Office of Inspector General

Semiannual Report to the Congress

October 1, 2017 – March 31, 2018

FDIC

Federal Deposit Insurance Corporation

Under the Inspector General Act of 1978, as amended, the Federal Deposit Insurance Corporation Office of Inspector General has oversight responsibility of the programs and operations of the FDIC.

The 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 5,880 individuals carry out the FDIC mission throughout the country.

According to most current FDIC data, the FDIC insured more than $7.1 trillion in deposits in 5,670 institutions, of which the FDIC supervised 3,637. The Deposit Insurance Fund balance totaled $92.7 billion as of December 31, 2017. Active receiverships as of December 31, 2017, totaled 338, with assets in liquidation of about $2.27 billion.

Office of Inspector General

Semiannual Report to the Congress

October 1, 2017 – March 31, 2018

Federal Deposit Insurance Corporation

Inspector General's Statement

I am pleased to present the Semiannual Report for the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) for the period of October 1, 2017 through March 31, 2018. The work highlighted in this Report illustrates the broad range of our oversight responsibilities and the importance of our work for the agency, financial sector, policymakers, and the American people.

During the reporting period, we issued our *Top Management and Performance Challenges* document, which identified the significant risks facing the FDIC. In particular, we identified seven primary Challenges for the agency: Emerging Cybersecurity Risks at Insured Financial Institutions; Management of Information Security and Privacy Programs; Utilizing Threat Information to Mitigate Risk in the Banking Sector; Readiness for Banking Crises; Enterprise Risk Management Practices; Acquisition Management and Oversight; and Measuring Costs and Benefits of FDIC Regulations. This assessment was based on our extensive oversight work and research relating to reports by other oversight bodies, review of academic and other relevant literature, perspectives from Government agencies and officials, and information from private sector entities.

In addition, we completed several audit and evaluation reports during this Semiannual Report period. These reports included a review of the FDIC's information security program; an evaluation of the agency's implementation of two rules regarding the ability of consumers to repay mortgages; a Material Loss Review of the causes of failure and FDIC's supervision of First NBC Bank in New Orleans, Louisiana; and an evaluation of the Claims Administration System, an important platform to identify insurance determinations for failed or failing financial institutions.

Our reports for this period contained 33 important recommendations for improvement to the FDIC's operations and functions. Our recommendations are significant in prompting and encouraging improvements and efficiencies at the FDIC, and therefore, we closely monitor the agency's progress and implementation of the OIG recommendations. This Semiannual Report highlights an important information security-related recommendation that was implemented during the reporting period. In addition, we note that certain significant recommendations have remained unimplemented for extended periods of time.

In addition to these reports, the OIG conducts significant investigations into criminal and administrative matters. Many of our cases are complex multi-million-dollar ones involving sophisticated schemes of bank fraud, embezzlement, money laundering, and other crimes committed by bank executives and insiders. Our OIG investigations achieved significant impact, resulting in 45 convictions and fines, restitution orders, and forfeitures over $221 million. In addition, our cases led to the arrest of 20 individuals and 39 indictments and informations. In many instances, we worked these cases collaboratively with our law enforcement colleagues. For example, in a recent case, HSBC Holdings, the parent company of HSBC Bank, entered into a Deferred Prosecution Agreement and agreed to pay more than $100 million. A related case involved a front-running scheme in the foreign currency exchange markets. An HSBC trader misused his position to execute trades for millions of dollars in profits to the bank at the expense of one of the bank's clients.

Of special note, Thomas Hoenig concluded his service as Vice Chairman at the FDIC, and we are grateful for his leadership as Chairman of the Audit Committee and for his focus on implementing the OIG's recommendations to improve the FDIC. We also bade farewell to a long-time colleague, Marshall Gentry, Assistant IG for Program Audits and Evaluations. Moreover, we welcomed two new leaders to the Office – a Director for our newly-established Office of Information Technology (IT), and a Special Agent in Charge for the Electronic Crimes Unit – in order to develop and strengthen our foundation for further IT innovations within the OIG.

Our Office appreciates the continued support of Members of Congress and staff, the FDIC and its leaders, as well as our colleagues within the Inspector General (IG) community. In addition, I am very thankful to the women and men of the OIG for their dedication to our mission. We remain committed to serving the American people as a leader in the IG community.

Jay N. Lerner
Inspector General
April 30, 2018

Table of Contents

Inspector General's Statement	i
Acronyms and Abbreviations	2
Introduction and Overall Results	4
Audits, Evaluations, and Other Reviews	6
Investigations	22
Other Key Priorities	31
Reporting Requirements	37
Appendix 1 Information Required by the Inspector General Act of 1978, as amended	39
Appendix 2 Information on Failure Review Activity	54
Appendix 3 Peer Review Activity	55
Congratulations and Farewell	58

Acronyms and Abbreviations

APT	Advanced Persistent Threat
C&C	Cotton & Company LLP
CAS	Claims Administration System
CEO	Chief Executive Officer
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CRS	Congressional Research Service
DATA Act	Digital Accountability and Transparency Act of 2014
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
ERM	Enterprise Risk Management
FBI	Federal Bureau of Investigation
FCD	Federal Continuity Directive
FDIC	Federal Deposit Insurance Corporation
FEMA	Federal Emergency Management Agency
FI	Financial Institution
FISMA	Federal Information Security Modernization Act of 2014

FX	Foreign Exchange
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IRS-CI	Internal Revenue Service-Criminal Investigation
IT	Information Technology
MEF	Mission Essential Function
NIST	National Institute of Standards and Technology
OFI	Office of Financial Institutions
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PMEF	Primary Mission Essential Function
RMIC	Risk Management and Internal Control
SAR	Suspicious Activity Report
SBA	Small Business Administration
TSP	Technology Service Provider
TVA	Tennessee Valley Authority
USAO	U.S. Attorney's Office

Introduction and Overall Results

The FDIC OIG mission is to prevent, deter, and detect fraud, waste, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

Our vision is to serve the American people as a recognized leader in the Inspector General community: driving change and making a difference by prompting and encouraging improvements and efficiencies at the FDIC; and helping to preserve the integrity of the agency and the banking system, and protect depositors and financial consumers.

These important values are hallmarks of our work:

- **Integrity**
- **Independence**
- **Accuracy**
- **Fairness**
- **Objectivity**
- **Accountability**
- **Transparency**
- **Professionalism**
- **Judgment**

Our Office carries out its mission in line with a set of Guiding Principles that we have adopted as "One OIG," and the results of our work during the reporting period are presented in this report within the framework of those principles. Our Guiding Principles focus on impactful audits and evaluations; significant investigations; partnerships with external stakeholders (the FDIC, Congress, whistleblowers, and our fellow OIGs); efforts to maximize use of resources; leadership skills and abilities; and importantly, teamwork.

The following table presents overall statistical results from the reporting period.

Overall Results (October 1, 2017 – March 31, 2018)	
Audit and Evaluation Reports Issued	5
Nonmonetary Recommendations	33
Investigations Opened	31
Investigations Closed	28
OIG Subpoenas Issued	7
Judicial Actions:	
Indictments/Informations	39
Convictions	45
Arrests	20
OIG Investigations Resulted in:	
Fines	$153,239,860
Restitution	$66,937,051*
Asset Forfeitures	$1,396,077
Total	$221,572,988
Referrals to the Department of Justice (U.S. Attorneys)	59
Proposed Regulations and Legislation Reviewed	5
Responses to Requests Under the Freedom of Information/Privacy Act	22

*Of this total amount, $14,970,145 was ordered joint and several with other individuals sentenced during this or prior reporting periods.

Audits, Evaluations, and Other Reviews

The FDIC OIG seeks to conduct superior, high-quality audits, evaluations, and reviews. We do so by:

- Performing audits, evaluations, and reviews in accordance with the highest professional standards and best practices.
- Issuing relevant, timely, and topical audits, evaluations, and reviews.
- Producing reports based on reliable evidence, sound analysis, logical reasoning, and critical thinking.
- Writing reports that are clear, compelling, thorough, precise, persuasive, concise, readable, and accessible to all readers.
- Making meaningful recommendations focused on outcome-oriented impact and cost savings.
- Following up on recommendations to ensure proper implementation.

We issued five audit and evaluation reports during the reporting period, as discussed below. These reports contained 33 recommendations, and spanned various FDIC programs and activities. Our office also reviews all failures of FDIC-supervised institutions that cause losses to the Deposit Insurance Fund (DIF) of less than the material loss threshold outlined in the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) to determine whether circumstances surrounding the failures would warrant further review. We issued two failed bank reviews and this activity is presented in Appendix 2.

Claims Administration System Functionality

The FDIC's Claims Administration System (CAS) is a mission-critical system that FDIC personnel use to identify depositors' insured and uninsured funds in failing and failed financial institutions. CAS's capabilities affect the FDIC's ability to pay deposit insurance claims in a prompt and accurate manner. We evaluated the extent to which CAS has achieved the FDIC's performance expectations for capacity, timeliness, and accuracy in making insurance determinations.

CAS has substantially met the FDIC's expectations for capacity, timeliness, and accuracy in making insurance determinations for most insured institutions. Recognizing the difficulties in resolving a large institution over a closing weekend, the FDIC issued rules intended to mitigate potential shortfalls in CAS capability. The largest financial institutions (those with 2 million or more deposit accounts) are required to configure their information systems and data to enable the FDIC to make insurance determinations by April 2020. We recommended further simulation and testing for failing and failed large bank scenarios in order to facilitate resolution planning for potential large bank failures and decrease the risk of untimely insurance determinations.

The FDIC has not fully validated the maximum processing capacity of CAS. In the original justification for CAS in 2006, FDIC program officials initially expected that CAS could make insurance determinations for an institution of any size, up to 5 million deposit accounts. Because the FDIC recognized that it could not achieve this expectation due to the account complexities at larger institutions, the FDIC adjusted its expectations for institutions with up to 2 million deposit accounts.

CAS improved timeliness of insurance determinations compared to the FDIC's predecessor system. The FDIC's goal is to provide depositors at failed institutions with access to their insured funds within one or two business days of failure. Although the FDIC has never failed to meet this timeliness standard, CAS may not be able to meet the FDIC's goal for the largest institutions due to the volume and complexity of large bank deposit platforms. In such cases, the FDIC may withhold a portion of the failed institution's deposits until an insurance determination can be made.

Regarding accuracy in making insurance determinations, CAS has reduced the risk of inaccurate insurance determinations as compared to the FDIC's predecessor system by decreasing the opportunity for human error. The FDIC strives to provide an accurate estimate of uninsured deposits during pre-closing activities. In this regard, the FDIC believes that CAS capabilities and procedures provide reasonable assurance of the accuracy of insurance determinations.

We made three recommendations to improve CAS functionality through additional testing, and FDIC management concurred.

The full report is available at https://www.fdicoig.gov/sites/default/files/publications/EVAL-18-002_0.pdf.

Audit of the FDIC's Information Security Program—2017

We issued our report on the *Audit of the FDIC's Information Security Program—2017*. We contracted with Cotton & Company LLP to conduct this audit, which evaluated the effectiveness of the FDIC's information security program and practices, as required by the Federal Information Security Modernization Act (FISMA).

We found that the FDIC had established a number of information security program controls and practices that were generally consistent with applicable Federal requirements, policies, standards, and guidelines. The FDIC had also taken steps to strengthen its information security program controls following the 2016 FISMA audit and was working to further strengthen controls in a number of areas at the close of the 2017 audit. However, we found security control weaknesses that limited the effectiveness of the FDIC's information security program and practices, and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk.

The report contained a total of 19 findings: 14 were identified during the current year FISMA audit and the remaining 5 were identified in prior reports. The most significant findings include the following:

Contingency Planning: The FDIC's IT restoration capabilities were limited, and the agency had not taken timely action to address known limitations with respect to its ability to maintain or restore critical IT systems and applications during a disaster. Therefore, the FDIC could not be sure that it could maintain or restore its mission essential functions during an emergency within applicable timeframes. The FDIC developed a plan to address these contingency planning issues at the close of our audit. The FDIC should also implement appropriate governance over its efforts to strengthen the resiliency and availability of its IT systems and applications.

