JULY 2018

Annual Report of the Council of Inspectors General on Financial Oversight

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Message from the Chair

In keeping with its mission, the Council of Inspectors General on Financial Oversight (CIGFO), which is authorized to oversee the Financial Stability Oversight Council (FSOC) operations, continued its work in 2017 and 2018. In its oversight role, it has, since 2011, established working groups that are comprised of staff from the CIGFO member Inspector General offices to conduct audits of FSOC operations. CIGFO convened a Working Group in December 2017 to assess FSOC's monitoring of international financial regulatory proposals and developments. According to the Dodd-Frank Wall Street Reform and Consumer Protection Act, one of FSOC's duties is to monitor domestic and international financial regulatory proposals and developments, including insurance and accounting issues, and to advise Congress and make recommendations in such areas that will enhance the integrity, efficiency, competitiveness, and stability of U.S. financial markets. The working group's audit is expected to be completed in 2018.

In addition to this oversight activity, CIGFO continued monitoring activities to include sharing financial regulatory information which enhanced Inspectors General knowledge and insight about specific issues related to members' current and future work. For example, during its quarterly meetings, CIGFO members discussed the implementation of the Cybersecurity Information Sharing Act, Treasury's efforts to fulfill the directives outlined in the President's Executive Order on Core Principles for Regulating the U.S. Financial System, as well as other legislative activities that could impact the financial regulatory system.

In the coming year, CIGFO members will continue, through their individual and joint work, to help strengthen the financial system by oversight of FSOC and its Federal member agencies.

/s /

Eric M. Thorson
Chair, Council of Inspectors General on Financial Oversight
Inspector General, Department of the Treasury

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Table of Contents

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Council of Inspectors General on Financial Oversight

The Council of Inspectors General on Financial Oversight (CIGFO) was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), and meets on a quarterly basis to facilitate the sharing of information among Inspectors General. The CIGFO members discuss the ongoing work of each Inspector General who is a member of the Council, with a focus on concerns that may apply to the broader financial sector, and exchange ideas about ways to improve financial oversight. The CIGFO publishes an annual report that includes separate sections within the exclusive editorial control of each Inspector General. Those sections describe the concerns and recommendations of each Inspector General and a discussion of ongoing and completed work.

During the course of the year, the CIGFO continued to monitor coordination efforts among and between Financial Stability Oversight Council (FSOC) members. Specifically, CIGFO members discussed the following:

- Office of Financial Research's activities and proposed restructuring
- FSOC's proposal to modify its process to designate financial institutions
- FSOC's annual reevaluation of nonbank financial company designations

CIGFO recognizes that it has been 8 years since the Dodd-Frank Act was enacted and agency implementation of different provisions of the Act continues. CIGFO encourages FSOC to continually assess its processes and procedures to ensure the Act is applied in a fair, consistent, and transparent manner.

The Council of Inspectors General on Financial Oversight Audits

The Dodd-Frank Act authorizes the CIGFO to convene a working group, by a majority vote, for the purpose of evaluating the effectiveness and internal operations of the FSOC.

To date, CIGFO has conducted the following audits—

- **2012**- *Audit of the Financial Stability Oversight Council's Controls over Non-public Information*
- **2013**- *Audit of the Financial Stability Oversight Council's Designation of Financial Market Utilities*
- **2014**- *Audit of the Financial Stability Oversight Council's Compliance with Its Transparency Policy*
- **2015**- *Audit of the Financial Stability Oversight Council's Monitoring of Interest Rate Risk to the Financial System*
- **2017**- *Audit of the Financial Stability Oversight Council's Efforts to Promote Market Discipline*
- **2017**- *Corrective Action Verification of FSOC's Implementation of CIGFO's Audit Recommendations in the 2013 Audit of FSOC's Financial Market Utility Designation Process*

The corrective actions described by FSOC, with respect to the audits listed above, met the intent of our recommendations, and may be subject to verification in future CIGFO working group reviews.

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Office of Inspector General Board of Governors of Federal Reserve System and Bureau of Consumer Financial Protection

The Office of Inspector General (OIG) provides independent oversight by conducting audits, inspections, evaluations, investigations, and other reviews of the programs and operations of the Board of Governors of the Federal Reserve System (Board) and the Bureau of Consumer Financial Protection (Bureau) and demonstrates leadership by making recommendations to improve economy, efficiency, and effectiveness, and by preventing and detecting fraud, waste, and abuse.

