Office of Inspector General

# Semiannual Report to the Congress

**April 1, 2018 – September 30, 2018**

FDIC

Federal Deposit Insurance Corporation

**Under the Inspector General Act of 1978, as amended, the Federal Deposit Insurance Corporation Office of Inspector General (FDIC OIG) 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 5,800 individuals carry out the FDIC mission throughout the country.**

**According to most current FDIC data, the FDIC insured almost $7.4 trillion in deposits in 5,542 institutions, of which the FDIC supervised 3,569. The Deposit Insurance Fund balance totaled $97.6 billion as of June 30, 2018. Active receiverships as of September 30, 2018, totaled 282, with assets in liquidation of about $1.25 billion.**

# Office of Inspector General

# Semiannual Report to the Congress

April 1, 2018 – September 30, 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 April 1 through September 30, 2018. The work highlighted in this Report illustrates the broad range and importance of our oversight responsibilities.

We completed several audit and evaluation reviews during this Semiannual Report period. These included an assessment of the FDIC's governance of its information technology initiatives, the FDIC's Forward-Looking Supervision approach in conducting examinations of financial institutions, and the processing of consumer complaints. We also issued a Special Inquiry report examining the FDIC's handling of eight information security incidents involving highly sensitive information. We made 13 recommendations in this report to address the systemic issues associated with the FDIC's incident response and reporting and interactions with the Congress.

In addition, we joined other members of the Council of Inspectors General on Financial Oversight (CIGFO) to issue *The Top Management and Performance Challenges Facing Financial Regulatory Organizations*. The Dodd-Frank Act established CIGFO to suggest measures for improving financial oversight. This report identifies cross-cutting Challenges facing the financial regulators: Enhancing Oversight of Financial Institution Cybersecurity; Managing and Securing Information Technology at Regulatory Organizations; Sharing Threat Information; Readiness for Crises, Strengthening Agency Governance; and Managing Human Capital. These Challenges highlight the importance of Government-wide coordination and information sharing throughout the financial sector.

Our Office also conducts significant investigations into criminal and administrative matters, and our cases involve sophisticated multi-million dollar schemes of bank fraud, embezzlement, money laundering, and other crimes committed by bank executives and insiders. During the reporting period, our investigations led to the arrest of 20 individuals, 17 convictions, and criminal charges in 28 indictments and informations. In addition, these cases resulted in fines, restitution orders, and forfeitures of more than $135 million.

In one such case, the former Chief Executive Officer and Chief Lending Officer of the failed Sonoma Valley Bank were each sentenced to 100 months in prison for conspiracy, bank fraud, wire fraud, money laundering, falsifying bank records, lying to bank regulators, and other crimes. An attorney for a developer involved in the scheme was also sentenced to 80 months in prison. These individuals were ordered to pay more than $19 million in restitution for their roles in the fraud.

Our Office appreciates the continued support of Members of the Congress and staff, the FDIC, and our colleagues in the IG community, with whom we recently celebrated the 40th Anniversary of the Inspector General Act of 1978. Also, during the reporting period, the FDIC welcomed a new Chairman, Jelena McWilliams. My Office is committed to working with her to provide independent oversight of FDIC programs and activities.

Jay N. Lerner
Inspector General
October 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** | 17 |
| **Other Key Priorities** | 25 |
| **Reporting Requirements** | 31 |
| **Appendix 1** Information Required by the Inspector General Act of 1978, as amended | 33 |
| **Appendix 2** Information on Failure Review Activity | 49 |
| **Appendix 3** Peer Review Activity | 50 |
| **Congratulations and Farewell** | 53 |

# Acronyms and Abbreviations

| | |
|---|---|
| **CAS** | Claims Administration System |
| **CB&T** | Coastal Bank & Trust |
| **C&C** | Cotton & Company LLP |
| **CEO** | Chief Executive Officer |
| **CIGFO** | Council of Inspectors General on Financial Oversight |
| **CIGIE** | Council of the Inspectors General on Integrity and Efficiency |
| **CLO** | Chief Loan Officer |
| **DCP** | Division of Depositor and Consumer Protection |
| **DIF** | Deposit Insurance Fund |
| **DIT** | Division of Information Technology |
| **DOA** | Division of Administration |
| **Dodd-Frank Act** | Dodd-Frank Wall Street Reform and Consumer Protection Act |
| **DOF** | Division of Finance |
| **DOJ** | Department of Justice |
| **DRR** | Division of Resolutions and Receiverships |
| **FBI** | Federal Bureau of Investigation |
| **FDIC** | Federal Deposit Insurance Corporation |
| **FEDSIM** | Federal Systems Integration and Management Center |
| **FHFA** | Federal Housing Finance Agency |
| **FI** | Financial Institution |
| **FISMA** | Federal Information Security Modernization Act of 2014 |
| **FRB** | Federal Reserve Board |
| **FSOC** | Financial Stability Oversight Council |

| | |
|---|---|
| **GAO** | Government Accountability Office |
| **GSA** | General Services Administration |
| **ICAM** | Identity, Credential, and Access Management |
| **IG** | Inspector General |
| **IRS-CI** | Internal Revenue Service-Criminal Investigation |
| **ISC-3** | Infrastructure Support Contract 3 |
| **IT** | Information Technology |
| **MOU** | Memorandum of Understanding |
| **OIG** | Office of Inspector General |
| **OM** | Oversight Manager |
| **OMB** | Office of Management and Budget |
| **PII** | Personally Identifiable Information |
| **PIV** | Personal Identity Verification |
| **RMS** | Division of Risk Management Supervision |
| **SAR** | Suspicious Activity Report |
| **SBA** | Small Business Administration |
| **SIGTARP** | Special Inspector General for the Troubled Asset Relief Program |
| **SST Committee** | Committee on Science, Space, and Technology, U.S. House of Representatives |
| **TM** | Technical Monitor |
| **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.

Our Office conducts its work 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.

This year the Inspector General (IG) community marks the 40th anniversary of the Inspector General Act. In October 1978, President Jimmy Carter signed the Act, establishing the first 12 presidentially appointed IGs in Federal departments and agencies. Since that time, the community has grown to include 73 statutory IGs who collectively oversee the operations of nearly every aspect of the Federal government. In the years to come, we look forward to continuing our efforts to provide independent and effective oversight of the FDIC and working with the Council of the Inspectors General on Integrity and Efficiency on important issues that cut across our government.

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

| Overall Results (April 1, 2018 – September 30, 2018) | |
|---|---|
| Audit, Evaluation, and Other Reports Issued | 6 |
| Nonmonetary Recommendations | 29 |
| Investigations Opened | 29 |
| Investigations Closed | 46 |
| OIG Subpoenas Issued | 1 |
| Judicial Actions: | |
| Indictments/Informations | 28 |
| Convictions | 17 |
| Arrests | 20 |
| OIG Investigations Resulted in: | |
| Fines | $322,600 |
| Restitution | $ 104,852,552 * |
| Asset Forfeitures | $ 29,851,643** |
| Total | $ 135,026,795 |
| Referrals to the Department of Justice (U.S. Attorneys) | 52 |
| Proposed Regulations and Legislation Reviewed | 6 |
| Responses to Requests Under the Freedom of Information/Privacy Act | 8 |

*Of this total amount, $51,459,701 was ordered joint and several with other individuals sentenced during this reporting period.
**Includes forfeited property appraised at $20.8 million in 2014.

# 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 the results of six audit, evaluation, and Special Inquiry reviews during the reporting period, as summarized below. These reports contained 29 recommendations, and spanned various FDIC programs and activities. Our office also reviews all failed FDIC-supervised institutions causing 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. There have been no FDIC-supervised financial institution failures since October 13, 2017, and we conducted no such reviews during the reporting period, as noted in Appendix 2.