Information Security Risk Management: The FDIC established the Information Security Risk Advisory Council (the Council) in 2015. However, the Council did not fulfill several of its key responsibilities as defined in FDIC policy. Notably, the Council did not develop information security risk management standards and guidelines, a security risk tolerance level, or a Corporate risk profile.

Enterprise Security Architecture: The FDIC had not established an enterprise security architecture that (i) described the FDIC's current and desired state of security and (ii) defined a plan for transitioning between the two. The lack of an enterprise security architecture increased the risk that the FDIC's information systems would be developed with inconsistent security controls that are costly to maintain.

Technology Obsolescence: The FDIC was using certain software in its server operating environment that was at the end of its useful life and for which the vendor was not providing support to the FDIC. When the vendor does not provide support for software components, adversaries can exploit new weaknesses. This placed portions of the FDIC's IT infrastructure at increased risk of malicious attacks and exploits.

Other areas warranting attention included assessments of outsourced information service providers, finalizing the FDIC's information security strategic plan, patch management, credential scanning, and logging data to the FDIC's security information and event management tool.

We made 18 recommendations to improve the effectiveness of the FDIC's information security program controls and practices. FDIC management concurred with all recommendations.

The full report is available at https://www.fdicoig.gov/sites/default/files/publications/18-001AUD.pdf.

Material Loss Review—First NBC Bank, New Orleans, Louisiana

The Louisiana Office of Financial Institutions (OFI) closed First NBC Bank (First NBC), New Orleans, Louisiana and appointed the FDIC as Receiver on April 28, 2017. First NBC's total assets at closing were $4 billion, and the estimated loss to the DIF was about $997 million. We issued a Material Loss Review of the failure of First NBC, analyzing the causes of First NBC's failure and evaluating the FDIC's supervision of First NBC.

Causes of Failure: First NBC exhibited many of the characteristics of bank failures that we have identified in prior Material Loss Reviews and other reviews of the FDIC's supervision program:

- A dominant official with broad lending authority and limited Board of Directors oversight;
- Rapid growth funded by high-cost deposits; and
- Large lending relationships and concentrations without adequate risk management controls to mitigate the risks.

The bank also developed significant concentrations in trade receivables and complex tax credit investments. The losses the bank realized on its large loan relationships, trade receivables, and tax credit investments severely diminished earnings and depleted capital to a point at which the bank could not recover.

The FDIC's Supervision of First NBC: Between 2006 and 2017, the FDIC and OFI conducted nine full-scope joint safety and soundness examinations and six visitations of First NBC consistent with requirements. However, the FDIC's use of enforcement actions and examination ratings to address First NBC's issues was counter to the agency's forward-looking supervisory approach. That is, although examiners identified repeated risk management weaknesses, they relied too heavily on the bank's financial condition and ability to raise capital in taking supervisory action and assigning management and asset quality ratings.

From 2009 to 2015, First NBC adopted four Board Resolutions to address examination findings and matters requiring board attention. The FDIC's continued reliance on these Board resolutions and matters requiring board attention was largely ineffective in correcting the issues raised. A stronger enforcement action was warranted as early as 2010 based on the bank's risk profile. Instead, the FDIC did not take more formal action at First NBC until late 2016 once the bank's financial condition had deteriorated significantly.

Examiners rated First NBC as satisfactory overall from inception through 2015. Examiners reported repeated concerns with bank management and asset quality but assigned improved ratings to both areas in 2011 and 2014, years when First NBC received significant capital injections. As for the management rating, a more critical assessment of the Chief Executive Officer's influence on the bank's activities was warranted in light of the bank's rapid growth, reliance of volatile funding, and concentrations in risky loans and complex investments.

With respect to asset quality, we could not identify any significant improvements in the bank's adversely classified assets trends during the 2011 and 2014 examinations that would warrant an increase in the asset quality rating. The ratings did not reflect the impact of the loan administration issues identified nor the complex nature of First NBC's assets, which required robust management practices.

We made two recommendations in this report and management concurred.

The full report is available at https://www.fdicoig.gov/sites/default/files/publications/18-002AUD.pdf.

FDIC's Implementation of Consumer Protection Rules Regarding Ability to Repay Mortgages and Compensation for Loan Originators

We issued a report assessing the FDIC's implementation of two rules required by the Dodd-Frank Act. These rules placed new requirements on the banking industry to (1) determine if a consumer has a reasonable ability to repay a mortgage loan and (2) limit loan originator compensation and subject loan originators to new requirements. We reviewed a judgmental sample of 12 FDIC compliance examinations completed in 2016 to assess the FDIC's coverage of these rules and related workpaper documentation.

We found that the FDIC took steps to implement the two rules by incorporating them into its examination program, training its examiners, and communicating the regulatory changes to FDIC-supervised institutions.

The FDIC also tracks financial institution violations of the rules and reasons for those violations. In this regard, we identified regional variances in the number of rule violations in relation to the number of banks examined. However, we could not assess the significance of the variances because the FDIC did not track how many institutions were subject to the rules and how frequently examiners elected to test compliance with the rules.

Our report noted that the FDIC should track such information to better understand the impact the rules have on FDIC-supervised institutions, put the frequency of examination findings and violations into context, determine to what extent examiners are reviewing or electing to not review compliance with the rules, and assess institution compliance and examination coverage trends by FDIC regional office.

We also found that examination workpapers needed improvement. Examiners did not consistently document why they excluded compliance testing for the two rules. In some instances, examiners' workpapers were incomplete, filled out incorrectly, or not stored in accordance with FDIC policy, thus precluding an independent assessment to fully understand the FDIC examinations based on the workpapers alone.

We recommended that the FDIC research potential reasons for the regional variances in the number of rule violations by banks in its six regional offices, track the aggregate number of FDIC-supervised institutions in each region that are subject to the rules and how often examiners test for compliance with the rules, and improve workpaper documentation and retention. The FDIC concurred with our recommendations.

The full report is available at https://www.fdicoig.gov/sites/default/files/publications/18-001EV.pdf.

The FDIC's Compliance with the Digital Accountability and Transparency Act of 2014

The purpose of the Digital Accountability and Transparency Act of 2014 (DATA Act) is to expand the Federal Funding Accountability and Transparency Act of 2006 by increasing the accountability and transparency in federal spending, and for other purposes. We issued the results of our audit of the FDIC's compliance with the DATA Act, in which we assessed (1) the completeness, timeliness, quality, and accuracy of the financial and award data that the FDIC submitted for the second quarter of Fiscal Year 2017 and published on USASpending.gov and (2) the FDIC's implementation and use of the government-wide financial data standards established by the Office of Management and Budget (OMB) and Department of the Treasury.

We concluded that the FDIC could reasonably rely on its source financial system for the DATA Act submission for the second quarter of fiscal year 2017. However, the FDIC incorrectly reported certain data elements obtained from its source financial system when submitting its files. Therefore, although the FDIC's data submission was timely and complete, the data lacked quality and was inaccurate in certain respects. Specifically, we identified three reporting errors:

- The FDIC should have reported a certain value as $1.067 billion and, instead, reported it as zero;
- The FDIC incorrectly overstated another data element by $10.9 million; and
- The FDIC misclassified another data element, which led to an understatement in one object class and an overstatement in another.

We found that the FDIC did not correctly implement all data definitions as evidenced by the errors in the DATA Act submissions. We also identified control weaknesses in FDIC processes that contributed to the reporting inaccuracies. For example, the FDIC should strengthen controls around the submission process, including enhancing written procedures, defining roles and responsibilities of individuals tasked with DATA Act submissions, and establishing adequate segregation of duties and back-up resources. Without such control improvements, the FDIC is at risk for further inaccurate and lesser quality DATA Act submissions.

We made six recommendations to the Director of the Division of Finance to enhance DATA Act procedures, establish a mapping between DATA Act reporting requirements and financial system data elements, strengthen segregation of duties, train DATA Act team members and back-up resources, document quality review of DATA Act submissions, and correct and recertify the DATA Act submission for the second quarter of 2017. Management concurred with our recommendations.

The full report is available at https://www.fdicoig.gov/sites/default/files/publications/18-003AUD.pdf.

Ongoing audit and evaluation reviews at the end of the reporting period were addressing such issues as the FDIC's governance of IT initiatives, controls for preventing and detecting cyber threats, the FDIC's physical security risk management program, the FDIC's implementation of forward-looking supervision, the FDIC's contract oversight management program, and the FDIC's Minority Depository Institution program, among others. These ongoing reviews are also listed on our Website and, when completed, their results will be presented in an upcoming semiannual report.

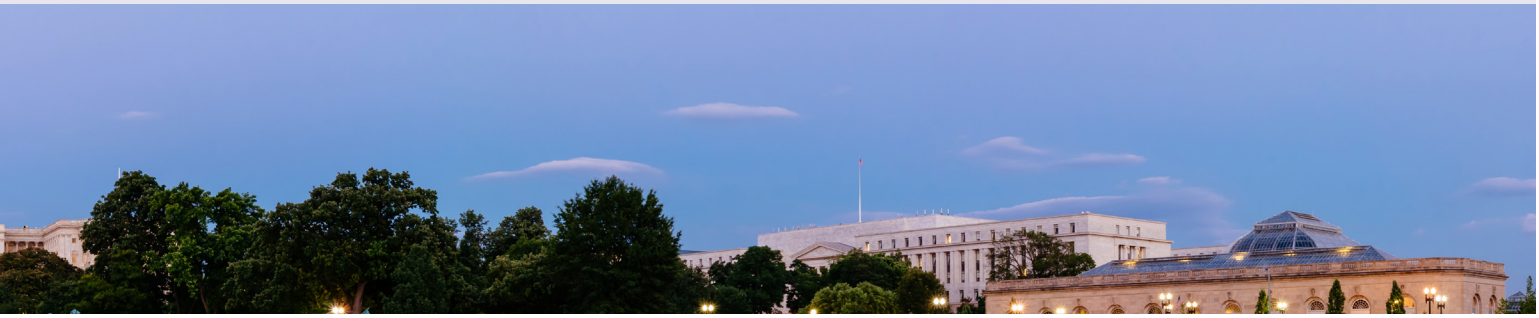
Implementing OIG Recommendations

The OIG continues efforts to ensure that the FDIC implements OIG recommendations in a timely manner and that the FDIC's corrective actions are fully responsive to the OIG's concerns. A recent example of successful perseverance and communications with FDIC management involving a significant information security-related OIG recommendation follows:

In November 2013, we issued an audit report, *Independent Evaluation of the FDIC's Information Security Program—2013* (Report Number AUD-14-002). That report noted that Homeland Security Presidential Directive-20, National Continuity Policy, (HSPD-20) and the Federal Emergency Management Agency's (FEMA) Federal Continuity Directive 1 (FCD) required the FDIC to continuously perform its primary mission essential function (PMEF) and supporting mission essential functions (MEFs) following an emergency event, or resume them within 12 hours of such an event. However, the FDIC had established a recovery time objective for all of its mission-critical IT systems and applications of 72 hours after an emergency declaration or business disruption. We recommended that the FDIC address potential gaps that may exist between the 12-hour minimum timeframe required to restore MEFs following an emergency and the 72-hour recovery time objective for restoring mission-critical IT systems and applications.

FDIC management concurred with the recommendation and indicated that it had recently established a working group to assess and enhance the Corporation's business continuity plans and identify potential gaps in support service recovery capabilities (including IT systems and applications). At the conclusion of this effort, a set of options and recommendations would be presented to FDIC executive management to either accept identified risks or authorize resources necessary to close identified gaps. The FDIC planned to complete all of these actions by December 31, 2014.

As reported in our previous semiannual report, management noted that, subsequent to the issuance of our recommendation, the President had replaced HPSD 20 with Presidential Policy Directive-40, National Continuity Policy, and FEMA had updated its FCDs to clarify continuity requirements imposed on federal agencies. In light of these changes, FDIC management formally notified our office on September 27, 2017, that it had taken alternative corrective action to address the recommendation and provided us with a written plan and other materials describing actions the FDIC had taken and planned. These materials included the results of an analysis performed by the Business Continuity



Working Group (BCWG) to identify the FDIC's MEFs and supporting IT systems and applications. They also included a plan for conducting a comprehensive Business Process Analysis and Business Impact Analysis to validate the Corporation's PMEF and supporting MEFs.

