been made by the commencement of the reporting period.	0	\$0
B. Which were issued during the reporting period.	1	\$4,586,022
Subtotals of A & B	1	\$4,586,022
C. For which a management decision was made during the reporting period.	1	\$4,586,022
(i) dollar value of recommendations that were agreed to by management.	1	\$4,586,022
- based on proposed management action.	1	\$4,586,022
- based on proposed legislative action.	0	\$0
(ii) dollar value of recommendations that were not agreed to by management	0	\$0
D. For which no management decision has been made by the end of the reporting period.	0	\$0
Reports for which no management decision was made within 6 months of issuance.	0	\$0

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

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

**Table VI
Significant Revised Management
Decisions**

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

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

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

**Table VIII
Instances Where Information
Was Refused**

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

Information on Failure Review Activity

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

FDIC OIG Review Activity for the Period April 1, 2015 through September 30, 2015
 (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 (\$ millions)	Grounds Identified by the State Bank Supervisor for Appointing the FDIC as Receiver	Unusual Circumstances Warranting In-Depth Review?	Reason for In-Depth Review	Due Date or Date Issued
Failure Review Activity – Updated from Previous Semiannual Report						
Reviews Pending or Ongoing as of the End of the Reporting Period						
Edgebrook Bank Chicago, Illinois	5/8/15	\$16.8				
Highland Community Bank Chicago, Illinois	1/23/15	\$5.8				
Northern Star Bank Mankato, Minnesota	12/19/14	\$5.9				
Eastside Commercial Bank Conyers, Georgia	7/18/14	\$33.9				
The Freedom State Bank Freedom, Oklahoma	6/27/14	\$5.8				

Peer Review Activity

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

Section 989C of the Dodd-Frank Act contains additional semiannual reporting requirements pertaining to peer review reports. Federal Inspectors General are required to engage in peer review processes related to both their audit and investigative operations. In keeping with Section 989C, the FDIC OIG is reporting the following information related to its peer review activities. These activities cover our most recent roles as both the reviewed and the reviewing OIG and relate to both audit and investigative peer reviews.

Audit Peer Reviews

Definition of Audit Peer Review Ratings

Pass

The system of quality control for the audit organization has been suitably designed and complied with to provide the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

Pass with Deficiencies

The system of quality control for the audit organization has been suitably designed and complied with to provide the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects with the exception of a certain deficiency or deficiencies that are described in the report.

Fail

The review team has identified significant deficiencies and concludes that the system of quality control for the audit organization is not suitably designed to provide the reviewed OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects or the audit organization has not complied with its system of quality control to provide the reviewed OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

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

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

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

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

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

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

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

As is customary, we also issued a Letter of Comment, dated April 30, 2014, that set forth findings and recommendations that were not considered to be of sufficient significance to affect our opinion expressed in the system review report. We made 14 recommendations. NARA OIG agreed with 11 of the 14 recommendations, partially agreed with one recommendation, and did not agree with the remaining two recommendations. NARA's planned actions adequately addressed the 11 recommendations with which NARA agreed. With respect to the remaining three, NARA's response included a rationale for its decision not to fully address those recommendations. Estimated completion dates for corrective actions ranged from June 30, 2014 to September 30, 2014. In 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, 2015. NARA OIG recently informed us that full implementation of the two recommendations is anticipated by September 30, 2016.

Investigative Peer Reviews

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

- The Department of Energy OIG conducted the most recent peer review of our investigative function and issued its final report on the quality assessment review of the investigative operations of the FDIC OIG on July 31, 2012. The Department of Energy OIG reported that in its opinion, the system of internal safeguards and management procedures for the investigative function of the FDIC OIG in effect for the year ending June 22, 2012, was in compliance with quality standards established by CIGIE and applicable Attorney General guidelines. These safeguards and procedures provided reasonable assurance of conforming with professional standards in the planning, execution, and reporting of FDIC OIG investigations.
- The FDIC OIG conducted a peer review of the investigative function of the Environmental Protection Agency OIG. We issued our final report to EPA OIG on December 2, 2014. We reported that, in our opinion, the system of internal safeguards and management procedures for the investigative function of the EPA OIG in effect for the period October 1, 2012 through September 30, 2013 was in compliance with the quality standards established by CIGIE and Attorney General Guidelines.

Our Office of Investigations will be reviewed by the Department of the Treasury OIG in 2015.

We congratulate two members of the FDIC OIG who were honored at the Annual CIGIE Award Ceremony on October 22, 2015

CIGIE Awards



Special Agent Kelvin Zwiefelhofer of our San Francisco Office was honored, along with other law enforcement partners involved in the case, with a CIGIE Award for Excellence for Uncovering and Jointly Investigating and Prosecuting a Multi-Million Dollar Bank, Securities, and TARP Fraud Scheme. The team's outstanding efforts led to the convictions of former bank officers of United Commercial Bank.