### The FDIC's Governance of Information Technology Initiatives

Our Office issued an audit report that highlights challenges and risks facing the FDIC with respect to the governance of its information technology (IT) initiatives. The audit focused on key components of the FDIC's IT strategic planning, enterprise architecture, and governance bodies and practices. We reviewed these components in light of three IT initiatives: (1) migration of FDIC email operations to the cloud; (2) deployment of laptop computers to FDIC employees and contractor personnel; and (3) proposed adoption of a managed services solution for mobile IT devices.

We reported that the FDIC faced a number of challenges and risks with respect to the governance of its IT initiatives. Although the FDIC had planned to develop an enterprise cloud strategy in 2017, it had not done so prior to pursuing cloud initiatives. Specifically, the FDIC had not fully developed a strategy to migrate IT services and applications to the cloud prior to executing initiatives, nor had the FDIC obtained the acceptance of organizational stakeholders across the FDIC's Divisions and Offices.

In addition, the FDIC did not have an effective enterprise architecture to support its IT decision-making and guide the execution of its strategic goals and objectives. We found that the FDIC's architecture was immature, and it did not guide the three IT initiatives we reviewed nor the FDIC's transition of IT services to the cloud.

Also, the FDIC had not established a security architecture for its IT Governance Framework and IT Governance Processes, nor adequately defined the roles and responsibilities of information security officials. Notably, a third-party consultant assessed the FDIC's enterprise security architecture, noting it was "ad hoc" and was "inconsistently documented and implemented." The consultant further found that the FDIC's IT Governance Processes did not clearly document roles and responsibilities for IT security.

Moreover, the FDIC had not acquired adequate resources and expertise needed to improve the FDIC's IT Governance Framework and did not use complete cost information when evaluating cloud solutions. The FDIC's plans for significant and rapid transformation in the delivery of IT resources required individuals with expertise that the FDIC lacked in 2016 and improved financial information such as relevant intangible benefits to evaluate IT initiatives.

These challenges created uncertainty among FDIC Divisions and Offices regarding the implementation of the FDIC's IT strategic goals and objectives and the impact such efforts would have on their respective program areas. We also found that due to the limited IT governance applied to the cloud and laptop deployment initiatives that we reviewed, the former FDIC Chief Information Officer pursued overly aggressive implementation schedules and did not obtain broad business stakeholder involvement during the early stages of two of the three initiatives we reviewed. This resulted in unaddressed business needs and security risks, and it created inefficiencies, increased costs, and delayed the initiatives.

We made eight recommendations to address the IT Governance weaknesses we identified. These recommendations included the FDIC developing an implementation plan that supports the IT Strategic Plan; implementing an enterprise architecture as part of the IT Governance Framework; defining and documenting roles and responsibilities for information security; and identifying IT resources and expertise to execute the IT Strategic Plan. FDIC management concurred with our recommendations.

## Forward-Looking Supervision

An evaluation report that we issued during the reporting period assessed the FDIC's Forward-Looking Supervision approach in conducting examinations of financial institutions. The evaluation focused on the FDIC's Forward-Looking Supervisory initiative as part of its risk-focused supervision program. The goals of this supervisory approach are to identify and assess risk before it impacts a financial institution's financial condition and to ensure early risk mitigation.

Our evaluation objective was to determine whether the Forward-Looking Supervision approach achieved its outcomes—the Division of Risk Management Supervision (RMS) pursued supervisory action upon identifying risks and the financial institutions implemented corrective measures. Our review showed that examiners substantially achieved the intended outcomes of the Forward-Looking Supervision approach for our sampled institutions. Examiners applied Forward-Looking Supervision concepts during their financial institution examinations, rated institutions based on risk, and recommended corrective actions based on their risk assessments. Also, the financial institutions committed to implement the corrective actions.

We found that:

- The FDIC did not have a comprehensive policy guidance document on Forward-Looking Supervision and should clarify guidance associated with its purpose, goals, roles, and responsibilities;
- Examiners typically documented their overall conclusions regarding the financial institutions' concentration risk management practices; however, they did not always document certain Forward-Looking Supervision concepts in pre-examination planning documents and when reporting examination results;
- Examiners typically reported or elevated identified overall concentration risk management conclusions and concerns; however, a greater number of these concerns should have appeared in the report section that includes issues requiring the attention of the institution's board; and
- Examiners generally identified concentration risk management concerns on a timely basis; however, in certain instances, they identified concentration risk management concerns that had not been identified during the prior examination cycle.

We made four recommendations to the FDIC to: (1) issue a comprehensive policy guidance document defining Forward-Looking Supervision; (2) issue guidance to reinforce how and where examiners should be documenting concentrations and an institution's concentration risk management practices in the Report of Examination; (3) provide additional case studies on Forward-Looking Supervision to strengthen training for examiners; and (4) conduct recurring retrospective reviews to ensure examiners are documenting the concentration risk management analysis. The FDIC concurred with these recommendations.

## Processing of Consumer Complaints

The FDIC plays an important role in helping to protect consumers from unfair and unlawful banking practices that could result in consumer harm. In connection with that role, the FDIC receives, investigates, and answers consumer complaints and inquiries. We issued a report on the FDIC's Processing of Consumer Complaints, in which we assessed the FDIC's compliance with key requirements and determined how the FDIC used consumer complaint information and trends data in its operations.

FDIC personnel categorize complaints in one of two ways: "Fair Lending" complaints allege possible discrimination in lending under the Fair Housing Act or the Equal Credit Opportunity Act. Complaints that do not meet this definition are considered "Non-Fair Lending" cases. In 2017, the FDIC finalized 82 Fair Lending complaints and 3,907 Non-Fair Lending complaints.

We reviewed 60 complaint cases (22 Fair Lending and 38 Non-Fair Lending cases). We found that the FDIC substantially complied with the key requirements to acknowledge, investigate, and respond to the complaints that we sampled. However, we identified 32 case processing exceptions. The exceptions primarily involved instances when the FDIC did not include all required information in recommendation memorandums, which are prepared to document its review of Fair Lending cases and recommendations to conduct or waive on-site investigations at subject banks.

We also found that the FDIC did not process 45 percent of the Fair Lending cases that we sampled in accordance with its case processing timeframe of 120 days. The FDIC took from 126 to 506 days to process the Fair Lending cases that we sampled, with an average processing time of 284 days – nearly 9½ months. Five Fair Lending cases from our sample took more than 300 days for the FDIC to process, with one of these cases taking nearly 17 months. Similarly, the FDIC did not process 45 percent of its Fair Lending cases over the 3-year period from 2015 through 2017 in a timely manner.

As for Non-Fair Lending cases, we found that the FDIC did not process 11 percent of the cases that we sampled in accordance with its case processing timeframe of 60 days. Notably, however, the FDIC processed 95 percent of its Non-Fair Lending cases within 60 days from 2015 through 2017.

The FDIC tracked consumer complaint issues, trends, and concerns, and FDIC senior management received monthly and quarterly reports on consumer complaint trends. The FDIC informed the OIG that examiners reviewed complaint documentation as part of their pre-examination planning processes and followed up on complaints during examinations, as warranted.

We made four recommendations to help ensure the FDIC includes all required information in recommendation memorandums and to help improve the FDIC's timeliness in processing Fair Lending cases.

FDIC management concurred with our recommendations.

### Employee-Initiated Transfers and Associated Travel

From September through December 2017, the OIG Hotline received three complaints alleging that a Program Office within the FDIC had engaged in management practices regarding hiring, personnel, and travel that were not consistent with FDIC policies and procedures. We reviewed these matters and on September 10, 2018, issued a memorandum identifying several concerns related to the FDIC's handling of employee-initiated transfers and associated travel. Our work did not constitute an audit in accordance with Government Auditing Standards.

According to FDIC officials, employee-initiated transfers are intended to accommodate an employee's personal situation by allowing the employees to transfer from their original duty station to a different geographic location to perform their work as a result of a personal hardship. FDIC supervisors evaluate requests for these transfers on a case-by-case basis. As of March 8, 2018, Division of Administration (DOA) officials identified six employees who were approved for employee-initiated transfers as a result of personal hardships and had memorandums of understanding (MOU) reflecting the terms of their transfers.