We reviewed the materials and identified a number of concerns. Specifically, the BCWG's analysis was not comprehensive, and portions of the analysis were outdated. Further, a set of options and recommendations to either accept identified risks or authorize resources to close identified gaps had not been presented to executive management. Such a presentation was a key part of the agreed-to corrective action to address our recommendation. We held a series of meetings with FDIC management during 2017 seeking clarification, and requesting additional information regarding management's corrective actions.

On January 25, 2018, we received revised materials containing substantially more responsive information from what we received initially. Of particular note, the materials included a more comprehensive plan to address the recommendation; a new analysis that identified the IT applications and systems supporting the FDIC's MEFs, along with maximum tolerable downtimes; and a case approved by the FDIC's Board of Directors in December 2017 that provided authorization and initial funding to implement a 2-year Backup Data Center Migration project. This project, which the FDIC estimated would cost $55-60 million, involves remediating designated applications, systems, and databases supporting MEFs to ensure they can be recovered within established timeframes and migrating them to the new backup data center.

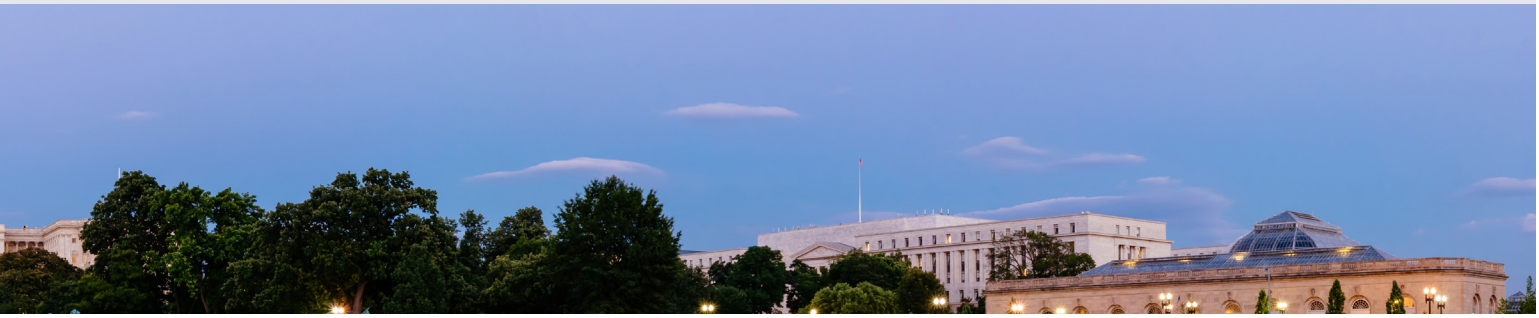
Based on our review of the revised materials and related actions, we concluded that they were responsive to the recommendation in our report. Accordingly, we closed that recommendation.

This example highlights the importance of continued attention to implementing recommendations in order to achieve their intended impact. As required by the IG Act, as amended, our semiannual report includes information on recommendations that remain unimplemented, some of which have been open for periods ranging from about 500 to 900 days as of March 31, 2018.

As indicated in Appendix 1, examples of unimplemented recommendations include, among others, recommendations associated with assessing the effectiveness of the FDIC's supervisory policy and approach related to issues surrounding Operation Choke Point; developing a comprehensive information security strategic plan; and establishing controls to ensure Congressional notifications of major incidents include appropriate context and statements of risk supported by sufficient evidence.

The OIG will continue to monitor progress on these and all other recommendations, and coordinate with the FDIC's Risk Management and Internal Control group in the Division of Finance and with FDIC management to ensure that OIG recommendations are implemented in a timely manner.

(See also Unimplemented Recommendations listing at https://www.fdicig.gov/sites/default/files/attachments/UnimplementedRecommendationListingforWebSite-4-15-18.pdf)



The OIG Issues Top Management and Performance Challenges Document

Under the Reports Consolidation Act of 2000, the OIG identifies the management and performance challenges facing the FDIC and provides its assessment to the Corporation for inclusion in the FDIC's annual performance and accountability report. We identify these challenges based on our experience and observations from our oversight work, reports by other oversight bodies, review of academic and other relevant literature, perspectives from Government agencies and officials, and information from private sector entities. We consider this body of information in light of the operating environment and circumstances, as well as our independent judgment.

In February 2018 we identified seven areas representing the most significant challenges for the FDIC:

- Emerging Cybersecurity Risks at Insured Financial Institutions
- Management of Information Security and Privacy Programs
- Utilizing Threat Information to Mitigate Risk in the Banking Sector
- Readiness for Banking Crises
- Enterprise Risk Management Practices
- Acquisition Management and Oversight
- Measuring Costs and Benefits of FDIC Regulations

The identification of these challenges helps inform our audit and evaluation work, as shown in the following summaries of each of these challenges.

Emerging Cybersecurity Risks at Insured Financial Institutions

Cybersecurity is a significant concern for the banking industry because of the industry's use of and reliance on technology – not only in bank operations, but also as an interface with customers. It has become one of the most critical challenges facing the financial services sector due to the frequency and increasing sophistication of cyber-attacks. The FDIC has a significant financial interest in mitigating cybersecurity risks at insured banks. If a bank fails, the FDIC will need to step in and may have to fund the losses from the DIF.

Given the significance of cybersecurity risk to U.S. financial institutions, FDIC IT examinations are an important tool to identify weaknesses and vulnerabilities in FDIC-supervised institutions. FDIC IT examinations assess the management of IT risks, including cybersecurity, at FDIC-supervised institutions and at select third-party technology service providers. In September 2016, the FDIC implemented a new Information Technology Risk Examination (InTREx) program for financial institutions. We will be conducting an audit that will assess the InTREx program.

A key challenge associated with IT examinations is ensuring that the FDIC has the right number of examiners with appropriate skills, training, and experience to match institution IT complexity. We are planning to conduct an evaluation of the FDIC's approach to examiner staffing, including IT examination resources.

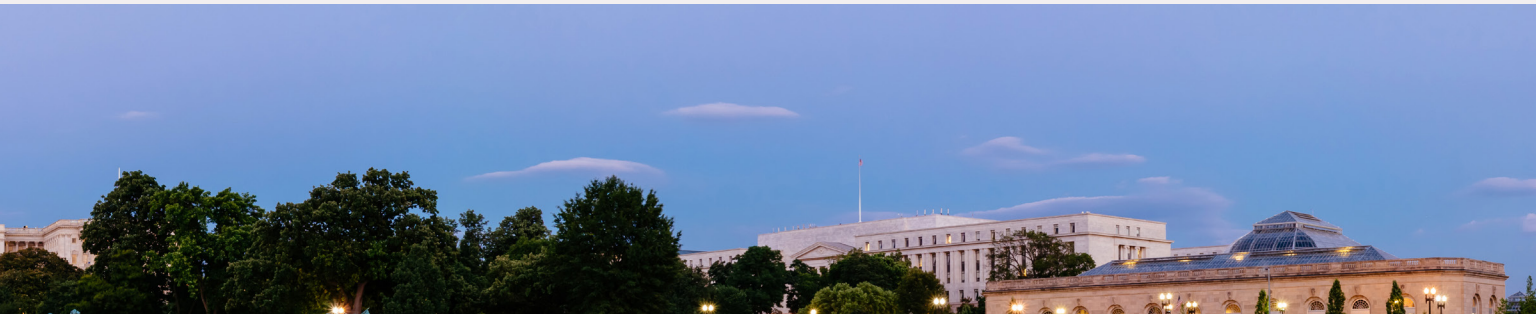
Management of Information Security and Privacy Programs

Safeguarding computer systems from cyber threats is a high risk across the Federal government and has been a long-standing concern. Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions that can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks.

The FDIC uses IT systems and applications to perform its goals regarding safety and soundness for financial institutions, consumer protection, managing the DIF, and resolution and receivership of failed institutions. These systems and applications hold significant amounts of sensitive data. For example, the FDIC's Failed Bank Data System contains more than 2,500 terabytes of sensitive information from more than 500 bank failures. In addition, FDIC systems contain substantial amounts of personally identifiable information (PII), including, for example, names, Social Security Numbers, and addresses related to bank officials, depositors, and borrowers at FDIC-insured institutions and failed banks, and FDIC employees. Of the FDIC's 261 system applications, 151 applications required Privacy Impact Assessments because they collect, maintain, or disseminate PII.

Over time, the FDIC has experienced a number of cybersecurity incidents. In August 2011, the FDIC began to experience a sophisticated, targeted attack on its network known as an Advanced Persistent Threat (APT). The attacker behind the APT penetrated more than 90 workstations or servers within the FDIC's network over a significant period of time, including computers used by the former Chairman and other senior FDIC officials. In late 2015 and early 2016, the FDIC was again impacted by significant cybersecurity incidents. In these cases, the FDIC detected seven data breaches as departing employees improperly took sensitive information shortly before leaving the FDIC. The FDIC initially estimated that this sensitive information included the PII of approximately 200,000 individual bank customers associated with approximately 380 financial institutions, as well as the proprietary and sensitive data of financial institutions; however, the FDIC later revised the number of affected individuals to 121,633.

We will continue to perform annual reviews of the FDIC's information security program and practices pursuant to FISMA. We also have work planned in specific areas of the FDIC's information security program.



Utilizing Threat Information to Mitigate Risk in the Banking Sector

The banking sector is vital to public confidence and the nation's safety, prosperity, and well-being. According to Presidential Policy Directive 21, the national preparedness systems must be integrated to secure critical infrastructure, withstand all hazards, and rapidly recover from disasters. Both the Departments of the Treasury and Homeland Security recognized that sharing timely and actionable information is critical to managing risk. In its Annual Report for 2017, the Financial Stability Oversight Council (FSOC) recognized that there was a body of relevant information held by the government that was classified as national security information and must maintain its classification restrictions. Nevertheless, the FSOC encouraged agencies to "balance the need to keep information secure with efforts to share information with industry to enhance cybersecurity resilience."

The financial sector also faces threats based on new technology, such as the rapid growth of the virtual currency markets. At present, the United States does not have a direct and comprehensive program to conduct oversight of the virtual currency markets. Among the challenges identified are the potential for illicit use and connection to criminal activity, legal and supervisory challenges, and integration with and risk to financial institutions. Further, physical threats, such as natural disasters, terrorist attacks, and floods have significant potential to disrupt the financial system. Threats to financial institutions also may come from, or be exacerbated by, their dependence on other critical infrastructure services, such as energy, electricity, communication, and transportation.

Threat information held by the U.S. Government is critical to financial institutions and their service providers. As discussed in FDIC's *Supervisory Insights, A Framework for Cybersecurity*, "financial institutions should have a program for gathering, analyzing, understanding, and sharing information about vulnerabilities to arrive at 'actionable intelligence.'" In order to secure their systems, institutions must have timely and actionable threat information. The financial crisis provided an example of how the default of poorly underwritten mortgages at one bank rippled through the financial system to other banks, brokerages, and insurance companies through asset-backed securities and collateralized debt obligations backed by those mortgages.

Threat information held by the U.S. Government is also critical to FDIC examiners. Examiners should have access to relevant threat information and an understanding of the current threat level and types of threats, in order to focus examinations and prioritize areas for supervisory attention. We intend to perform work that assesses whether examiner personnel and financial institutions have access to threat information that enables them to mitigate risks in their respective roles.