I. Background

Congress established the OIG as an independent oversight authority for the Board, the government agency component of the broader Federal Reserve System, and the Bureau.

Under the authority of the Inspector General Act of 1978, as amended (IG Act), the OIG conducts independent and objective audits, inspections, evaluations, investigations, and other reviews related to the programs and operations of the Board and the Bureau.

- We make recommendations to improve economy, efficiency, and effectiveness, and we prevent and detect fraud, waste, and abuse.
- We share our findings and make corrective action recommendations to the Board and the Bureau, but we do not have the authority to manage agency programs or implement changes.
- We keep the Board's Chair, the Bureau's Director, and Congress fully informed of our findings and corrective action recommendations, as well as the agencies' progress in implementing corrective action.

In addition to the duties set forth in the IG Act, Congress has mandated additional responsibilities for the OIG. Section 38(k) of the Federal Deposit Insurance Act (FDI Act) requires that the OIG review failed financial institutions supervised by the Board that result in a material loss to the Deposit Insurance Fund (DIF) and produce a report within 6 months. The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) amended section 38(k) of the FDI Act by raising the materiality threshold and requiring the OIG to report on the results of any nonmaterial losses to the DIF that exhibit unusual circumstances warranting an in-depth review.

Section 211(f) of the Dodd-Frank Act also requires the OIG to review the Board's supervision of any covered financial company that is placed into receivership under title II of the act and produce a report that evaluates the effectiveness of the Board's supervision, identifies any acts or omissions by the Board that contributed to or could have prevented the company's receivership status, and recommends appropriate administrative or legislative action.

The Federal Information Security Modernization Act of 2014 (FISMA) established a legislative mandate for ensuring the effectiveness of information security controls over resources that support federal operations and assets. In a manner consistent with FISMA requirements, we perform annual independent reviews of the Board's and the Bureau's information security programs and practices, including the effectiveness of security controls and techniques for selected information systems.

II. OIG Reports and Other Products Related to the Broader Financial Sector

In accordance with section 989E(a)(2)(B) of the Dodd-Frank Act, the following highlights the completed and ongoing work of our office, with a focus on issues that may apply to the broader financial sector.

Completed work

Major Management Challenges for the Board and the Bureau

Although not required by statute, we annually report on the major management challenges facing the Board and the Bureau. These challenges identify the areas that, if not addressed, are most likely to hamper the Board's and the Bureau's accomplishment of their strategic objectives.

Among other items, we identified five major management challenges for the Board that apply to the financial sector in 2017:

- Enhancing Governance, Including Using an Enterprise Approach to Carry Out Agency wide Functions
- Enhancing Oversight of Cybersecurity at Supervised Financial Institutions
- Ensuring an Effective Information Security Program
- Continuing to Strengthen the Regulatory and Supervisory Framework While Remaining Sufficiently Nimble to Address Potential Internal or External Developments
- Managing the Handling and Release of Sensitive Federal Open Market Committee and Board- Generated Information

Among other items, we identified four major management challenges for the Bureau that apply to the financial sector in 2017:

- Ensuring an Effective Information Security Program
- Maturing the Human Capital Program
- Strengthening the System of Internal Controls
- Effectively Managing and Acquiring Workspace

The Board's Organizational Governance System Can Be Strengthened, OIG Report 2017-FMIC-B-020, December 11, 2017

An organization's governance system determines how decision-making, accountability, controls, and behaviors help accomplish its objectives. Our evaluation (1) describes the current state of the Board's organizational governance structures and processes and (2) assesses the extent to which these structures and processes align with those of other relevant institutions and with governance principles.

The Board's core organizational governance structure aligns with benchmark institutions and selected governance principles, as does its public disclosure of governance documents.

Nonetheless, the Board can strengthen its governance system by

- clarifying and regularly reviewing purposes, roles and responsibilities, authorities, and working procedures of its standing committees
- enhancing the orientation program for new Governors and reviewing and formalizing the process for selecting dedicated advisors
- setting clearer communication expectations and exploring additional opportunities for information sharing among Governors
- reviewing, communicating, and reinforcing the Board of Governors' expectations of the Chief Operating Officer and the heads of the administrative functions
- establishing and documenting the Executive Committee's mission, protocols, and authorities

Strengthening its core governance structures should enable the Board to more efficiently and effectively achieve its objectives.