We reviewed the six MOUs and identified the following concerns:

- The FDIC did not have policies or procedures related to employee-initiated transfers.
- The FDIC did not track employee-initiated transfers, meaning the FDIC could not readily determine the total number of transfers that it has granted and it could not be sure that it was aware of all such transfers.
- The FDIC did not periodically review the basis for employee-initiated transfers.
- The FDIC's Program Offices did not inform the Division of Finance (DOF) about the MOUs that were executed to reflect the employee-initiated transfers. Thus, DOF could not ensure that the MOUs complied with the FDIC's General Travel Regulations related to employee relocations.
- The Legal Division did not have a defined role or process for reviewing employee-initiated transfers.
- The FDIC did not consider tax implications for one employee-initiated transfer. According to DOF travel records, one employee spent more than 50 percent of work time in travel status to a single location over a 32-month period, which could trigger tax implications.
- The FDIC may not have considered lodging costs for one employee-initiated transfer.
- DOF was not aware of unusual agreements with employees regarding travel reimbursements, despite each Program Office recently informing DOF that it did not have any unusual employee travel arrangements in response to a recommendation in an OIG evaluation report.

FDIC management committed to developing and implementing a policy to address employee-initiated transfers. The FDIC's response described actions that management will take to ensure that the FDIC processes employee-initiated transfers and associated travel appropriately and consistent with FDIC policy.

## Infrastructure Support Contract 3 with CSRA, Inc.

In October 2017, we initiated preliminary research in support of a planned audit of the FDIC's Infrastructure Support Contract 3 (ISC-3 contract). During this phase of the assignment, we conducted interviews with representatives from the FDIC's Division of Information Technology (DIT) and DOA; the General Services Administration (GSA) and GSA's Federal Systems Integration and Management Center (FEDSIM); and CSRA Inc. (CSRA). We also gathered relevant information and performed limited testing in connection with a sample of billings and procedural operations. Our work did not constitute an audit in accordance with Government Auditing Standards.

The ISC-3 contract with CSRA covers the day-to-day operations of the FDIC's infrastructure facilities, hardware, software, and systems. The contract primarily supports operational security, client support/help desk functions, data center operations, asset management, and systems engineering areas.

The ISC-3 contract is a Government–Wide Acquisition Contract and, as such, is subject to the Federal Acquisition Regulation. The ISC-3 contract is administered through and managed by FEDSIM, which provides acquisition services to federal agencies and is housed in GSA. The FDIC reimburses FEDSIM for actual contract costs and pays FEDSIM a monthly fee for managing and administering the contract.

We concluded that there was an increased risk that both errors and fraudulent activity would go undetected due to the complexity of CSRA's accounting entries for contractor and subcontractor billings. With respect to training for Oversight Managers (OM) and Technical Monitors (TM), we also found that two TMs never took the FDIC's required contract oversight training and two other TMs took the training, but their certificates had expired in 2008. The training is current for 3 years.

Based on our limited testing, we did not find CSRA's invoices to be inaccurate or unsupported, nor did we identify questioned costs. In addition, the ISC-3 contract was to expire in July 2018, and the future contract for these infrastructure, hardware, software, and systems functions would be administered through a time and materials contract that the FDIC would manage in-house. For these reasons, we determined that additional work was not warranted, and we did not perform an audit. We did, however, leverage our work with respect to this contract in another ongoing evaluation of the FDIC's overall Contract Oversight Management Program.

In response to a draft memorandum conveying our results, DIT and DOA officials expressed the view that the new contract to replace the current ISC-3 contract would have a less complex billing process that would facilitate greater transparency. FDIC management would continue to expect the subsequent vendor to properly reconcile its invoices and do so within a reasonable timeframe. Further, DIT and DOA officials informed the OIG that management had initiated and would ensure that all required oversight management training was conducted for ISC-3 OMs and TMs in a timely manner.

### Special Inquiry: The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches

During late 2015 and early 2016, the FDIC experienced eight information security incidents as departing employees improperly took sensitive information shortly before leaving the FDIC. Seven of the eight incidents involved Personally Identifiable Information (PII), including Social Security Numbers, and thus constituted breaches. In the eighth incident, the departing employee took highly sensitive components of resolution plans submitted by certain large systemically important financial institutions without authorization.

In April and May 2016, the Committee on Science, Space, and Technology of the House of Representatives (SST Committee) examined the FDIC's handling of these incidents, its data security policies, and reporting of the "major incidents." As part of its investigation, the SST Committee requested pertinent documents from the FDIC about the incidents. The SST Committee held two hearings in May and July 2016 about the incidents at the FDIC and issued an interim report on the matter. During the hearings and in its interim report, as well in correspondence with the FDIC, the SST Committee expressed concerns about the FDIC's information security program, the accuracy of certain FDIC statements, and the completeness of the FDIC's document productions.

On June 28, 2016, the then-Chairman of the Senate Committee on Banking, Housing, and Urban Affairs requested that our Office examine issues at the FDIC related to data security, incident reporting, and policies, as well as the representations made by FDIC officials.

The FDIC OIG conducted a Special Inquiry in response to that request. We examined the circumstances surrounding the eight information security incidents. The FDIC initially estimated that the incidents involved sensitive information that included the PII of approximately 200,000 individual bank customers related to approximately 380 financial institutions, as well as the proprietary and sensitive data of financial institutions. Based on additional analysis, the FDIC later revised the number of affected individuals to 121,633.

Our work revealed certain systemic weaknesses that hindered the FDIC's ability to handle multiple information security incidents and breaches efficiently and effectively; contributed to untimely, inaccurate, and imprecise reporting of information to the Congress; and led to document productions that did not fully comply with Congressional document requests. We also identified shortcomings in the performance of certain individuals in key leadership positions as they handled the incidents and related activities.

Importantly, in its handling of the information security incidents, the FDIC did not fully consider the range of impacts on bank customers whose information had been compromised or consider customer notification as a separate decision from whether it would provide credit monitoring services. As a result, the FDIC delayed notifying consumers and thus precluded them from taking proactive steps to protect themselves. Also of note, when reporting incidents to the Congress, the FDIC used broad characterizations and referenced mitigating factors that were sometimes inaccurate and imprecise, and tended to diminish the potential risks. Despite several opportunities to clarify or correct the record regarding the nature of the incidents, the FDIC did not provide the Congress with accurate and complete information about the incidents. Finally, with regard to document production, the SST Committee had requested that the FDIC produce relevant documents and information. The FDIC did not initially respond to these requests in a complete manner and should have been clear in its communications with the Committee as to its approach and progress in complying with the document production requests. Later, the FDIC took steps to better identify and provide responsive records.

Throughout and subsequent to our Special Inquiry, the FDIC took steps to address prior recommendations pertaining to incident and breach response. In addition, we made 13 recommendations in this Special Inquiry report to address the systemic issues associated with the FDIC's incident response and reporting and interactions with the Congress. We also requested that the FDIC review the performance issues we identified and advise the OIG of actions taken to address them.

The FDIC concurred with the 13 recommendations in this Special Inquiry report.

### The Council of Inspectors General on Financial Oversight Issues Top Management and Performance Challenges Facing Financial Regulatory Organizations

The Dodd-Frank Act established the Council of Inspectors General on Financial Oversight (CIGFO) to oversee the Financial Stability Oversight Council (FSOC) and suggest measures to improve financial oversight. FSOC has a statutory mandate that established collective accountability for identifying risks and responding to emerging threats to U.S. financial stability.

The Inspectors General within CIGFO report annually on the Top Management and Performance Challenges affecting their respective organizations.[1] We joined our CIGFO colleagues during the reporting period in issuing a report that identified the following cross-cutting challenges and that reflected the consolidated input from the Inspectors General in CIGFO:

- Enhancing Oversight of Financial Institution Cybersecurity
- Managing and Securing Information Technology at Regulatory Organizations
- Sharing Threat Information
- Readiness for Crises
- Strengthening Agency Governance
- Managing Human Capital

This report emphasizes the importance of government-wide coordination and information sharing for a particular sector – such as the financial sector – in a whole-of-government approach, as distinct from considering the issues on an agency-by-agency basis. Financial regulators may require this approach to coordinate and share information to support combating cybersecurity threats, take action when a crisis occurs, identify and address emerging risks and threats through strong governance, and ensure appropriate numbers of trained staff to recognize and mitigate financial system risks.