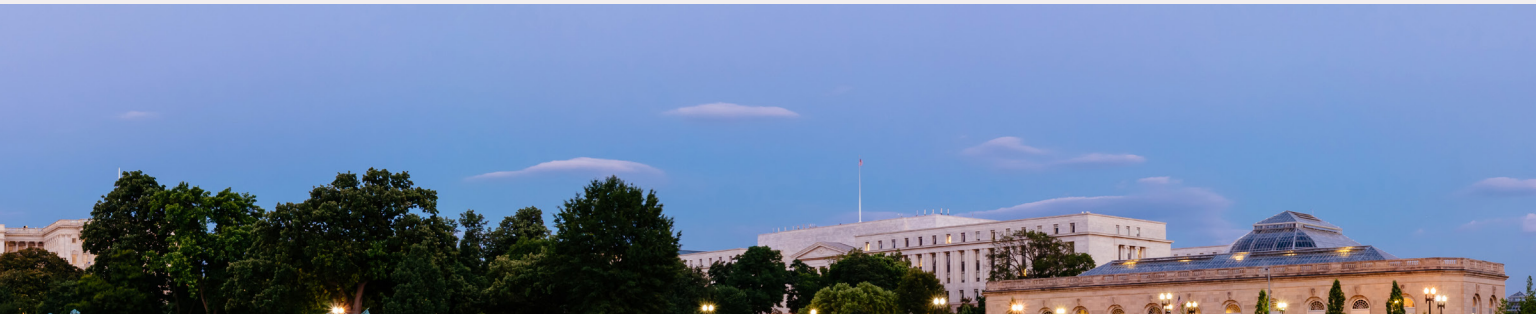
Readiness for Banking Crises

As the financial crisis that began in 2008 unfolded, it challenged every aspect of the FDIC's operations, not only because of its severity, but also because of the speed with which problems unfolded. New vulnerabilities have emerged since the previous financial crisis, and they represent key threats to the financial system. There have been several changes in the financial markets since the crisis – for example: the increased use of automated trading systems, increased speed of executing financial transactions, and a wider variety of trading venues and liquidity providers.

The FDIC must ensure that it has adequate plans in place to address disruptions to the banking system, irrespective of their cause, nature, magnitude, or scope. Further, its plans should be current and up-to-date, and incorporate lessons learned from past crises and the related bank failures. In addition, the plans should contemplate the present and foreseeable state of the banking and financial services sector, as banking industry practices and technologies continue to evolve. Proper authorities, tools, and mechanisms are also needed to address failing institutions in the next crisis.

As noted earlier, when resolving a failing or failed bank, the FDIC uses the automated tool called CAS to identify a depositor's insured and uninsured funds. When planning for the development of the CAS program, the FDIC expected that CAS could make insurance determinations for an institution of any size, up to 5 million deposit accounts; however, over time, the FDIC recognized the challenges of inconsistent and incomplete data at institutions.

Determining the right number and skillsets of permanent staff needed to carry out and support the FDIC's program areas is a fundamental challenge. The FDIC has developed staffing models and operational readiness frameworks to be prepared for both current workload and to deploy resources rapidly in the case of a crisis. A proper infrastructure is also critical in order to address the administrative functions of the agency—such as hiring, contracting, and legal support—in a timely manner. We have work underway to address the FDIC's readiness to respond to any type of crisis.



Enterprise Risk Management Practices

Enterprise Risk Management (ERM) is a decision-making tool that assists federal leaders in anticipating and managing risks at an agency, and helps to consider and compare multiple risks and how they present challenges and opportunities when viewed across the organization. According to Office of Management and Budget (OMB) guidance, ERM is beneficial because it addresses a fundamental organizational issue: the need for information about major risks to flow both vertically (i.e., up and down the organization) and horizontally (i.e., across its organizational units) to improve the quality of decision-making. When implemented effectively, ERM seeks to open channels of communication, so that managers have access to the information they need to make sound decisions. ERM can also help executives recognize how risks interact (i.e., how one risk can exacerbate or offset another risk). Further, ERM examines the interaction of risk treatments (actions taken to address a risk), such as acceptance or avoidance. We intend to conduct an evaluation of the effectiveness of the FDIC ERM Program.

Acquisition Management and Oversight

Agencies must properly oversee contractor performance and identify any deficiencies, as well ensure appropriate verification of expenditures. Over the last 10 years (2008 through 2017), the FDIC awarded more than 12,600 contracts totaling nearly $11.2 billion.

Contracting Officers are responsible for ensuring the performance of all actions necessary for efficient and effective contracting, compliance with contract terms, and protection of the FDIC's interests in all of its contractual relationships. In addition, FDIC program offices develop contract requirements, and program office Oversight Managers and Technical Monitors oversee the contractor's performance and technical work. Oversight management involves monitoring contract expenses and ensuring that the contractor delivers the required goods or performs the work according to the delivery schedule in the contract.

In our work, we have noted several shortcomings in contractor oversight, which can lead to delays and cost overruns. In our report entitled *The FDIC's Failed Bank Data Services Project* (March 2017), we reviewed a 10-year, $295 million project related to the transition of the management of failed financial institution data from one contractor to another. Our review focused on transition costs of approximately $24.4 million. The audit concluded that transition milestones were not met, resulting in a one year delay. Further, transition costs, while less than projected in the approval, were greater than the initial estimates

at contract inception by $14.5 million. We concluded that the reasons for the increase were that the FDIC faced challenges related to defining contract requirements, coordinating contracting and program office personnel, and establishing implementation milestones.

We have initiated an evaluation to review FDIC's current contract oversight management program.

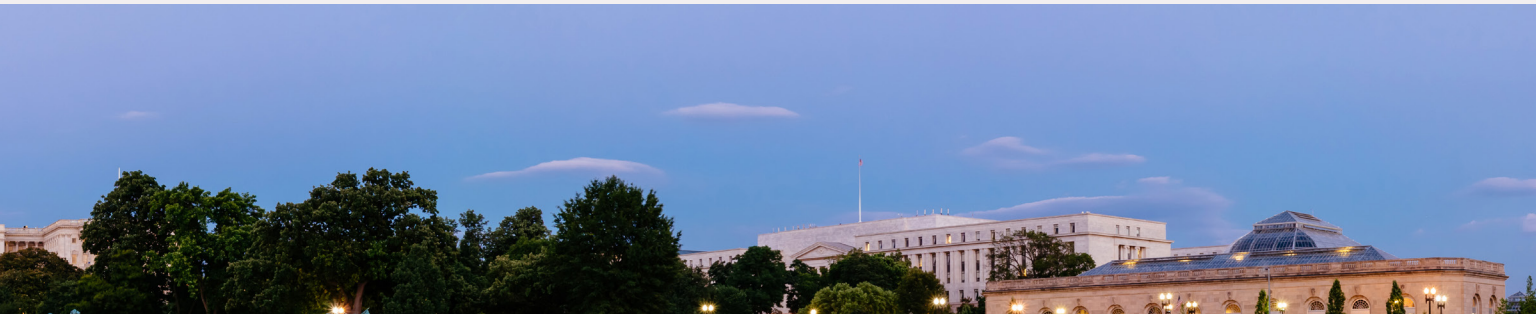
Measuring Costs and Benefits of FDIC Regulations

In June 2017, the Department of the Treasury issued a report, *A Financial System That Creates Economic Opportunities*, examining costs relating to compliance with regulations imposed on banks. This report recommended that financial regulatory agencies should conduct rigorous cost-benefit analysis and make greater use of proposed rulemaking to solicit public comment. The FDIC generally conducts this analysis on its own initiative for proposed rules.

The Congressional Research Service (CRS) recognized that the use of cost-benefit analysis may improve the quality and effectiveness of federal rules and minimize burden in its *Cost-Benefit and Other Analysis Requirements in the Rulemaking Process* (2014). However, the report notes that performing cost-benefit analysis can be a difficult and time-consuming process, and it produces uncertain results because it involves making assumptions about future outcomes. The CRS also noted that cost-benefit analysis "for financial regulation is particularly challenging, due largely to the high degree of uncertainty over precise regulatory costs and outcomes." The report identified three challenges to making accurate cost-benefit analysis: (1) behavioral changes of people as they adapt to a new regulation, (2) quantification that must overcome uncertainty over the causal relationship between the regulation and outcomes, and (3) monetization, which is difficult for outcomes that do not have easily discernable monetary values.

The FDIC faces challenges with proper data collection and lack of available information with respect to measuring costs and identifying benefits for a particular rule, and we will continue to monitor the FDIC's efforts in this area.

The full report on the Top Management and Performance Challenges is available at https://www.fdicig.gov/sites/default/files/attachments/2017TMPC_Final.pdf.



Investigations

The FDIC OIG investigates significant matters of wrongdoing and misconduct relating to FDIC employees, contractors, and institutions. We do so by:

- Conducting thorough investigations consistent with the highest professional standards and best practices.
- Working on important and relevant cases that have the greatest impact.
- Building and maintaining relations with FDIC and law enforcement partners to be involved in leading banking cases.
- Enhancing information flow to proactively identify law enforcement initiatives and cases.
- Recognizing and adapting to emerging trends in the financial sector.
- Developing expertise to shape the character of the OIG's investigative component and its Field Offices.

The cases discussed below are illustrative of some of the OIG's investigative success during the reporting period. Special agents in headquarters, regional offices, and the OIG's Electronic Crimes Unit are responsible for these results. These cases reflect the cooperative efforts of OIG investigators, FDIC divisions and offices, other OIGs, U.S. Attorneys' Offices (USAO), and others in the law enforcement community throughout the country, as illustrated at the end of this section of our report. These working partnerships contribute to ensuring the continued safety and soundness of the nation's banks and help ensure integrity in the FDIC's programs and activities.

HSBC Holdings Plc Agrees to Pay More Than $100 Million to Resolve Fraud Charges

In January 2018, HSBC Holdings plc, the parent company of HSBC Bank plc, entered into a deferred prosecution agreement and agreed to pay a $63.1 million criminal penalty and $38.4 million in disgorgement and restitution to resolve charges that it engaged in a multi-million dollar front-running scheme to defraud two bank clients.

According to HSBC's admissions, on two separate occasions in 2010 and 2011, traders on its foreign exchange desk misused confidential information from clients that had hired HSBC to execute multi-billion dollar foreign exchange (FX) transactions involving the British Pound Sterling. After executing confidentiality agreements with its clients that required the bank to keep the details of their planned transactions confidential, traders on HSBC's foreign exchange desk transacted in the Pound Sterling for the traders' and HSBC's own benefit. HSBC traders then caused the clients' large transactions to be executed in a manner designed to drive the price of the Pound Sterling in a direction that benefited HSBC and harmed their clients. HSBC also made misrepresentations to one of the clients to conceal the self-serving nature of its actions. In total, HSBC admitted to making profits of approximately $38.4 million on the first transaction in March 2010, and approximately $8 million on the transaction in December 2011.

HSBC agreed to continue to cooperate with the Department of Justice (DOJ) and with foreign authorities in any ongoing investigations and prosecutions relating to the conduct and enhance its compliance program. In addition to the criminal penalty, the $38.4 million in disgorgement and restitution was based on HSBC's conduct related to one of the two victim companies. HSBC previously settled with the other victim company for approximately $8 million, which the Department of Justice credited as full restitution for that company.

Source: *Fraud Section, Criminal Division, DOJ.*
Responsible Agencies: *This was a joint investigation by the FDIC OIG and Federal Bureau of Investigation's (FBI) Washington Field Office. The case was prosecuted by the DOJ Criminal Division's Fraud Section. The Criminal Division's Office of International Affairs and the USAO for the Eastern District of New York provided significant support.*

BNP Paribas USA Inc. Pleads Guilty to Antitrust Conspiracy

On January 25, 2018, BNP Paribas USA Inc. (BNPP USA), a subsidiary of BNP Paribas S.A., pleaded guilty to participating in a price-fixing conspiracy in the foreign currency exchange market. According to the one-count information, between September 2011 and July 2013, BNPP USA conspired to suppress and eliminate competition by fixing prices in Central and Eastern European, Middle Eastern, and African currencies, in violation of the Sherman Act, 15 U.S.C. §1. The conspiracy involved manipulation of prices on an electronic FX trading platform through the creation of non-bona fide trades, coordination of bids and offers on that platform, and agreements on currency prices to quote specific customers, among other conduct.

As part of its sentence, BNPP USA has agreed to pay a criminal fine of $90 million. Since the illegal activity, the bank has made substantial efforts relating to compliance and remediation and has agreed to cooperate with the government's ongoing criminal investigation into the FX market and report relevant information to the government.

BNPP USA is the sixth major bank to plead guilty as a result of the Department of Justice's ongoing investigation into antitrust and fraud crimes in the FX market. On May 20, 2015, four major banks – Citicorp, JPMorgan Chase & Co., Barclays PLC and The Royal Bank of Scotland plc – pleaded guilty at the parent level and agreed to pay collectively more than $2.5 billion in criminal fines for their participation in an antitrust conspiracy to manipulate the price of U.S. dollars and euros exchanged in the FX market. A fifth bank, UBS AG, pleaded guilty to manipulating the London Interbank Offered Rate (LIBOR) and other benchmark interest rates and agreed to pay a $203 million criminal penalty, after breaching its December 2012 non-prosecution agreement resolving the LIBOR investigation.