L. to R. CIGIE Vice Chair, Allison Lerner, National Science Foundation IG; Kelvin Zwiefelhofer; CIGIE Chair, Michael Horowitz, Department of Justice IG.

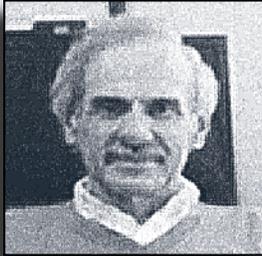
Congratulations to:

Kelvin Zwiefelhofer, Special Agent, FDIC OIG
Marius Greenspan, Special Agent, SIGTARP
Ryan Wat, Special Agent, FRB/CFPB OIG
John Broderick, Special Agent, FBI
Phillip Villanueva, Financial Fraud Investigator, DOJ
Denise Oki, Paralegal Specialist, DOJ
Robert Rees, Assistant U.S. Attorney, Northern District of California
Adam Reeves, Assistant U.S. Attorney, Northern District of California

Senior IT Specialist Daniel Craven received an Award for Excellence—IT, along with other IT professionals from the Inspector General community in recognition of exceptional and unique contributions, by collaborating across the OIG community, to create an innovative maturity model and methodology that strengthened the assessment and oversight of agencies' information security under the Federal Information Security Management Act (FISMA). The team's outstanding efforts led to development of a maturity model to guide OIG FISMA reviews of agencies' continuous monitoring management programs.

Congratulations to:

Daniel Craven, FDIC OIG
Michael Bowman, Department of Veterans Affairs OIG
John Garceau, Department of Housing and Urban Development OIG
Khalid Hasan, FRB/CFPB OIG
Louis King, Department of Transportation OIG
Michael Marshlick, Department of Transportation OIG
Gwendolyn McGowan, Treasury Inspector General for Tax Administration
Andrew Patchen, FRB/CFPB OIG
Peter Sheridan, FRB/CFPB OIG

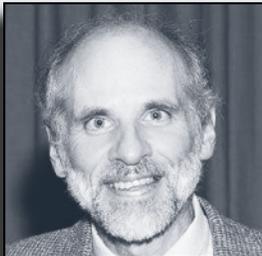


David Graf Retirement

David Graf retired from the FDIC after more than 32 years of federal service. He began his federal career in September 1972 as a management analyst with the Department of the Army in Picatinny, New Jersey. Over the course of the next 37 years, he served many other federal entities, including the Department of the Air Force, Department of Transportation, Department of Education, Department of Justice's Immigration and Naturalization Service, and Department of the Treasury. Those assignments brought him to such locations as St. Louis, Missouri; Chambersburg, Pennsylvania; Vicksburg, Mississippi; Huachuca City, Arizona; Wright-Patterson Air Force Base, Ohio; Baltimore, Maryland; and Fort Hood, San Antonio, Houston, Dallas, and Fort Worth, Texas.

In January 2010, David joined the FDIC's East Coast Temporary Satellite Office in Jacksonville, Florida, as a human resources specialist. He joined the FDIC OIG headquarters office in August 2011, where he made exceptional contributions to our workplace.

David handled sensitive employee relations issues and helped resolve a number of situations to the satisfaction of all parties involved. His sense of fairness was largely responsible for his success. David also made countless other contributions to the OIG, including classifying positions, helping with hiring efforts, on-boarding new staff, administering the OIG's drug-free workplace program, and assisting with the OIG's furlough process during the government shutdown in October 2013.



Duane Rosenberg Retirement

Duane Rosenberg retired from the FDIC after more than 35 years of federal service. His career began in 1979 when he worked as an auditor with the Civil Aeronautics Board in Denver, Colorado. In 1980, he transferred to the Civil Aeronautics Board in Washington D.C. where he advanced steadily in his career as an auditor. In June 1982, he began working at the Federal Communications Commission in Washington, D.C., where he worked as both a systems accountant and an auditor for the next 6 years. He then transferred to the FDIC OIG as a senior auditor, and during his nearly 27-year tenure in the OIG, he advanced to a senior audit specialist position. During his earlier years at the FDIC OIG, on several occasions, he contributed as a team member assisting the U.S. General Accounting Office (now the Government Accountability Office) in its conduct of annual audits of the FDIC's financial statements. Many of the other audits that Duane worked on over the years led to improvements in the economy, efficiency, and effectiveness of financial and administrative operations of the Corporation. Duane also contributed during the recent financial crisis to the FDIC OIG's important in-depth reviews and failed bank reviews of failed FDIC-supervised institutions.



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**), 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.