Addressing these Challenges in a coordinated and cohesive fashion is important, because the financial sector is one of 16 critical infrastructure sectors that are vital to public confidence and the nation's safety, prosperity, and well-being. Moreover, the financial sector has changed considerably since the last financial crisis. It is more diverse, technology dependent, and interconnected, spanning from Federal, state and local government regulators, to the largest institutions and the smallest community banks and credit unions, as well as those institutions' associated service providers. According to the Department of the Treasury, from 2010 to 2017, more than 3,300 financial service technology-based firms were founded, and those firms represent 36 percent of all U.S. personal loans, an increase from 1 percent in 2010. Also, in 2018, 50 percent of people with bank accounts use mobile devices to access their information, compared to 20 percent in 2011. Further, the speed of technological advances in the financial sector and increased targeting of the financial system by malicious actors highlight the need for financial regulators to address the Challenges identified in this report.

[1] Department of the Treasury (Chair), Federal Deposit Insurance Corporation, Federal Housing Finance Agency, Commodity Futures Trading Commission, Department of Housing and Urban Development, Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection, National Credit Union Administration, Securities and Exchange Commission, Special Inspector General for the Troubled Asset Relief Program.

CIGFO initiated the project to provide useful information to the leaders of financial-sector regulatory organizations as they look to develop strategies to improve efficiency, economy, effectiveness, and accountability at their agencies, consistent with Executive Order 13781, Comprehensive Plan for Reorganizing the Executive Branch. By consolidating and reporting these Challenges, CIGFO aims to inform regulatory organizations, FSOC, the Congress, and the American public as to the assessments by the Council's Inspectors General.

**********

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

# 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 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.

### Former Global Head of HSBC's Foreign Exchange Cash-Trading Sentenced to 24 Months' Imprisonment for Front-Running Scheme

On April 26, 2018, the former head of global foreign exchange cash-trading at HSBC Bank plc, a subsidiary of HSBC Holdings plc, was sentenced to 24 months' imprisonment for committing wire fraud and wire fraud conspiracy, to be followed by 5 years of supervised release. He was also ordered to pay a $300,000 fine. The former bank executive was convicted by a federal jury in October 2017, following a 4-week trial, of one count of wire fraud conspiracy and eight counts of wire fraud.

As established at trial, HSBC was selected to execute a foreign exchange 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, Department of Justice (DOJ).*
***Responsible Agencies:*** *This is a joint investigation by the FDIC OIG and the Federal Bureau of Investigation's (FBI) Washington Field Office. The case was prosecuted by the DOJ Criminal Division's Fraud Section and the USAO for the Eastern District of New York.*

### Two Sentenced to Over 4 Years in Prison Each for Their Roles in a $22 Million Fraud Scheme

On June 1, 2018, a California developer was sentenced to 4 years and 8 months in prison for his role in a bank fraud scheme. He was also ordered to pay $15,879,945 in restitution. He had previously pled guilty to wire fraud, bank fraud, and making false statements to a federally insured financial institution. On June 22, 2018, a former title company employee was sentenced to 4 years and 2 months in prison for her role in the scheme. She was also ordered to pay $15,387,945 in restitution.

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 the 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 entire scheme, involving at least six properties in the Sacramento area, resulted in a loss to various financial institutions of over $22 million.

***Source:*** *FDIC OIG.*
***Responsible Agencies:*** *This is a joint investigation by the FDIC OIG, FBI, and Internal Revenue Service—Criminal Investigation (IRS-CI). The case was prosecuted by the USAO for the Eastern District of California.*

### Former President and Chief Executive Officer of Coastal Bank & Trust Sentenced for Bank Fraud Conspiracy and Obstruction

On June 5, 2018, the former president and chief executive officer (CEO) of Coastal Bank & Trust, (CB&T) was sentenced to 48 months in prison followed by 3 years of supervised release for conspiracy to commit bank fraud and obstruction of a federal bank examination. He was also ordered to pay $2,397,475 in restitution. He formerly pled guilty to the charges in May 2017.

According to court records, in June 2013, it was discovered that the former bank president had engaged in a scheme to defraud CB&T by engineering fraudulent loan transactions with straw borrowers where the true beneficiaries of the loans were co-conspirators, businesses controlled by the bank president, or the bank president himself. The fraudulent loans included unsecured lines of credit, small business loans, and mortgages for commercial and residential properties. The bank president used his position of trust and authority at CB&T to circumvent the bank's internal controls and normal loan underwriting procedures. To conceal his scheme, he withheld relevant information about the loans from CB&T's board of directors and examiners from the Board of Governors of the Federal Reserve System. CB&T suffered losses of approximately $2.4 million as a result of his conduct.

***Source:*** *Board of Governors of the Federal Reserve System (FRB) OIG.*
***Responsible Agencies:*** *This was a joint investigation by the FDIC OIG, FBI, and the FRB OIG. The case was prosecuted by the USAO for the Eastern District of North Carolina.*

### Former Charity Executive Pleads Guilty to Bribery and Embezzlement Scheme

On June 7, 2018, a former charity executive from Arkansas pled guilty to one count of federal program bribery.

The former executive of a Springfield, Missouri, charity, Preferred Family Healthcare Inc., oversaw the charity's operations and lobbying efforts in Arkansas. During his time as an executive, he, along with other Preferred Family Healthcare executives, paid bribes to Arkansas State Senator Jonathan Woods, Arkansas State Legislator Henry Wilkins IV, and others in order to provide favorable legislative action for himself, his clients, and the nonprofit he oversaw. As a result, officials steered Arkansas General Improvement Fund money to Preferred Family Healthcare and the former executive's other clients; held up agency budgets; requested legislative audits; and sponsored, filed, and voted for bills that favored the charity and his clients.

These extra funds allowed the former executive and other executives of the charity to embezzle, steal, and enrich themselves at the expense of the charity.

The former executive also paid over $600,000 in illegal kickbacks to another charity executive in exchange for more than $3.5 million in payments to benefit his coalition. He also admitted to his role in a second illegal kickback scheme involving the charity's contract with a Pennsylvania-based political operative and another charity employee. In exchange for facilitating the charity's contract with the political operative, under which the individual earned nearly $1 million, the former charity executive received kickbacks of over $200,000 from the political operative, and the other charity employee received over $60,000. In separate but related cases, both the political operative and the other charity employee previously entered guilty pleas acknowledging their roles in that kickback scheme.

The former charity executive has not yet been sentenced.

***Source:*** *USAO.*
***Responsible Agencies:*** *This is a joint investigation by the FDIC OIG, IRS-CI, FBI, and the Offices of Inspector General from the Departments of Labor, Health and Human Services, Housing and Urban Development, and Veterans Affairs. The combined investigation involved the Western District of Arkansas, the Eastern District of Arkansas, and the Eastern District of Pennsylvania. The case is being prosecuted by the USAO for the Western District of Missouri and the DOJ Criminal Division's Public Integrity Section.*

### Indiana Man Sentenced to 14 Months in Prison and Ordered to Pay Over $1 Million in Restitution

On June 22, 2018, a Crown Point, Indiana, man was sentenced to 14 months in prison followed by 24 months of home detention after previously pleading guilty to conspiracy to commit mail fraud. He was also ordered to pay $1,004,991 in restitution.