Source: *Antitrust Division, DOJ.*
Responsible Agencies: *This is a joint investigation being conducted by the FDIC OIG, the DOJ Antitrust Division's New York Office, and the FBI's Washington Field Office, with substantial assistance from the Department of Justice Criminal Division's Fraud Section.*

Former Global Head of HSBC's Foreign Exchange Cash-Trading Found Guilty of Orchestrating Multimillion-Dollar Front-Running Scheme

On October 23, 2017, the former head of global FX cash trading at HSBC Bank plc was convicted at trial of one count of conspiracy to commit wire fraud and eight counts of wire fraud for his role in defrauding two bank clients through a multi-million dollar front-running scheme.

HSBC was selected to execute an FX transaction related to a planned sale of one of a client's foreign subsidiaries, which would require converting approximately $3.5 billion in sales proceeds into British Pounds Sterling. HSBC's agreement with the client required the bank to keep the details of the planned transaction confidential.

Instead, the former bank executive and other traders acting under the former bank executive's direction purchased Pounds Sterling for their own benefit in their HSBC proprietary accounts. The former bank executive then caused the $3.5 billion foreign exchange transaction to be executed in a manner that was designed to drive up the price of the Pounds Sterling, generating $7.3 million in profits for their proprietary positions and HSBC at the expense of their client.

Source: *Fraud Section, Criminal Division, DOJ.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG and FBI's Washington Field Office. The case is being prosecuted by the DOJ Criminal Division's Fraud Section and the USAO for the Eastern District of New York.*

Former Financial Advisor Sentenced to Two Years in Prison for Defrauding Client in Private Investment Scheme

On February 23, 2018, a former financial advisor at an Illinois bank was sentenced to two years in prison for falsely representing a private investment scheme to a customer that resulted in the client losing money. The former financial advisor was also ordered to pay $100,000 in restitution.

On October 24, 2017, the former financial advisor entered pleas of guilty to wire fraud and money laundering. He admitted that in early 2012, he falsely represented to a bank customer that he had a private investment opportunity that would provide a 10 percent rate of return. The customer gave him $100,000 to invest. Instead of investing the money, the former financial advisor deposited the money into a personal bank account and used it for his personal benefit, including paying off personal debts.

Source: *Local defense attorney.*
Responsible Agencies: *The FDIC OIG conducted this investigation. The case was prosecuted by the USAO for the Central District of Illinois.*

Former Arkansas Lawmaker Pleads Guilty to $4 Million Charity Scheme

On February 12, 2018, a former Arkansas state representative pleaded guilty to one count of conspiracy for his role in a conspiracy to embezzle more than $4 million from a Springfield, Missouri-based health care charity. During some of the time he served as a lawmaker, the former state representative also worked as a regional director for Preferred Family Healthcare, Inc. a non-profit charity headquartered in Springfield. He also served on the charity's Board of Directors and worked as a lobbyist.

The former state representative admitted that he conspired with several executives of Preferred Family Healthcare to use the charity's funds for unlawful political contributions; for excessive, unreported lobbying; and to financially benefit themselves. For example, conspirators caused personal contributions to elected officials and their political campaigns to be reimbursed by the charity. Such indirect contributions are prohibited by law just as if the payments had been made by the charity directly.

The former state representative received a total of at least $387,501 from a lobbying firm and at least $63,000 in kickbacks as a result of his participation in the conspiracy. Under the terms of the plea agreement, he must forfeit his gain from the conspiracy to the government. In order to provide a veneer of legitimacy for the kickbacks paid to themselves and others, and to disguise the nature and source of the payments, conspirators caused the payments to be described in the records as business expenses, such as "consulting" and "training" services, and executed sham "consulting agreements."

Part of the scheme involved $3 million in payments and kickbacks with a company identified as Lobbying Firm A, an Arkansas firm owned and operated by a co-conspirator that also employed the former state representative as a lobbyist. The payments were falsely classified as consulting expenses when in fact they were for lobbying and advocacy services, including soliciting the assistance of elected and appointed officials regarding legislative issues that impacted the charity, in particular matters involving the charity, and in steering grants and other sources of funding to the charity.

The scheme also involved another nearly $1 million in payments to a Pennsylvania-based lobbying firm for illegal lobbying and political activity on behalf of the charity. According to court documents, the firm occasionally suggested that charity executives make political contributions to legislators they wanted to influence and/or thank for assistance. From time to time, the lobbying firm's owner delivered their contribution checks directly to legislators in Washington D.C., to increase the impact of the donations.

Under federal statutes, the former state representative is subject to a sentence of up to five years in federal prison without parole.

Source: *USAO.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG; Internal Revenue Service-Criminal Investigation (IRS-CI); FBI; and the OIGs of the Departments of Labor, Health and Human Services, Housing and Urban Development, and Veterans Affairs. The case is being prosecuted by the DOJ Criminal Division's Fraud Section and the USAO for the Western District of Missouri, with assistance from the Western District of Arkansas, the Eastern District of Arkansas, the Eastern District of Pennsylvania, and the Public Integrity Section of the DOJ.*

Florida Couple Pleads Guilty to Structuring

On February 12, 2018, a Florida couple pleaded guilty to conspiracy to structure financial transactions to evade reporting requirements. According to the plea agreement, the couple travelled across Florida to banks in Jacksonville, Orlando, and Tampa to structure deposits and withdrawals so that each transaction was below the $10,000 threshold that would have required a Currency Transaction Report.

The couple structured deposits by making individual deposits of less than $10,000 at different credit unions or different branches of the same credit union. The couple structured withdrawals by writing and cashing checks payable to themselves. The couple wrote and cashed over 1,750 checks to themselves over about a year – meaning an average of nearly 5 checks per day. In less than a year, the couple structured more than $4.5 million.

The couple faces up to 5 years in federal prison.

Source: *Department of the Treasury OIG.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, the Treasury OIG, IRS-CI, the Social Security Administration OIG, the U.S. Secret Service, and the Marion County Sheriff's Office. The case is being prosecuted by the USAO for the Middle District of Florida.*

Sacramento-Area Real Estate Developer Pleads Guilty to $22 Million Fraud

On January 12, 2018, a Sacramento-area real estate developer pleaded guilty to wire fraud, bank fraud, and making false statements to a federally insured financial institution.

According to court documents, the developer, a Sacramento-area commercial real estate developer and restauranteur, came up with a scheme to fraudulently purchase land that he planned to develop. The developer would submit altered purchase contracts to the banks from which he was seeking loans that greatly inflated the purchase price of the property, which caused the banks to loan him more money.

The developer also conspired with a title company employee in order to minimize or avoid paying down payments for the properties. The title company employee would delay depositing the developer's down payment check until after escrow closed. Once escrow closed, the title company employee disbursed funds from the title company's escrow trust account to the developer's company, which then used those funds to clear the down payment and cover other costs. This made it seem like the developer was making a substantial down payment when the down payment was actually made from loan proceeds.

The developer's entire scheme, involving at least six properties in the Sacramento area, resulted in a loss to various financial institutions of over $22 million. He faces a maximum statutory penalty of thirty years in prison on each count and a $1 million fine.

Source: *FDIC OIG.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, FBI, and IRS-CI. The case is being prosecuted by the USAO for the Eastern District of California.*

Former Chief Executive Officer (CEO) and Former Chief Loan Officer of Failed Sonoma Valley Bank Convicted of Bank Fraud

On December 18, 2017, the former CEO and former Chief Loan Officer of the failed Sonoma Valley Bank were convicted at trial of conspiracy, bank fraud, money laundering, falsifying bank records, lying to bank regulators, and other crimes. An attorney for a real estate developer (who had been indicted on these charges before his death) was also convicted of conspiracy, bank fraud, attempted obstruction of justice, and other offenses.

Between 2004 and 2010, Sonoma Valley Bank loaned the developer and the individuals and entities he controlled in excess of $35 million, nearly $25 million more than the legal lending limit set by the bank's regulators. To conceal this high concentration of lending, the former CEO and Chief Loan Officer recommended that the bank approve multi-million dollar loans to straw borrowers. The former Chief Loan Officer was also convicted of taking a $50,000 bribe from the developer for some of the loans made to the straw borrowers.

The former CEO and Chief Loan Officer also conspired with the developer's attorney to mislead Sonoma Valley Bank into lending millions more to the developer, again in the name of a straw borrower, so the developer could illegally buy back, at a steep discount, a debt he owed to IndyMac Bank, which had failed and been taken over by the FDIC. FDIC rules specifically prohibited delinquent borrowers, like the developer, from purchasing their own notes at auction.

The former CEO and Chief Loan Officer were convicted of making false statements to Sonoma Valley Bank's regulators, the FDIC, and the California Department of Financial Institutions about the true nature and extent of the bank's lending to the developer and the persons and entities he controlled.

The failure of Sonoma Valley Bank caused in excess of $20 million in losses to taxpayers, approximately $11.47 million to the FDIC, and $8.65 million to the Troubled Asset Relief Program.

Source: *FDIC's Division of Resolutions and Receiverships.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, Special Inspector General for the Troubled Asset Relief Program, and the Federal Housing Finance Agency OIG, with the assistance of the Marin County Sheriff's Office, the Sonoma County Sheriff's Office, and the Santa Rosa Police Department. The case is being prosecuted by the USAO for the Northern District of California.*

Strong Partnerships with Law Enforcement Colleagues

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

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

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

Keeping Current with Criminal Activities Nationwide

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

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; New York Identity Theft Task Force; Newark Suspicious Activity Report (SAR) Review Task Force; Philadelphia SAR Review Team; El Dorado Task Force - New York/ New Jersey High Intensity Drug Trafficking Area; South Jersey Bankers Association; Eastern District of New York SAR Meeting Group; New York External Fraud Group; Philadelphia Financial Exploitation Prevention Task Force; Bergen County New Jersey Financial Crimes Association; Long Island Fraud and Forgery Association; Connecticut USAO Bank Secrecy Act Working Group; Connecticut U.S. Secret Service Financial Crimes Task Force; South Jersey SAR Task Force; Pennsylvania Electronic Crimes Task Force; National Crime Prevention Council, Philadelphia Chapter; Northern Virginia Financial Initiative SAR Review Team; International Association of Financial Crimes Investigators.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force, 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, Richmond Tidewater Financial Crimes 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.
Chicago Region	Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Central District of Illinois Financial Fraud Working Group; Northern District of Illinois SAR Review Team; Southern District of Illinois SAR Review Team; Cook County Region Organized Crime Organization; Financial Investigative Team, Milwaukee, Wisconsin; Milwaukee Mortgage Fraud Task Force; Madison, Wisconsin, SAR Review Team; Indiana Bank Fraud Working Group; Northern District of Indiana SAR Review Team; Southern District of Indiana SAR Review Team; FBI Louisville Financial Crime Task Force; U.S. Secret Service Louisville Electronic Crimes Task Force; Western District of Kentucky SAR Review Team; Eastern District of Kentucky SAR Review Team.
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, Orange County Financial Crimes Task Force-Central District of California, High Intensity Financial Crime Area Task Force, Northern Nevada Financial Crimes Task Force.
Dallas Region	SAR Review Team for Northern District of Mississippi, SAR Review Team for Southern District of Mississippi, Oklahoma City Financial Crimes SAR Review Working Group, Austin SAR Review Working Group, Hurricane Harvey Working Group.
Electronic Crimes Unit	Washington Metro Electronic Crimes 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.

Other Key Priorities

In addition to the audits, evaluations, and investigations conducted during the reporting period, our Office has emphasized other key initiatives. Specifically, in keeping with our Guiding Principles, we have focused on relations with partners and stakeholders, resource administration, and leadership and teamwork. A brief listing of some of our efforts in these areas follows.

Strengthening relations with partners and stakeholders.