Our report contains recommendations designed to strengthen the Board's organizational governance structures. The Board generally concurred with our recommendations.

Review of the Failure of Allied Bank, OIG Report 2018-SR-B-007, March 19, 2018

After more than 100 years in business, Arkansas-based Allied Bank failed in 2016, resulting in an estimated $6.9 million loss to the DIF. In accordance with the Dodd-Frank Act, we conducted an in-depth review of the bank's failure.

Allied Bank failed because of corporate governance weaknesses and asset quality deterioration resulting from deficient credit risk-management practices. Ineffective oversight by Allied Bank's board of directors allowed two management officials to exert a dominant influence over the bank's affairs, including lending decisions, and allegedly engage in insider abuse. Allied Bank's management also failed to establish adequate credit risk-management practices commensurate with the risks in the bank's loan portfolio. Weak credit underwriting and administration practices resulted in violations of certain regulations and bank lending policies, significant loan concentrations, and an excessive volume of classified assets. The bank's asset quality deterioration significantly impaired profitability and eventually depleted the bank's capital levels, resulting in the bank's failure.

Although the Federal Reserve Bank of St. Louis took decisive supervisory action to address Allied Bank's weaknesses, it could have also recommended that the Board report suspicious activity to law enforcement when the Reserve Bank first identified signs of insider abuse. Our review resulted in a finding related to Suspicious Activity Report filings by the Federal Reserve System and a finding related to enhanced communication between the Board's Legal Division and the Reserve Banks.

Our report contains recommendations designed to improve supervisory processes and to enhance communication between the Board's Legal Division and the Reserve Banks following requests for enforcement action. The Board concurred with our recommendations.

Security Control Review of the RADAR Data Warehouse, OIG Report 2018-IT-B-006R, March 7, 2018

The Risk Assessment, Data Analysis, and Research (RADAR) Data Warehouse gives Federal Reserve System and Board staff access to mortgage and consumer data for supervision and research purposes. It has been classified as a moderate-risk system. To meet FISMA requirements, we assessed the effectiveness of select security controls for the RADAR Data Warehouse and associated query tools.

Overall, the information security controls that we tested were operating effectively. However, controls in the areas of contingency planning, configuration management, and security assessment and authorization can be strengthened.

Our report includes recommendations to strengthen the security of the RADAR Data Warehouse as well as three matters for management's consideration. The Board concurred with our recommendations.

The CFPB Can Improve Its Examination Workpaper Documentation Practices, OIG Report 2017-SR-C-016, September 27, 2017

We assessed the Bureau's guidance and practices to promote effective and consistent examination workpaper documentation. Specifically, we reviewed workpaper documentation in each of the Bureau's four regions for compliance with the *CFPB Supervision and Examination Manual* and other policies that govern examination work.

We found that, subject to certain conditions being met, the Bureau's Division of Supervision, Enforcement, and Fair Lending's (SEFL) approach was to grant examination employees in each region open access to all examination workpaper documentation and supporting materials in the initial system of record and on the current shared drive for examinations conducted in that region. One region used a similar open-access approach for the prior shared drive. This approach resulted in certain SEFL employees having access to materials with confidential supervisory information and personally identifiable information when they did not appear to have a business need to know that information.

In addition, we found that file size limitations in the initial system of record led examiners to store workpapers in multiple locations. We also found opportunities to reinforce the need to store workpapers in the appropriate location and to document supervisory reviews and sampling methods. Further, we recommended that SEFL develop workpaper training and an ongoing quality review process.

Our report contains recommendations designed to improve SEFL's approach to documenting examination results and protecting sensitive information. We acknowledge that SEFL management has acted to address some of the issues discussed in this report, but we have not tested these actions to determine whether they fully address our recommendations. The Bureau concurred with our recommendations.

The CFPB Can Enhance the Effectiveness of Its Examiner Commissioning Program and On-the-Job Training Program, OIG Report 2017-SR-C-014, September 20, 2017

We evaluated the effectiveness of the Bureau's management of the Examiner Commissioning Program (ECP) and the On-the-Job Training (OJT) program. As part of this evaluation, we assessed the programs' design, implementation, and execution.