According to case documents, in 2006 and 2007 the Indiana man worked with a mortgage broker in Texas to purchase 14 residential properties in Northwest Indiana in the span of 30 days with no money down. The Indiana man would obtain mortgages that the broker found for him, closing on properties roughly twice a week over a one-month period. They knew that by closing on the properties so quickly, mortgages the Indiana man obtained in early January 2007 would not hit his credit report for at least 30 days. As a result, subsequent lenders, including lenders who purchased these mortgages in the secondary market, would be deprived of material information they would want and need to know about his debts for purposes of evaluating credit worthiness. The broker participated in the scheme for the commission he received on the mortgages the Indiana man obtained.

The mortgage broker was sentenced on February 22, 2018, to a 14-month prison term, 2 years of supervised release, and ordered to pay $1,004,991 in restitution.

***Source:*** *USAO for the Northern District of Indiana.*
***Responsible Agencies:*** *This case was investigated by the FDIC OIG. The case was prosecuted by the USAO for the Northern District of Indiana.*

### Former CEO and Chief Loan Officer of Failed Sonoma Valley Bank, and Borrower's California Attorney Sentenced to Multi-Year Prison Terms for Bank Fraud and Other Crimes

On August 3, 2018, the former CEO and former chief loan officer (CLO) of Sonoma Valley Bank were sentenced for their December 2017 convictions for conspiracy, bank fraud, wire fraud, money laundering, falsifying bank records, lying to bank regulators, and other crimes. An attorney for a real estate developer involved in the scheme was also sentenced for his conviction on bank fraud, wire fraud, attempted obstruction of justice, and other offenses. The court sentenced the former CEO to 100 months in prison, the former CLO to 100 months in prison, and the attorney to 80 months in prison. The individuals were ordered to pay the government more than $19 million for their roles in the scheme.

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 CLO recommended that the bank approve multi-million dollar loans to straw borrowers. The former CLO 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 CLO 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 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:*** *The FDIC's Division of Resolutions and Receiverships (DRR).*
***Responsible Agencies:*** *This is a joint investigation by the FDIC OIG, Special Inspector General for the Troubled Asset Relief Program (SIGTARP), and the Federal Housing Finance Agency (FHFA) 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 was prosecuted by the USAO for the Northern District of California.*

### Thousand Oaks Man Sentenced to Nearly 5 Years in Federal Prison in $11 Million Bank Fraud Case

On August 27, 2018, a California man was sentenced to 57 months in prison for his role in a bank fraud scheme where he fraudulently obtained more than $11 million in loans to purchase a gas station and car washes. He was also ordered to pay $5,737,585 in restitution to the victim financial institutions.

The California man submitted false information to banks in 2006 and 2007 to obtain the loans, the proceeds of which he used to purchase a gas station in Santa Paula, California, and two car washes in South Los Angeles. The banks suffered losses when he later defaulted on the loans. One of the banks, Mirae Bank, failed as a result of his fraudulent conduct.

The California man was initially charged in 2014, but he fled to Iran for nearly 4 years before surrendering in February 2018. At least one bank insider also participated in the scheme, pled guilty, and is awaiting sentencing.

***Source:*** *The FDIC's RMS and DRR.*
***Responsible Agencies:*** *This was a joint investigation by the FDIC OIG, FBI, FHFA OIG, and SIGTARP. The case was prosecuted by the USAO for the Central District of California.*

### Former Center Point Bank Vice President Pleads Guilty to Aiding and Abetting the Obstruction of an FDIC Examination

On August 27, 2018, a former vice president at Center Point Bank & Trust pled guilty to aiding and abetting the obstruction of an FDIC examination. At his plea hearing, the former vice president admitted that he backdated a refinancing loan to obstruct an FDIC investigation.

The former bank executive faces a possible maximum sentence of 5 years' imprisonment, a $250,000 fine, and 3 years of supervised release following any imprisonment. A sentencing date has not yet been set.

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

### Former Insurance Agent Sentenced to Prison for Fraud Scheme

On September 7, 2018, a former Northern Virginia insurance agent was sentenced to 2 years in prison for engaging in an insurance fraud scheme involving a loss of approximately $182,000.

The former insurance agent was convicted on February 1. According to court records, the former insurance agent sold a life insurance policy to her close friend. The policy included an accelerated death benefit option that permitted the holder to claim the proceeds before death in the event the holder was ever diagnosed with a terminal illness. The close friend was diagnosed with a terminal illness a few months later.

Shortly thereafter, the former insurance agent engaged in a scheme to fraudulently obtain the proceeds of the insurance policy for herself. She changed information on the policy and submitted a claim for the accelerated death benefit without her friend's knowledge or consent. The insurance company paid the claim, and the former insurance agent deposited the proceeds into her own account. She then transferred the bulk of the money through several accounts in an apparent attempt to prevent the transaction from being reversed.

***Source:*** *Financial Institution.*
***Responsible Agencies:*** *This was a joint investigation by the FDIC OIG and FBI's Washington Field Office. The case was prosecuted by the USAO for the Eastern District of Virginia.*

## 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, Colorado, 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.

| | |
|---|---|
| **New York Region** | Financial Fraud Enforcement Task Force; 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** | Minnesota Inspector General Council; Minnesota Financial Crimes Task Force; Kansas City SAR Review Team; 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; 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** | 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, investigations, and other reveiws 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, FDIC Director, 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 Director, 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 FDIC Director 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, evaluation, and other work; monitoring FDIC-related hearings on issues of concern to various oversight Committees; and coordinating with the FDIC's Office of Legislative Affairs on any Congressional correspondence pertaining to the OIG.
- Briefed Senate Committee on Homeland Security and Governmental Affairs Minority Staff on the FDIC OIG's assessment of Top Management and Performance Challenges facing the FDIC and our Special Inquiry report on *The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches*. Also briefed Majority and Minority staffs of the House Committee on Science, Space, and Technology, and the Senate Committee on Banking, Housing, and Urban Affairs on the Special Inquiry report.

- Maintained the OIG Hotline to field complaints and other inquiries from the public and other stakeholders. The OIG's Whistleblower Protection Coordinator 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. Publicized Whistleblower Appreciation Day to OIG staff on July 30.
- 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, Inspection and Evaluation Committee, Investigations Committee, Professional Development Committee, Legislation 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 Legislation Committee. Helped plan CIGIE's IG Act 40th Anniversary event.
- Participated on 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 the Council's issuance of the *Top Management and Performance Challenges Facing Financial Regulatory Organizations*.
- Coordinated with the Government Accountability Office (GAO) on ongoing efforts related to the annual financial statement audit of the FDIC, including meeting to discuss the risk of fraud at the FDIC, and on other GAO work of mutual interest.
- Coordinated with the Office of Management and Budget to address budget matters of interest.
- 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. Joined law enforcement partners in numerous financial, mortgage, and cyber fraud-related working groups nationwide. Formed part of the planning team and made presentations at the 2018 FDIC/DOJ Financial Crimes Conference.
- 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.**

- Continued efforts by 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, and IT governance and related policies and procedures. A key focus during the reporting period has been on the OIG's Email to the Cloud initiative.
- Conducted mandatory training for all OIG staff on Protecting Sensitive Information, with particular attention to the various types of information the OIG handles in its day-to-day work and the controls needed to safeguard such information. Supplemented training with additional communications to staff throughout the reporting period.
- Relied on the OIG's Office of General Counsel 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 the Assistant Inspector General for Program Audits and Evaluations, Senior Criminal Investigator, Special Agent, Financial Management Analyst, and two Associate Counsel.
- 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, with particular attention to expenses involved in procuring equipment, software, and services to improve the OIG's IT environment.
- Continued to analyze OIG business processes to evaluate the OIG's Electronic Crimes Unit lab and make needed enhancements to best serve Office needs.