- Communicated with the Chairman, Vice Chairman, other FDIC Board Members, the Chief Financial Officer, and other senior FDIC officials through the IG's and senior OIG leadership's regularly scheduled meetings with them and through other forums.
- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.
- Coordinated with the FDIC Vice Chairman, in his capacity as Chairman of the FDIC Audit Committee, to provide status briefings and present the results of completed audits, evaluations, and related matters for his and other Committee members' consideration.
- Coordinated with DOJ and U.S. Attorneys' Offices throughout the country in the issuance of press releases announcing results of cases with FDIC OIG involvement and routinely informed the Chairman and Vice Chairman of such releases.
- Attended FDIC Board Meetings and certain other senior-level management meetings to monitor or discuss emerging risks at the Corporation and tailor OIG work accordingly.
- Maintained Congressional working relationships by communicating with various Committee staff on issues of interest to them; providing them our semiannual report to the Congress; notifying interested Congressional parties regarding the OIG's completed audit and evaluation work; monitoring FDIC-related hearings on issues of concern to various oversight Committees; and coordinating with the Corporation's Office of Legislative Affairs on issues of mutual interest.
- Met with Congressional majority and minority staff from the Senate Banking, Senate Homeland Security and Governmental Affairs, and House Financial Services Committees to discuss recently issued OIG reports, including the *Top Management and Performance Challenges Facing the FDIC*.

- Maintained the OIG Hotline to field complaints and other inquiries from the public and other stakeholders. The OIG's Whistleblower Protection Ombudsperson also helped educate FDIC employees who had made or were contemplating making a protected disclosure as to their rights and remedies against retaliation for such protected disclosures.
- Supported the IG community by attending monthly Council of the Inspectors General on Integrity and Efficiency (CIGIE) meetings; and other meetings such as those of the CIGIE Audit Committee, the Professional Development Committee, Legislative Committee, Assistant Inspectors General for Investigations, Council of Counsels to the IGs, Federal Audit Executive Council; responding to multiple requests for information on IG community issues of common concern; and commenting on various legislative matters through CIGIE's Legislative Committee.
- Participated on the Council of Inspectors General on Financial Oversight (CIGFO), as established by the Dodd-Frank Act, and coordinated with the IGs on that council. This Council facilitates sharing of information among CIGFO member Inspectors General and discusses ongoing work of each member IG as it relates to the broader financial sector and ways to improve financial oversight.
- Coordinated with the Government Accountability Office (GAO) on ongoing efforts related to the annual financial statement audit of the FDIC and on other GAO work of mutual interest, such as GAO's work on IG vacancies.
- Coordinated with OMB on the OIG's budget submission for FY 2019 and other matters requiring OIG attention.
- Worked closely with representatives of the DOJ, including Main Justice Department, the FBI, and U.S. Attorneys' Offices, to coordinate our criminal investigative work and pursue matters of mutual interest. We also joined law enforcement partners in numerous financial, mortgage, and cyber fraud-related working groups nationwide.
- Promoted transparency to keep the American public informed through three main means: the FDIC OIG Website to include, for example, summaries of completed work, listings of ongoing work, and information on unimplemented recommendations; Twitter communications to immediately disseminate news of report and press release issuances and other news of note; and participation in the IG community's oversight.gov Website, which enables users to access, sort, and search thousands of previously-issued IG reports and other oversight areas of interest.

Administering resources prudently, safely, securely, and efficiently.

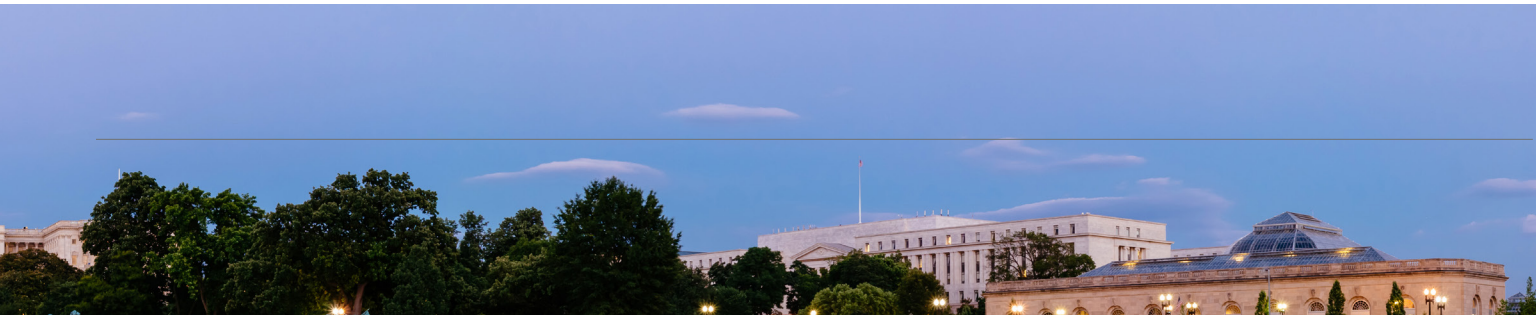
- Established the OIG's Office of Information Technology to coordinate a strategic approach to facilitate the integration of technology in OIG processes. This group is responsible for the OIG's enterprise architecture, IT governance, and related policies and procedures.
- Relied on OIG Counsel's Office to ensure the office complied with legal and ethical standards, rules, principles, and guidelines; provide legal advice and counsel to teams conducting audits and evaluations; and support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.
- Continued to review and update a number of OIG internal policies related to audit, evaluation, investigation, management operations, and administrative processes of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the office.
- 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.
- 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 a Senior Advisor to the IG, Human Resources Specialist, IT Office Director, and Special Agent in Charge of the OIG's Electronic Crimes Unit.
- Prepared a budget justification document for OMB and for the FDIC OIG's Senate and House Appropriations Committees to support the FDIC Chairman's approval of a fiscal year 2019 budget of $43 million to fund 144 authorized positions.
- Oversaw contracts to qualified firms to provide audit, evaluation, investigation, and other services to the OIG to provide support and enhance the quality of our work and the breadth of our expertise as we conduct audits, evaluations, and investigations, and to complement other OIG functions and closely monitored contractor performance.

- Continued to closely monitor, track, and control OIG spending, particularly in light of the Continuing Resolution under which the OIG operated for FY 2018.
- Explored options for the OIG's email to the Cloud initiative and continued to work with contracted resources for business process analysis services to evaluate the OIG's Electronic Crimes Unit lab and make needed enhancements.

Exercising leadership skills and promoting teamwork.

- Held an OIG-wide conference, *One OIG: From Principles to Practice*, featuring speakers from the OIG, FDIC management, IG community, and Office of Special Counsel, to reiterate the Office's guiding principles and the mission and vision of the FDIC OIG.
- Continued biweekly OIG senior leadership meetings to affirm the OIG's unified commitment to the FDIC IG mission and to strengthen working relationships among all FDIC OIG offices.
- Developed strategic plans for individual OIG offices, taking into consideration current resources, skills, accomplishments, challenges, and goals for the future. These individual plans form the basis for budget requests, promote further understanding of component offices, and help ensure that office-wide efforts in pursuit of the OIG mission are efficient, effective, and economical.
- Supported efforts of the IG Advisory Council, a cross-cutting group of OIG staff whose mission is to provide leadership toward "One OIG" by promoting collaboration and innovation.
- Leveraged the OIG's Data Analytics capabilities to improve the overall efficiency and effectiveness of the OIG's audit and evaluation assignments; identify and reduce fraud, waste, and abuse; and facilitate OIG decision-making.
- Kept OIG staff informed of office priorities and key activities through regular meetings among staff and management, bi-weekly updates from senior management meetings, and issuance of OIG newsletters. Conducted two POWER Lunch and Learn sessions–one relating to the OIG's successful Banamex USA investigation and the other with FDIC Chairman Gruenberg–and held other Office events to promote the concept of "One OIG."

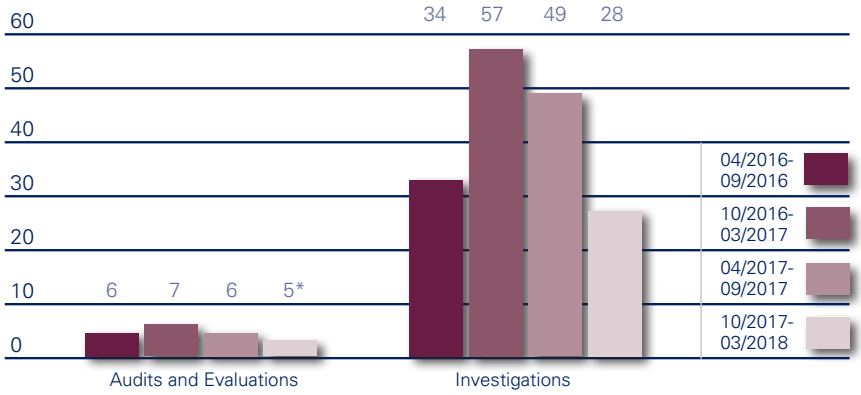
- Formed working groups to leverage skills and knowledge in addressing office projects—for example, an audit and evaluation team addressing process improvement and alternative reporting options and an interdisciplinary team formed to address office-wide information security-related issues and solutions.
- Enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities.
- Carried out monthly coordination meetings for audit, evaluation, and investigation leadership to better communicate, coordinate, and maximize the effectiveness of ongoing work.
- Acknowledged individual and group accomplishments through an ongoing awards and recognition program, and solicited nominations for three OIG special awards to recognize outstanding efforts: Distinguished Professional Award, Spirit of the OIG Award, and IG Award for Excellence. Also solicited nominations of OIG individuals and teams for CIGIE awards.
- 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.



Cumulative Results
(2-year period)

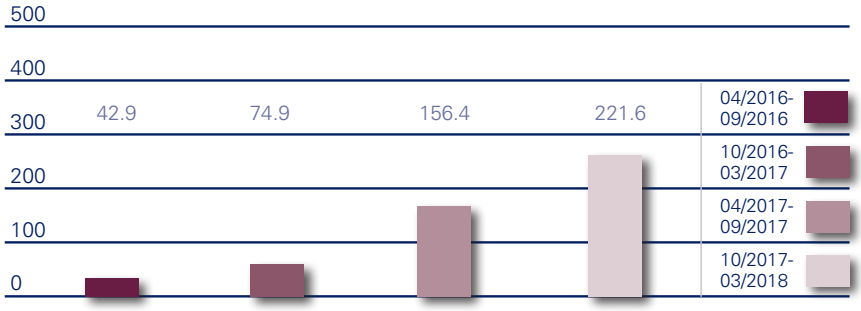
Nonmonetary Recommendations	
April 2016 – September 2016	16
October 2016 – March 2017	27
April 2017 – September 2017	36
October 2017 – March 2018	33

Reports Issued and Investigations Closed



Does not include two Failed Bank Review reports.

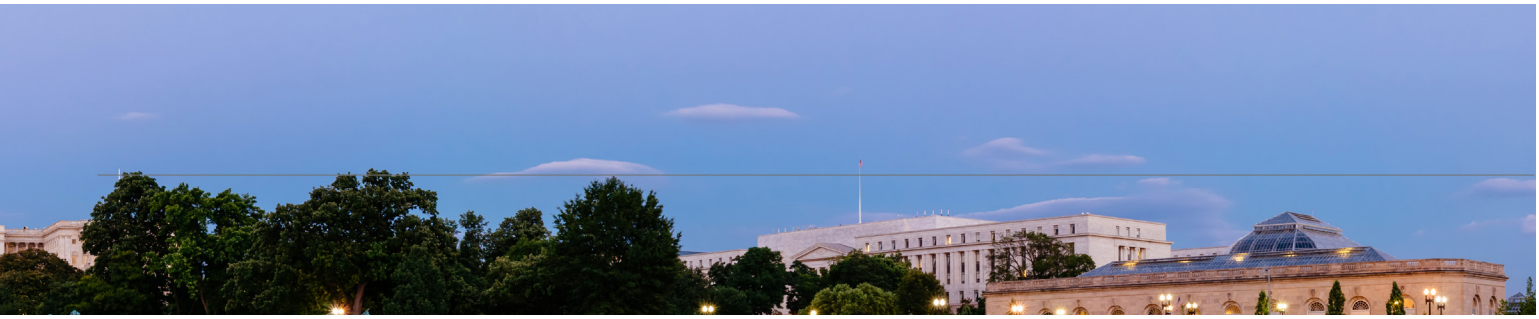
Fines, Restitution, and Monetary Recoveries Resulting from OIG Investigations ($ millions)