Although the Bureau has taken steps to enhance the ECP since its implementation in October 2014, we identified additional ways in which the agency could improve the program. First, some examiners appeared to be pursuing components of the ECP before being fully prepared. Second, some examiners did not appear to receive adequate training or developmental opportunities and exposure to certain Bureau internal processes before starting certain components of the ECP. Third, the Bureau did not have a formal method to evaluate and update the ECP. Fourth, the Bureau did not consistently communicate ECP requirements to prospective employees. Fifth, the ECP policy should be updated to clarify when the 5-year time requirement for examiners' obtaining their commissioning begins.

Finally, the Bureau could enhance its implementation of the OJT program. Specifically, Bureau regions have not consistently implemented the OJT program, and examiners have not clearly understood the requirements, expectations, and purpose of the program.

Our report contains recommendations designed to enhance the effectiveness of the Bureau's ECP and OJT program. The Bureau concurred with our recommendations.

The CFPB Generally Complies With Requirements for Issuing Civil Investigative Demands but Can Improve Certain Guidance and Centralize Recordkeeping, OIG Report 2017-SR-C-015, September 20, 2017

We assessed the Bureau's adherence to its policies and procedures for issuing civil investigative demands (CIDs) and its general compliance with the requirements in section 1052(c) of the Dodd-Frank Act. Specifically, our review determined whether the sampled CIDs contained the procedural elements required by the Dodd-Frank Act, including, but not limited to, the presence of certain information such as notifications of purpose, return dates, and custodians.

We found that the Bureau generally complied with the procedural elements of section 1052(c) of the Dodd- Frank Act and with internal procedures when issuing the sampled CIDs, but the agency can improve its guidance for crafting notifications of purpose associated with CIDs. During our review, we learned that in accordance with internal guidance, a CID's notification of purpose is identical to the statement of purpose in the associated investigation's opening memorandum, which may be revised later in the investigation. Internal guidance calls for broad statements of purpose, to allow for flexibility. The guidance does not expressly remind enforcement attorneys of the need for statements of purpose to be compliant with relevant case law on notifications of purpose, including any developments in such case law, or remind them to revisit the statement of purpose in a revised opening memorandum if the purposes of the investigation evolve. A potentially noncompliant notification of purpose may limit the recipient's ability to understand the basis for requests and thereby heighten the risk that the CID may face a legal challenge. In the event of such a challenge, the Bureau's ability to obtain the information needed to enforce consumer financial protection laws could be delayed, irrespective of the court's decision. Additionally, noncompliant notifications of purpose pose a reputational risk, potentially affecting interactions with CID recipients and other stakeholders. During the course of our review, the Bureau updated its internal policies to mitigate this potential risk.

We also found that the Bureau can improve its matter management system. Specifically, we found that the Office of the Executive Secretariat does not appear to maintain a complete record of all petitions and supporting documents. In addition, the Office of Enforcement does not use a centralized repository to maintain CIDs and related documentation; rather, the agency maintains CID documentation on the shared drives of multiple offices.

Our report contains a recommendation to improve the Office of Enforcement's practices for crafting notifications of purpose for CIDs to reduce the risk that notifications of purpose may result in legal challenges from CID recipients. Our report also contains recommendations for the agency to implement a centralized matter management system to ensure that official federal records are easily retrievable. The Bureau concurred with our recommendations.

The CFPB Can Improve Its Practices to Safeguard the Office of Enforcement's Confidential Investigative Information, OIG Report 2017-SR-C-011, May 15, 2017

We evaluated the Bureau Office of Enforcement's processes for protecting sensitive information to determine whether it has effective controls to manage and safeguard access to its confidential investigative information.

We found that the Office of Enforcement's sensitive information had not always been restricted to Office of Enforcement employees who needed access to that information to perform their assigned duties. This was due to the Office of Enforcement's challenges with updating access rights, as well as complications resulting from an information technology system migration. During our fieldwork, the Office of Enforcement took several steps to improve its approach to restricting access.

In addition, we found that the Office of Enforcement did not follow specific aspects of the document labeling and storage requirements contained in the Bureau's standards for handling and safeguarding sensitive information. Finally, we found that the Office of Enforcement used inconsistent naming conventions for matters across its four electronic applications and two internal drives, which hinders its ability to verify, maintain, and terminate access to files and to efficiently locate documents and data in matter folders. During our fieldwork, the Office of Enforcement took steps to improve its storage of sensitive information and its use of a consistent naming convention.