### Exercising leadership skills and promoting teamwork.

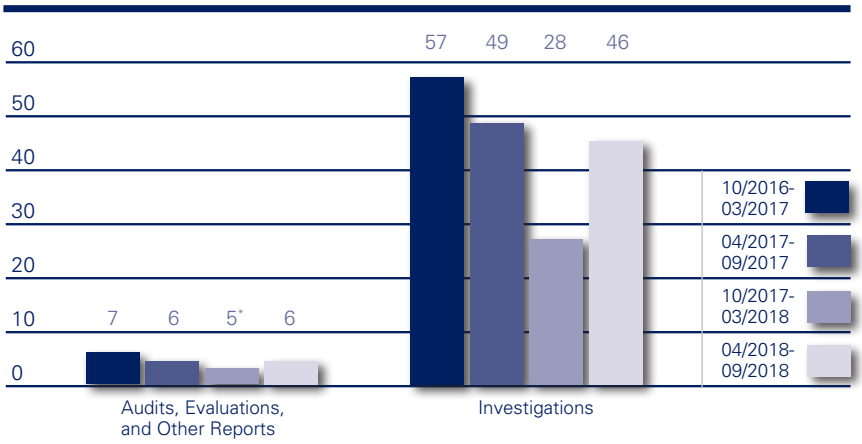
- Held an OIG-wide conference emphasizing leadership and teamwork: *One Mission. One Team*. Topics covered leading at all levels, communicating within teams, diversity and inclusion, unconscious bias, and ethics. The Comptroller General and the Chairman of the FDIC were keynote speakers.
- Continued 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.
- Continued to develop 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.
- Offered multiple POWER Lunch and Learn sessions to all OIG staff to enhance their knowledge of, and leadership in, such areas as Blockchain Technology, Oversight.gov, the role of the Partnership for Public Service, and examples of fellowship opportunities for federal employees.

- Formed working groups to leverage skills and knowledge in addressing office priorities—for example, a group comprised of senior staff who examined audit and evaluation assignment processes and reporting in the interest of a more efficient and effective manner of conducting assignments and reporting results.
- 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 awarded three types of OIG special awards to recognize outstanding efforts: Distinguished Professional Award, Spirit of the OIG Award, and IG Awards for Excellence. Also nominated OIG 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.
- Fostered a sense of teamwork and mutual respect through the establishment of the OIG's Diversity and Inclusiveness Working Group. Also launched the OIG Solutions Box to provide all staff a mechanism to suggest positive improvements to the workplace.

Cumulative Results
(2-year period)

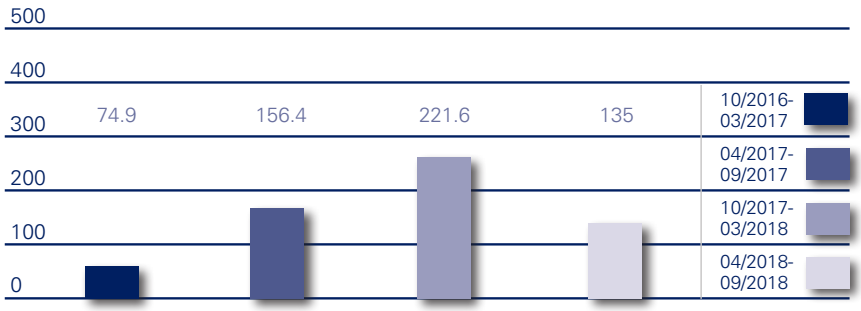
| Nonmonetary Recommendations | |
|---|---|
| October 2016 – March 2017 | 27 |
| April 2017 – September 2017 | 36 |
| October 2017 – March 2018 | 33 |
| April 2018 – September 2018 | 29 |

## Reports Issued and Investigations Closed




**Does not include two Failed Bank Review reports.*

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



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

| Reporting Requirements | Page |
|---|---|
| **Section 4(a)(2)** Review of legislation and regulations. | 33 |
| **Section 5(a)(1)** Significant problems, abuses, and deficiencies. | 6-16 |
| **Section 5(a)(2)** Recommendations with respect to significant problems, abuses, and deficiencies. | 6-16 |
| **Section 5(a)(3)** Recommendations described in previous semiannual reports on which corrective action has not been completed. | 34 |
| **Section 5(a)(4)** Matters referred to prosecutive authorities. | 47 |
| **Section 5(a)(5)** Summary of each report made to the head of the establishment regarding information or assistance refused or not provided. | 47 |
| **Section 5(a)(6)** Listing of audit, inspection, and evaluation reports by subject matter with monetary benefits. | 44 |
| **Section 5(a)(7)** Summary of particularly significant reports. | 6-16 |
| **Section 5(a)(8):** Statistical table showing the total number of audit reports and the total dollar value of questioned costs. | 45 |
| **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. | 46 |
| **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 | 46 |
| • no establishment comment was received within 60 days of providing the report to management | 46 |
| • there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations. | 34-43 |
| **Section 5(a)(11)** Significant revised management decisions during the current reporting period. | 47 |

| Reporting Requirements (continued) | Page |
|---|---|
| **Section 5(a)(12)** Significant management decisions with which the OIG disagreed. | 47 |
| **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. | 51 |
| **Section 5(a)(17):** Statistical tables showing, for the reporting period:<br>• number of investigative reports issued<br>• number of persons referred to the DOJ for criminal prosecution<br>• number of persons referred to state and local prosecuting authorities for criminal prosecution<br>• number of indictments and criminal Informations. | 47 |
| **Section 5(a)(18)** A description of metrics used for Section 5(a)17 information. | 47 |
| **Section 5(a)(19)** A report on each OIG investigation involving a senior government employee where allegations of misconduct were substantiated, including<br>• the facts and circumstances of the investigation<br>• 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. | 48 |
| **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. | 48 |
| **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. | 48 |
| **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. | 48 |

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 or proposed legislative matters, including the following:

#### Legislation, Statutes, and Related Documents

- Draft legislation: *The Executive Branch Waste and Fraud Recovery Act*, which would direct an agency to seek recoupment when the agency's IG determines that a political appointee at the agency made expenditures that were either unlawful or inconsistent with applicable regulations or agency policies. Office of General Counsel (OGC) provided comments to the CIGIE Legislation Committee.
- S. 2498, the *Payment Integrity Information Act of 2018*, which seeks to improve efforts to identify and reduce Government-wide improper payments. OGC reviewed the bill as introduced and had no comments; OGC had reviewed and commented on a draft version of the legislation and noted that such comments had been considered and adopted.
- S. 2178, the *Inspector General Recommendation Transparency Act of 2018*, which deals with OIGs' reporting on open (unimplemented) OIG recommendations. OGC reviewed a proposed edit from the Legislation Committee, which was advised that the FDIC OIG had no further comments.
- H.R. 6891, the *Anti-Deficiency Reform and Enforcement Act of 2018*, which would give the IGs a role in Anti-Deficiency Act reviews and would impose new IG reporting requirements in the semiannual reports to Congress. OGC provided comments to CIGIE Legislation Committee staff.
- Public Law No. 115-174, the *Economic Growth, Regulatory Relief, and Consumer Protection Act* (S. 2155). This statute contains various provisions affecting lending, housing, banking, and financial regulation but does not have IG-specific requirements. OGC and the Immediate Office prepared an analysis of the Act for OIG management's consideration.
- Provided information to the CIGIE Legislation Committee in connection with the Committee's efforts regarding the Program Fraud Civil Remedies Act.

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

We have closed the two recommendations that were included in this table in our previous Semiannual Report. We have no items to report for the current reporting period.

## Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods

| Report Number, Title, and Date | Report Summary | Recommendations Total | Recommendations Outstanding | Potential Cost Savings |
|---|---|---|---|---|
| AUD-16-001<br>**FDIC's Information Security Program – 2015**<br>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.<br><br>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.<br><br>The report contained six recommendations to improve the effectiveness of the FDIC's information security program controls and practices. | 6 | 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<br>**Audit of the FDIC's Information Security Program - 2016**<br>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.<br><br>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 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.<br><br>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.<br><br>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 | 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-17-004<br>**Technology Service Provider Contracts with FDIC-Supervised Institutions**<br>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. Based on results from two prior evaluations, we determined that greater scrutiny of the sufficiency of TSP contracts with FDIC-supervised institutions was warranted.<br><br>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.<br><br>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 FIs' 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 FIs' interests.<br><br>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.<br><br>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 to which FIs 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<br>**Follow-on Audit of the FDIC's Identity, Credential, and Access Management (ICAM) Program**<br>November 2, 2016 | 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 (HSPD)-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.<br><br>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.<br><br>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.<br><br>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-17-007<br>**Controls over Separating Personnel's Access to Sensitive Information**<br>February 14, 2017 | The FDIC experienced a number of data breaches in late 2015 and early 2016 that involved employees who were exiting the Corporation. In response, the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs requested that the FDIC OIG examine issues related to the FDIC's policies governing departing employees' access to sensitive financial information.<br><br>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.<br><br>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.<br><br>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.<br><br>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 | 3 | 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<br>**The FDIC's Processes for Responding to Breaches of Personally Identifiable Information**<br>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.<br><br>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.<br><br>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 those 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.<br><br>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 | 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-18-001<br>**Audit of the FDIC's Information Security Program – 2017**<br>October 25, 2017 | The FDIC OIG engaged the professional services firm of Cotton & Company LLP (C&C) to conduct an audit to evaluate the effectiveness of the FDIC's information security program and practices.<br><br>The audit included a review of selected security controls related to three general support systems, one business application, and the FDIC's risk management activities pertaining to four outsourced information service providers. As part of its work, C&C developed responses to security-related questions contained in the Department of Homeland Security's document, entitled *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V 1.0*, dated April 17, 2017 (the IG FISMA Reporting Metrics).<br><br>C&C's report describes 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. C&C reported a total of 19 findings, of which 14 were identified during the current year FISMA audit and the other 5 were identified in prior reports issued by the OIG or the Government Accountability Office.<br><br>C&C's report contained 18 recommendations addressed to the FDIC's Chief Information Officer that were intended to improve the effectiveness of the FDIC's information security program and practices. | 18 | 7 | NA |

| Table II: Outstanding Unimplemented Recommendations from Previous Semiannual Periods | | | | |
|---|---|---|---|---|
| **Report Number, Title, and Date** | **Report Summary** | **Recommendations** | | **Potential Cost Savings** |
| | | **Total** | **Outstanding** | |
| AUD-18-002<br>**Material Loss Review of First NBC Bank, New Orleans, Louisiana**<br>November 3, 2017 | First NBC Bank (First NBC) failed on April 28, 2017, resulting in a $996.9 million loss to the Deposit Insurance Fund (DIF). Our audit objectives were to (1) determine the causes of First NBC's failure and the resulting material loss to the DIF and (2) evaluate the FDIC's supervision of First NBC, including the FDIC's implementation of the Prompt Corrective Action (PCA) provisions of Section 38 of the Federal Deposit Insurance Act.<br><br>We concluded that First NBC's failure exhibited many characteristics of previous failures. These characteristics included 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.<br><br>With respect to supervision, we found that the FDIC conducted examination activities, as required, and properly implemented applicable PCA provisions. However, the FDIC's use of enforcement actions and assignment of examination ratings was counter to the agency's forward-looking supervisory approach.<br><br>We made two recommendations aimed at ensuring the lessons learned from this failure would be appropriately embedded in the FDIC's supervision program. | 2 | 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-18-001<br>**FDIC's Implementation of Consumer Protection Rules Regarding Ability to Repay Mortgages and Compensation for Loan Originators**<br>December 6, 2017 | The objective of this evaluation was to assess the FDIC's implementation of selected consumer protection rules. We focused on two rules that placed new requirements on the banking industry to (1) determine if a consumer had a reasonable ability to repay a mortgage loan and (2) limit loan originator compensation and subject loan originators to new requirements.<br><br>We found that the Division of Depositor and Consumer Protection (DCP) took steps to implement these rules. DCP incorporated the rules into its examination program, trained its examiners, communicated regulatory changes to FDIC-supervised institutions, and tracked rule violations. We also found that the FDIC should enhance its program monitoring efforts by researching the reasons for regional variances in complying with the rules, tracking how many institutions are subject to the rules, tracking how frequently examiners review compliance with the rules, and improving workpaper documentation.<br><br>The report contained four recommendations to strengthen DCP's compliance examination process. | 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-18-002<br>**Claims Administration System Functionality**<br>March 16, 2018 | The Claims Administration System (CAS) is a mission-critical system that Division of Resolutions and Receiverships (DRR) personnel use to identify insured and uninsured deposits in failing and failed financial institutions.<br><br>We evaluated the extent to which CAS had achieved DRR performance expectations for capacity, timeliness, and accuracy in making insurance determinations.<br><br>CAS substantially met the FDIC's expectations for capacity, timeliness, and accuracy in making insurance determinations for most insured institutions. However, we noted that CAS may not be able to meet the FDIC's expectations for capacity and timeliness for some large institutions. Recognizing the difficulties in resolving a large institution over a closing weekend, the FDIC issued rules intended to mitigate potential shortfalls in CAS capacity, but at a cost to the banking industry. Accordingly, the largest financial institutions are required to configure their information systems and data to enable the FDIC to make insurance determinations by April 2020. However, further simulation and testing for failing and failed large bank scenarios would provide the FDIC with greater certainty of CAS's capabilities. In comparison with the predecessor system, CAS improved the timeliness of insurance determinations through process automation and ongoing system improvements and has reduced the risk of inaccurate insurance determinations.<br><br>We made three recommendations to improve CAS functionality through additional testing. | 3 | 1 | 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** | | | | |
| EVAL-18-004<br>August 8, 2018 | *Forward-Looking Supervision* | | | |
| **Consumer Protection** | | | | |
| EVAL-18-003<br>May 2, 2018 | *Processing of Consumer Complaints* | | | |
| **Information Technology and Cybersecurity** | | | | |
| AUD-18-004<br>July 26, 2018 | *The FDIC's Governance of Information Technology Initiatives* | | | |
| **Totals for the Period** | | **$0** | **$0** | **$0** |

Other products issued:

- *Special Inquiry: The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches*
  OIG-18-001
  April 16, 2018
- *Infrastructure Support Contract 3 (ISC-3) with CSRA, Inc.*
  PAE Memorandum 18-001
  July 2, 2018
- *Employee-Initiated Transfers and Associated Travel*
  PAE Memorandum 18-002
  September 10, 2018

| Table IV: Audit and Evaluation Reports Issued with Questioned Costs | | | |
|---|---|---|---|
| | | Questioned Costs | |
| | Number | 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 the 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 | 46 |
| Number of Persons Referred to the Department of Justice for Criminal Prosecution | 52 |
| Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution | 2 |
| Number of Indictments and Criminal Informations | 28 |

**Description of the metrics used for the above information:** Reports issued reflects case closing memorandums issued to FDIC management. With respect to the 52 referrals to the Department of Justice, the total represents 42 individuals and 10 business entities. Two individuals were referred to state and local prosecutors. Our total indictments and criminal Informations includes indictments, Informations, and superseding indictments, as applicable.

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

During this reporting period, there were no investigations involving senior government employees where allegations of misconduct were substantiated.

## 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 and not disclosed to the public. There were no investigations involving senior government employees that were 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)

When the DIF incurs a loss under $50 million, Section 38(k) of the Federal Deposit Insurance Act requires the Inspector General of the appropriate federal banking agency to determine the grounds upon which the state or federal banking agency appointed the FDIC as receiver and whether any unusual circumstances exist that might warrant an in-depth review of the loss.

The FDIC OIG issued its most recent Failed Bank Review on February 14, 2018, that of Farmers and Merchants Bank, Argonia, Kansas, which failed on October 13, 2017. There have been no failures of FDIC-supervised financial institutions since that time. The OIG has no Failed Bank Reviews in process or pending.

# Appendix 3

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.

• 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.

**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 a significant deficiency or significant deficiencies and concludes that (1) 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 (2) the audit organization has not complied with generally accepted government auditing standards and policies and procedures in all material respects.

## 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 "compliant" or "noncompliant" with relevant standards. These standards are based on *Quality Standards for Investigations* and applicable Attorney General Guidelines.