Reporting Requirements

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

Reporting Requirements	Page
Section 4(a)(2) Review of legislation and regulations.	39
Section 5(a)(1) Significant problems, abuses, and deficiencies.	6-12
Section 5(a)(2) Recommendations with respect to significant problems, abuses, and deficiencies.	6-12
Section 5(a)(3) Recommendations described in previous semiannual reports on which corrective action has not been completed.	40
Section 5(a)(4) Matters referred to prosecutive authorities.	52
Section 5(a)(5) Summary of each report made to the head of the establishment regarding information or assistance refused or not provided.	52
Section 5(a)(6) Listing of audit, inspection, and evaluation reports by subject matter with monetary benefits.	49
Section 5(a)(7) Summary of particularly significant reports.	6-12
Section 5(a)(8): Statistical table showing the total number of audit reports and the total dollar value of questioned costs.	50
Section 5(a)(9) Statistical table showing the total number of audit reports and the total dollar value of recommendations that funds be put to better use.	51
Section 5(a)(10) Summary of each audit, inspection, and evaluation report issued before the commencement of the reporting period for which	
• no management decision has been made by the end of the reporting period	51
• no establishment comment was received within 60 days of providing the report to management	51
• there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.	41-48
Section 5(a)(11) Significant revised management decisions during the current reporting period.	52



Reporting Requirements (continued)	Page
Section 5(a)(12) Significant management decisions with which the OIG disagreed.	52
Section 5(a)(14, 15, 16) An appendix with the results of any peer review conducted by another OIG during the period or if no peer review was conducted, a statement identifying the last peer review conducted by another OIG.	55
Section 5(a)(17): Statistical tables showing, for the reporting period: • number of investigative reports issued • number of persons referred to the DOJ for criminal prosecution • number of persons referred to state and local prosecuting authorities for criminal prosecution • number of indictments and criminal Informations.	52
Section 5(a)(18) A description of metrics used for Section 5(a)17 information.	52
Section 5(a)(19) A report on each OIG investigation involving a senior government employee where allegations of misconduct were substantiated, including • the facts and circumstances of the investigation • the status and disposition of the matter, including if referred to the DOJ, the date of referral, and the date of DOJ declination, if applicable.	53
Section 5(a)(20) A detailed description of any instance of Whistleblower retaliation, including information about the official engaging in retaliation and what consequences the establishment imposed to hold the official responsible.	53
Section 5(a)(21) A detailed description of any attempt by the establishment to interfere with OIG independence, including with respect to budget constraints, resistance to oversight, or restrictions or delays involving access to information.	53
Section 5(a)(22) A detailed description of each OIG inspection, evaluation, and audit that is closed and was not disclosed to the public; and OIG investigation involving a senior government employee that is closed and was not disclosed to the public.	53

Appendix 1

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

Review of Legislation and Regulations

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

Legislation, Statutes, and Related Documents

- S. 2178, the Inspector General Recommendation Transparency Act of 2017, which would require Offices of Inspector General to include more information in their Semiannual Reports to the Congress regarding unimplemented recommendations that are more than one year old. Our Office's comments sought clarification of the scope of reports to which the bill would apply.
- Draft of the Payment Integrity Information Act of 2018, which would combine existing statutes regarding improper payments by certain federal agencies and reviews by the agencies' respective Inspectors General. Our comments sought clarification of the bill's provision regarding OIG computer matching practices.
- Draft of legislation to codify the Inspector General Act in title 5 of the United States Code, which would reorganize the current version of the IG Act but not make substantive revisions to it. We reviewed the bill and made technical comments on it.
- Draft of the Good Accounting Obligation in Government Act, which would require the budget justification statements of agency Inspectors General to include information about certain open OIG recommendations. Our comments sought clarification of certain terminology used in the bill.
- H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, which addressed a number of issues regarding the National Institute of Standards and Technology (NIST), including NIST's provision of assistance to agency Inspectors General. We reviewed the bill but provided no comments on it; we had provided comments on an earlier version of this bill.

Regulatory or Guidance Documents

From a regulatory standpoint, the OIG's Office of General Counsel worked with staff in the FDIC's Privacy Program in updating the FDIC's Privacy Act System of Records Notices that pertain to records maintained by the OIG.

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

This table shows the corrective actions management has agreed to implement but has not completed, along with associated monetary amounts, as applicable. The information in this table is based on (1) information supplied by the FDIC's Risk Management and Internal Control (RMIC) branch, Division of Finance, and (2) the OIG's determination of when a recommendation can be closed. RMIC has categorized the status of these recommendations as follows:

Management Action in Process: (two recommendations from two reports)

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

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

Report Number, Title and Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
Management Action in Process		
AUD-15-008 **FDIC's Role in Operation Choke Point and Supervisory Approach to Institutions that Conducted Business with Merchants Associated with High-Risk Activities** September 16, 2015	2	The Division of Risk Management Supervision's Internal Control and Review section will conduct horizontal and regional office reviews to assess compliance with the FDIC's actions to address the issues discussed in the report. The FDIC will also continue to report to the Board on deposit account terminations; highlight supervisory guidance in outreach events; and monitor inquiries and comments from the Office of the Ombudsman.
AUD-16-004 **The FDIC's Process for Identifying and Reporting Major Information Security Incidents** July 7, 2016	4*	The Chief Information Officer Organization will promptly establish a review process to ensure that future Congressional notifications of major incidents include appropriate context.

* The OIG has requested additional information to evaluate management's actions in response to the OIG recommendation.

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods				
Report Number, Title, and Date	**Report Summary**	**Recommendations**		**Potential Cost Savings**
		Total	**Outstanding**	
AUD-15-008 **The FDIC's Role in Operation Choke Point and Supervisory Approach to Institutions that Conducted Business with Merchants Associated with High-Risk Activities** September 16, 2015	In a letter dated October 23, 2014, 35 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. The objectives of the audit were 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. We concluded 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 considered the FDIC's involvement in Operation Choke Point to have been inconsequential to the overall direction and outcome of the initiative. We found no evidence that the FDIC used the high-risk list to target financial institutions. We also 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 Federal Deposit Insurance 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. The report contained three recommendations 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.	3	1	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods				
Report Number, Title, and Date	**Report Summary**	**Recommendations**		**Potential Cost Savings**
		Total	**Outstanding**	
AUD-16-001 **FDIC's Information Security Program – 2015** October 28, 2015	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct a performance audit to evaluate the effectiveness of the FDIC's information security program and practices, as required by the Federal Information Security Modernization Act of 2014 (FISMA). Overall, C&C concluded that the FDIC's information security program and practices were generally effective and noted several important improvements in the FDIC's information security program over the past year. However, C&C noted that the FDIC had not assessed whether Information Security Managers had requisite skills, training, and resources. Also the FDIC had not always timely completed outsourced information service provider assessments or review of user access to FDIC systems. Other findings involved control areas of risk management and configuration management. The report contained six recommendations to improve the effectiveness of the FDIC's information security program controls and practices.	6	1	NA
EVAL-16-004 **The FDIC's Process for Identifying and Reporting Major Information Security Incidents** July 7, 2016	FISMA required federal agencies to develop, document, and implement an agency-wide information security program that included (among other things) procedures for detecting, reporting, and responding to information security incidents. Such procedures were to include notifying and consulting with, as appropriate, the Congressional Committees referenced in the statute for major incidents. Our audit objective was to determine whether the FDIC had established key controls that provided reasonable assurance that major incidents were identified and reported in a timely manner. Although the FDIC had established various incident response policies, procedures, guidelines, and processes, these controls did not provide reasonable assurance that major incidents were identified and reported in a timely manner. The report contained five recommendations addressed to the Chief Information Officer that were intended to provide the FDIC with greater assurance that major incidents would be identified and reported consistent with FISMA and Office of Management and Budget Memorandum M-16-03.	5	1	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods				
Report Number, Title, and Date	**Report Summary**	**Recommendations**		**Potential Cost Savings**
		Total	**Outstanding**	
AUD-17-001 **Audit of the FDIC's Information Security Program – 2016** November 2, 2016	The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C& C) to conduct this performance audit. The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. C&C found that the FDIC had established a number of information security program controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable National Institute of Standards and Technology (NIST) standards and guidelines. However, C&C described security control weaknesses that impaired the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at elevated risk. C&C reported on 17 findings, of which 6 were identified during the current year FISMA audit and the remaining 11 were identified in prior OIG or Government Accountability Office reports. These weaknesses involved: strategic planning, vulnerability scanning, the Information Security Manager Program, configuration management, technology obsolescence, third-party software patching, multi-factor authentication, contingency planning, and service provider assessments. The report contained six new recommendations addressed to the Chief Information Officer to improve the effectiveness of the FDIC's information security program and practices.	6	2	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods				
Report Number, Title, and Date	**Report Summary**	**Recommendations**		**Potential Cost Savings**
		Total	**Outstanding**	
EVAL-17-004 **Technology Service Provider Contracts with FDIC-Supervised Institutions** February 14, 2017	Financial institutions (FI) increasingly rely on technology service providers (TSP) to provide or enable key banking functions. Every FI has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information, including when such FI customer information is maintained, processed, or accessed by a TSP. Our evaluation objective was to assess how clearly FDIC-supervised institutions' contracts with TSPs addressed the TSP's responsibilities related to (1) business continuity planning and (2) responding to and reporting on cybersecurity incidents. We did not see evidence that most of the FDIC-supervised institutions we reviewed fully considered and assessed the potential impact and risk that TSPs may have on the financial institutions' ability to manage their own business continuity planning and incident response and reporting operations. Institutions' contracts with TSPs typically did not clearly address TSP responsibilities and lacked specific contract provisions to protect financial institutions' interests. While the FDIC independently and the Federal Financial Institutions Examination Council members collectively took numerous steps to provide institutions comprehensive business continuity, cybersecurity, and vendor management guidance, as well as enhance examination programs, we concluded that more time was needed to allow those efforts to have an impact. The report contained two recommendations for the FDIC to continue communication efforts; and, at an appropriate time, to conduct a follow-on study to assess the extent that financial institutions have effectively addressed key issues.	2	2	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods				
Report Number, Title, and Date	**Report Summary**	**Recommendations**		**Potential Cost Savings**
		Total	**Outstanding**	
AUD-17-004 **Follow-on Audit of the FDIC's Identity, Credential, and Access Management (ICAM) Program** June 8, 2017	On September 30, 2015, we issued an audit report, entitled *The FDIC's Identity, Credential, and Access Management (ICAM) Program* (the ICAM Audit Report). The FDIC established the ICAM program in February 2011 to address the goals and objectives of Homeland Security Presidential Directive-12, Policy for a Common Identification Standard for Federal Employees and Contractors. The ICAM Audit Report indicated that the FDIC had not achieved its goal of issuing identity credentials (known as personal identity verification (PIV) cards) to all eligible employees and contractor personnel. In addition, the FDIC had not established appropriate governance to ensure the ICAM program's success. In light of the concerns raised in the ICAM Audit Report, the Chairman of the FDIC Audit Committee requested that we conduct follow-up audit work related to the ICAM program. We also determined that follow-on work in this area was warranted. The objective of this audit was to assess the FDIC's plans and actions to address the recommendations contained in the ICAM Audit Report. We found that the FDIC experienced considerable challenges and that there were risks warranting management's attention as the Corporation issued PIV cards to its employees and contractor personnel and enabled the cards to support access to the FDIC network. The FDIC took steps to address those challenges and risks during our audit. However, our report identified three additional aspects of the program that still needed improvement. We made four recommendations addressed to the FDIC Chief Information Officer and the Directors, Division of Administration, and Division of Information Technology, to strengthen internal controls over the issuance and maintenance of PIV cards used to access FDIC facilities and the FDIC network.	4	1	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods				
Report Number, Title, and Date	**Report Summary**	**Recommendations**		**Potential Cost Savings**
		Total	**Outstanding**	
EVAL-17-006 **FDIC's Process for Filling Certain DRR Time-Limited Positions** July 13, 2017	The Federal Government's Merit System Principles provide that a fundamental tenet of the federal civil service is that hiring decisions should consider qualified individuals based on merit and ability, after fair and open competition. We initiated this evaluation in response to three complaints received by the OIG Hotline in June and December 2015, regarding hiring practices in the FDIC's Division of Resolutions and Receiverships (DRR). The complaints included allegations that certain DRR vacancy announcements posted in 2015 were too restrictive, resulting in the exclusion of veterans and other applicants from meeting required qualification factors. The complainants also alleged that DRR's hiring process was not carried out in a fair and equitable manner. The objective of our evaluation was to assess the merits of hotline complaints that the OIG received, pertaining to hiring practices in DRR. To accomplish our objective, we focused on FDIC processes and controls for extending selected temporary positions. We substantiated aspects of the OIG hotline allegations and identified weaknesses in the FDIC's process for filling certain time-limited positions. We also found that certain qualification factors in vacancy announcements were narrowly written. Based on information we gathered, we were not able to substantiate allegations that DRR attempted to exclude qualified veterans from consideration. The report contained five recommendations to strengthen controls surrounding the FDIC's application posting and review processes.	5	3	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods				
Report Number, Title, and Date	**Report Summary**	**Recommendations**		**Potential Cost Savings**
		Total	**Outstanding**	
EVAL-17-007 **Controls over Separating Personnel's Access to Sensitive Information** September 18, 2017	Our evaluation objective was to determine the extent to which the FDIC had established controls to mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel. While the FDIC had established and implemented various control activities, we found that there were weaknesses in the design of certain controls, division and office records liaisons were not always following procedures, and opportunities existed to strengthen the pre-exit clearance process. As designed, the program controls did not provide reasonable assurance that the pre-exit clearance process would timely or effectively identify unauthorized access to, or inappropriate removal and disclosure of, sensitive information by separating employees. We noted that separating contractor employees (contractors) may present greater risks than separating FDIC employees. We found several differences between the pre-exit clearance process for FDIC employees and contractors that increased risks related to protecting sensitive information when contractors separated. We also found that the FDIC was not consistently following its pre-exit clearance procedures with respect to separating contractors, and we identified several opportunities for strengthening the contractor pre-exit clearance process. We made 11 recommendations to provide the FDIC with greater assurance that its controls mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel.	11	5	NA

Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods				
Report Number, Title, and Date	**Report Summary**	**Recommendations**		**Potential Cost Savings**
		Total	**Outstanding**	
AUD-17-006 **The FDIC's Processes for Responding to Breaches of Personally Identifiable Information** September 29, 2017	In fulfilling its mission of insuring deposits, supervising insured financial institutions, and resolving failed insured financial institutions, the FDIC collects and manages considerable amounts of personally identifiable information (PII). We initiated this audit in response to concerns raised by the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs regarding a series of data breaches reported by the FDIC in late 2015 and early 2016. Many of these data breaches involved PII. The objective of the audit was to assess the adequacy of the FDIC's processes for (1) evaluating the risk of harm to individuals potentially affected by a breach involving PII and (2) notifying and providing services to those individuals, when appropriate. The FDIC established formal processes for evaluating the risk of harm to individuals potentially affected by a breach involving PII and providing notification and services to those individuals, when appropriate. However, the implementation of these processes was not adequate. Our report included one additional matter that, although not within the scope of the audit, warranted management attention. Specifically, the FDIC needed to update its written Chief Privacy Officer designation to reflect organizational changes that had occurred since the original designation was made in March 2005. Our report contained seven recommendations addressed to the Chief Information Officer/Chief Privacy Officer to promote more timely breach response activities and strengthen controls for evaluating the risk of harm to individuals potentially affected by a breach and notifying and providing services to those individuals, when appropriate.	7	3	NA

Table III: Audit and Evaluation Reports Issued by Subject Area

Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	**Title**	**Total**	**Unsupported**	
Supervision				
AUD-18-002 November 3, 2017	*Material Loss Review of First NBC Bank, New Orleans, Louisiana*			
EVAL-18-001 December 6, 2017	*FDIC's Implementation of Consumer Protection Rules Regarding Ability to Repay Mortgages and Compensation for Loan Originators*			
Receivership Management				
EVAL-18-002 March 16, 2018	*Claims Administration System Functionality*			
Resources Management				
AUD-18-001 October 25, 2017	*Audit of the FDIC's Information Security Program—2017*			
AUD-18-003 November 8, 2017	*The FDIC's Compliance with the Digital Accountability and Transparency Act of 2014*			
Totals for the Period		**$0**	**$0**	**$0**

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

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

Table VI: Status of OIG Recommendations Without Management Decisions

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

Table VII: Status of OIG Reports Without Comments

During this reporting period, there were no reports where comments were received after 60 days of providing the report to management.

Table VIII: Significant Revised Management Decisions

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

Table IX: Significant Management Decisions with Which the OIG Disagreed

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

Table X: Instances Where Information Was Refused

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

Table XI: Investigative Statistical Information

Number of Investigative Reports Issued	28
Number of Persons Referred to the Department of Justice for Criminal Prosecution	59
Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution	2
Number of Indictments and Criminal Informations	39

Description of the metrics used for the above information: Reports issued reflects case closing memorandums issued to FDIC management. With respect to the 59 referrals to the Department of Justice, the total represents 53 individuals, 5 business entities, and 1 instance where the case was referred but the subject is unknown at this time. Two individuals were referred to state and local prosecutors. Our total indictments and criminal Informations includes indictments, Informations, and superseding indictments.

Table XII: OIG Investigations Involving Senior Government Employees Where Allegations of Misconduct Were Substantiated

The FDIC OIG investigated allegations that a corporate manager had directed a subordinate not to speak with the OIG and threatened retaliation. The investigation developed evidence that the manager had made statements discouraging the employee from speaking with the OIG. The investigation did not find that the employee was prevented from sharing information with the OIG or was actually retaliated against. The case was not referred to the Department of Justice because it did not involve evidence of criminal conduct. The OIG referred the report of investigation to FDIC management for consideration of administrative or disciplinary action. At the end of the semiannual period, FDIC management was considering what action to take.

Table XIII: Instances of Whistleblower Retaliation

During this reporting period, there were no instances of Whistleblower retaliation.

Table XIV: Instances of Agency Interference with OIG Independence

During this reporting period, there were no attempts to interfere with OIG independence.

Table XV: OIG Inspections, Evaluations, and Audits that Were Closed and Not Disclosed to the Public; and Investigations Involving Senior Government Employees that Were Closed and Not Disclosed to the Public

During the reporting period, there were no evaluations or audits closed. As noted in Table XII, the FDIC OIG investigated allegations involving a corporate manager and reported the results of that investigation to FDIC management. This matter was closed and not disclosed to the public.

Appendix 2

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

FDIC OIG Review Activity for the Period October 1, 2017 through March 31, 2018
(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 the DIF (Dollars in Millions)	Grounds Identified by the State Bank Supervisor for Appointing the FDIC as Receiver	Unusual Circumstances Warranting In-Depth Review?
Completed Reviews				
Proficio Bank (Cottonwood Heights, Utah)	3/3/17	$11.0	The bank was unable to meet capital and other requirements of a 2014 formal enforcement action, and operated in an unsafe and unsound manner.	No
Farmers and Merchants State Bank of Argonia (Argonia, Kansas)	10/13/17	$2.6	The bank could not sufficiently recapitalize, liquidate its indebtedness, or resume business to the satisfaction of depositors and creditors.	No

Appendix 3

Peer Review Activity

Federal Inspectors General are required to engage in peer review processes related to both their audit and investigative operations. The FDIC OIG is reporting the following information related to its peer review activities. These activities cover our most recent roles as both the reviewed and the reviewing OIG and relate to both audit and investigative peer reviews.

Audit Peer Reviews

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

Definition of Audit Peer Review Ratings

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

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

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

- The U.S. Railroad Retirement Board OIG conducted a peer review of the FDIC OIG's audit organization and issued its system review report on November 14, 2016. In the Railroad Retirement Board OIG's opinion, the system of quality control for our audit organization in effect for the year ending March 31, 2016, 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 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.

This peer review report is posted on our Website at www.fdicoig.gov.

FDIC OIG Peer Review of the Tennessee Valley Authority OIG

The FDIC OIG completed a peer review of the system of quality control for the audit organization of the Tennessee Valley Authority (TVA) OIG, and we issued our final report to that OIG on May 16, 2017. We reported that in our opinion, the system of quality control for the audit organization of the TVA OIG, in effect for the 12 months ended September 30, 2016, had been suitably designed and complied with to provide the TVA OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. The TVA OIG received a peer review rating of pass.

We also issued a letter of comment to the TVA OIG that set forth findings and recommendations that were not considered to be of sufficient significance to affect our overall opinion.

TVA OIG posted the peer review report on its Website at http://oig.tva.gov/peer_reports.html.

Investigative Peer Reviews

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

- The Department of the Treasury OIG conducted the most recent peer review of our investigative function and issued its final report on the quality assessment review of the investigative operations of the FDIC OIG on February 1, 2016. The Department of the Treasury OIG reported that in its opinion, the system of internal safeguards and management procedures for the investigative function of the FDIC OIG in effect for the year ending December 31, 2015, was in compliance with quality standards established by CIGIE and 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 Small Business Administration (SBA) OIG. We issued our final report to SBA OIG on December 19, 2017. We reported that, in our opinion, the system of internal safeguards and management procedures for the investigative function of the SBA OIG in effect for the period ending August 31, 2017 was in compliance with the quality standards established by CIGIE and other applicable guidelines and statutes.

Congratulations and Farewell

The following staff members retired from the FDIC OIG during the reporting period. We appreciate their many contributions over the years and wish them well in future endeavors.

Karen Davis

Jo Anne King

Annette Daley

Michael Horton

Celebrate

Building on 40 Years of Excellence in Independent Oversight

On Wednesday, July 11, 2018, at the U.S. Capitol Visitor Center, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) will host an all-day conference to educate the public about the impact of the Inspector General Act of 1978 and the work of federal Inspectors General in the 40 years since passage of the Act.

The Inspector General Act of 1978, as amended, established 73 independent Offices of Inspector General within federal agencies to provide oversight and to promote economy, efficiency, and effectiveness throughout the federal government. Today, over 14,000 OIG employees work to detect and deter waste, fraud, abuse, and misconduct in federal programs and personnel. This work has resulted in recommendations for hundreds of billions of dollars of potential savings, tens of thousands of successful prosecutions, and transformational government reforms.

"Inspectors General have had a profound impact on the U.S. government. Their independent oversight brings to bear incontrovertible improvement in federal programs, and continues to reveal instances of fraud, waste, abuse, and misconduct. This year, we will commemorate all that we have accomplished, and look forward to the future of continued stewardship and accountability in the federal government," stated CIGIE Chair Michael Horowitz, who is also the Inspector General of the U.S. Department of Justice.

The FDIC OIG is proud to be a member of the IG community and pleased to join our colleagues in celebrating 40 years of promoting effective and efficient government.

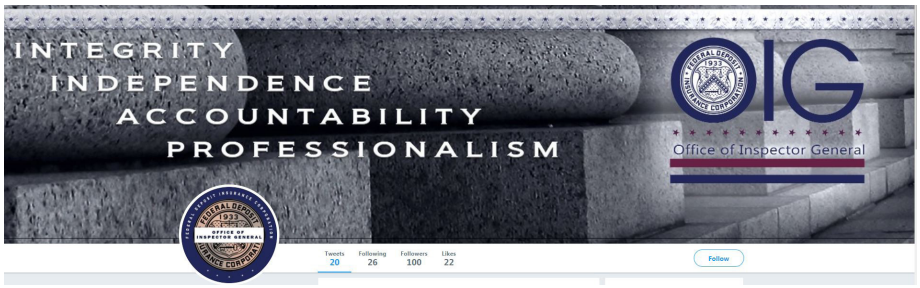
Visit www.ignet.gov/2018-commemoration for additional information about the event.

1978–2018
IG Act
Promoting Effective
& Efficient Government
40 Years

Keep Informed

Learn more about the FDIC OIG.
Visit our Website: www.fdicoig.gov

Follow us on Twitter: @FDIC_OIG



View the work of 73 Federal OIGs on the IG Community's Website

OVERSIGHT.GOV
ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE

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

OIG HOTLINE

The Office of Inspector General 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. Instructions for contacting the Hotline and an on-line form can be found at www.fdicoig.gov.

Whistleblowers can contact the OIG's Whistleblower Ombudsperson through the Hotline by indicating: Attention: Whistleblower Ombudsperson.

DESIGN: FDIC/DOA/CSB/GRAPHIC DESIGN AND PRINTING UNIT

FDIC-024-2018