Our report contains recommendations designed to improve the Office of Enforcement's practices for managing and safeguarding confidential investigative information. The Bureau concurred with our recommendations.

ONGOING WORK

Evaluation of Knowledge Management Practices Related to the Comprehensive Liquidity Analysis and Review (CLAR)

Preserving, transferring, and maintaining institutional knowledge contributes to effective supervision, particularly in light of examiner rotation requirements and examiner turnover. This evaluation is assessing the effectiveness of the knowledge management practices related to the CLAR program.

Effectiveness of Consolidated Supervision Within the Regional Banking Organization Portfolio

This evaluation is focused on the effectiveness of Board and Federal Reserve Bank supervisory activities for regional banking organizations. We are assessing the Board's and the Reserve Banks' oversight of bank and financial holding companies that own a national bank or state nonmember bank that is regulated by another federal banking agency. We are evaluating (1) the reliance that relevant Reserve Banks place on the primary federal regulator in executing consolidated supervision and (2) the effectiveness of interagency coordination.

In-Depth Review of the Failure of Fayette County Bank

In accordance with section 38(k) of the Federal Deposit Insurance Act, as amended, when a state member bank failure occurs that does not result in a material loss to the Deposit Insurance Fund, our office conducts a failed bank review to assess whether the failure presents unusual circumstances that would warrant an in-depth review. We determined that this state member bank failure warrants an in-depth review. As a result, we are conducting an in-depth review to

- assess the Board's supervision of the failed institution, including the Board's implementation of prompt corrective action
- ascertain why the institution's problems resulted in a nonmaterial loss to the Deposit Insurance Fund
- make recommendations for preventing any such loss in the future

Evaluation of the Board's Management of Currency Shipments and Associated Continuity of Operations Program

As the issuing authority for all Federal Reserve notes, the Board is responsible for issuing and directing the shipment of Federal Reserve notes to and between the Reserve Banks. We are evaluating the efficiency and effectiveness of the Board's management of currency shipments and the associated contingency planning and continuity of operations program.

Evaluation of the Office of Consumer Response's Efforts to Share Compliant Data Within the Bureau

The Office of Consumer Response (Consumer Response) is responsible for sharing consumer complaint information with internal stakeholders in order to help the Bureau supervise companies, enforce federal consumer financial laws, and write rules and regulations. The effective sharing of consumer complaint information can help the Bureau understand the problems consumers are experiencing in the financial marketplace and identify and prevent unfair practices from occurring before they become major issues. This evaluation is assessing the effectiveness of Consumer Response's complaint-sharing efforts. Specifically, this project is examining (1) the extent to which Consumer Response is achieving its goal to share complaint data and analysis with internal stakeholders and (2) Consumer Response's controls over access and distribution of shared complaint data, which can contain sensitive consumer information.

Evaluation of the Bureau's Risk Assessment Framework for Prioritizing Examination Activities

This evaluation is assessing the Division of Supervision, Enforcement, and Fair Lending's risk assessment framework and methodology for prioritizing its examination activities at its supervised institutions. As part of our initial evaluation of the supervision program, we developed an understanding of the division's institution product line approach to prioritizing its supervisory activities and how that approach affects its staffing assignments within the Bureau's regions. This evaluation involves an in-depth assessment of the risk assessment framework, the prioritization process, and the way in which those priorities cascade to the regions. We will also assess the regional approaches to executing these priorities.

Evaluation of the Bureau's Corrective Action Follow-Up Process

This evaluation is assessing the Division of Supervision, Enforcement, and Fair Lending's corrective action follow-up process. Corrective actions are specific improvement opportunities identified during the examination process that supervised entities must address. According to the Bureau's ***Supervision and Examination Manual***, corrective actions typically include a time frame in which the supervised institution is expected to complete the required actions. Our objective is to assess the Division of Supervision, Enforcement, and Fair Lending's effectiveness in monitoring and ensuring that supervised institutions resolve these feedback items in a timely manner.

Office of Inspector General Commodity Futures Trading Commission

The CFTC OIG acts as an independent Office within the CFTC that conducts audits, investigations, reviews, inspections, and other activities designed to identify fraud, waste and abuse in connection with CFTC programs and operations, and makes recommendations and referrals as appropriate.