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

  The Department of the Treasury OIG is currently conducting a peer review of our investigative function, and we will report the results of this more recent review in our upcoming semiannual report.

- 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 to FDIC OIG CIGIE Award Winners

The FDIC OIG received four Awards for Excellence from the Council of the Inspectors General on Integrity and Efficiency (CIGIE) at the Annual Awards Ceremony on October 17, 2018. The awards are recognition for the outstanding work and dedication of these individuals, as well as their commitment to preserving the integrity of banks and the banking system and to prompting greater efficiencies and improvements at the FDIC.

***From left: Matt Alessandrino, Sharon Tushin, Michael Eaton, Amanda King, Regina Sandler, Erin Bourassa, Fran Mace, Meg Faden, Michael Dann, IG Jay Lerner, Michael Delgado, John Carrillo, and Wade Walters. (Missing from photo: Steve Beard, Robin King, and Lisa Price)***

Congratulations to the following staff:

**John Carrillo**, for his efforts on the team investigating bank fraud involving Sonoma Valley Bank. As a result of the investigation, the former CEO and former Chief Loan Officer, as well as an attorney involved in the scheme, were convicted of charges including conspiracy, bank fraud, and other offenses. The former CEO and Chief Loan Officer were each sentenced to 100 months in prison, and the attorney was sentenced to 80 months in prison. The actions of these individuals contributed, in part, to the failure of Sonoma Valley Bank, which caused more than $20 million in losses, approximately $11.47 million to the FDIC, and $8.65 million to the Troubled Asset Relief Program.

**Michael Delgado**, for his contributions to an investigative team examining commercial loan fraud. The investigation revealed that over a three-year period, the former presidents of two companies fraudulently obtained approximately $190 million from banks and financing companies, eventually causing the lenders to lose at least $100 million. One of the presidents was sentenced to 60 months in prison, and the other was sentenced to 36 months; they were ordered to pay restitution of more than $97 million for their respective roles in the scheme. Michael was also part of another team selected for an Award for Excellence for its work on a case involving SBA loans obtained through the American Enterprise Bank in Illinois.

**Fran Mace** and **Meg Faden**, for their contributions to an investigation related to the Bank Secrecy Act (BSA) violations committed by Banamex USA (BUSA). Based upon the team's efforts, BUSA entered into a non-prosecution agreement to resolve the investigation. BUSA also agreed to pay $140 million in civil money penalties in connection with BSA deficiencies, and agreed to forfeit more than $97 million. Also, four former senior BUSA executives were removed from the banking industry.

**Regina Sandler**, **Amanda King**, **Michael Eaton**, **Michael Dann**, **Lisa Price**, **Tony Lehr** (formerly of the OIG), **Erin Bourassa**, **Robin King**, **Stephen Beard**, and **Sharon Tushin**, for their work in reviewing the FDIC's handling of data security incidents and breaches at the FDIC in 2015 and 2016, and the FDIC's statements and document productions to the Congress regarding those breaches.

## Farewell to Retirees

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

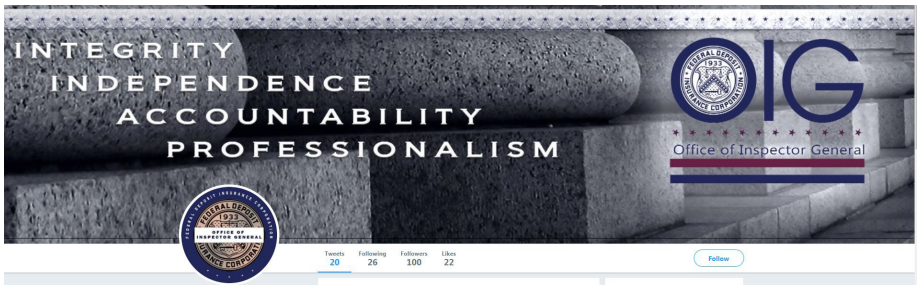
**Steve Overby**
Special Agent
Office of Investigations

**Christian Gieseler**
Associate Counsel
Office of General Counsel

# 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

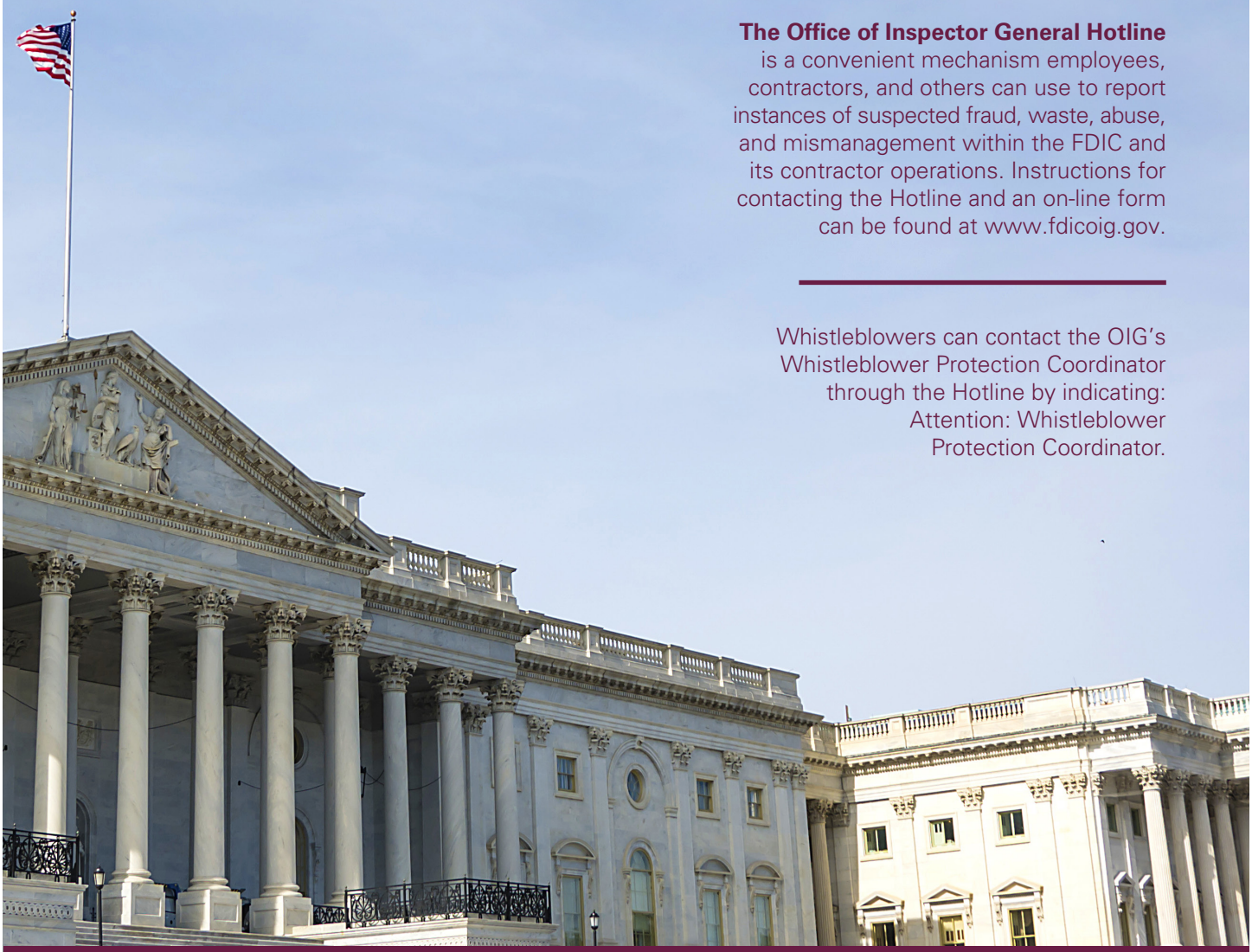
OVERSIGHT.GOV
ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE

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 Protection Coordinator through the Hotline by indicating: Attention: Whistleblower Protection Coordinator.



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

FDIC-039-2018