Background

The CFTC OIG was created in 1989 in accordance with the 1988 amendments to the Inspector General Act of 1978 (P.L. 95-452). OIG was established as an independent unit to:

- Promote economy, efficiency and effectiveness in the administration of CFTC programs and operations and detect and prevent fraud, waste and abuse in such programs and operations;
- Conduct and supervise audits and, where necessary, investigations relating to the administration of CFTC programs and operations;
- Review existing and proposed legislation, regulations and exchange rules and make recommendations concerning their impact on the economy and efficiency of CFTC programs and operations or the prevention and detection of fraud and abuse;
- Recommend policies for, and conduct, supervise, or coordinate other activities carried out or financed by such establishment for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in, its programs and operations; and
- Keep the Commission and Congress fully informed about any problems or deficiencies in the administration of CFTC programs and operations and provide recommendations for correction of these problems or deficiencies.

CFTC OIG operates independently of the Agency and has not experienced any interference from the CFTC Chairman in connection with the conduct of any investigation, inspection, evaluation, review, or audit, and our investigations have been pursued regardless of the rank or party affiliation of the target.[1] The CFTC OIG consists of the Inspector General, the Deputy Inspector General/Chief Counsel, the Assistant Inspector General for Auditing, three Attorney-Advisors (one part-time), two Auditors, one Senior Program Analyst, and an Audit Management Analyst. The CFTC OIG obtains additional audit, investigative, and administrative assistance through contracts and agreements.

1 The Inspector General Act of 1978, as amended, states: "Neither the head of the establishment nor the officer next in rank below such head shall prevent or prohibit the Inspector General from initiating, carrying out, or completing any audit or investigation…." 5 U.S.C. App. 3 sec. 3(a).

Role in Financial Oversight

The CFTC OIG has no direct statutory duties related to oversight of the futures, swaps and derivatives markets; rather, the CFTC OIG acts as an independent Office within the CFTC that conducts audits, investigations, reviews, inspections, and other activities designed to identify fraud, waste, and abuse in connection with CFTC programs and operations, and makes recommendations and referrals as appropriate. The CFTC's yearly financial statement and Customer Protection Fund audits are conducted by an independent public accounting firm, with OIG oversight.

Recent, Current or Ongoing Work in Financial Oversight

In addition to our work on CIGFO projects described elsewhere in this report, CFTC OIG worked on the following projects during the past year:

- Evaluation of CFTC Oversight of NFA

The CFTC relies on the National Futures Association (NFA), a self-regulatory organization for the U.S. futures and derivatives industry, to perform a number of delegated tasks. These delegated tasks enable CFTC to better focus its oversight responsibilities and resources on the derivatives markets. CFTC management performs periodic reviews of NFA's delivery of delegated services. OIG initiated a review to examine CFTC oversight activities of the NFA. The CFTC Division of Swap Dealer and Intermediary Oversight (DSIO) is the CFTC component charged with oversight of NFA and its duties. DSIO's Registration and Compliance Branch and Examination Branch perform the bulk of NFA oversight. Our objective was to evaluate CFTC's oversight of NFA's registration processes, examinations of Futures Commission Merchants and Swap Dealers, written reviews of NFA operations, and follow up of recommendations contained in written reviews. In addition, we evaluated the impact of NFA's efforts on CFTC staffing levels and the extent to which CFTC is able to leverage NFA's staff. A summary of our findings follows.

Daily interactions and quarterly meetings. In fulfilling oversight responsibilities, DSIO displayed a high degree of daily collaboration with NFA regarding registration and regulatory issues. Daily collaboration permits DSIO and NFA to address technical and compliance issues timely and with minimal bureaucracy. DSIO's quarterly meetings with NFA management permit DSIO to address technical and compliance issues in similar fashion.

FCM and SD examinations. While DSIO's oversight of NFA's FCM examinations appears adequate, CFTC has not finalized Swap Dealer exam criteria for financial requirements because the Commission has not yet adopted capital requirements and NFA therefore has not performed Swap Dealer financial examinations. NFA examinations are an essential part of its delegated registration authority given the significant size of the cleared swap market; a weekly average of $4.6 trillion during January 2017. In addition, NFA examinations tie directly to CFTC's objective of "strong governance and oversight of Commission registrants."

Written reviews or reports. For four of eight NFA program areas, DSIO could not show that it performed written reviews periodically. As such, DSIO cannot demonstrate how well NFA performs delegated tasks related to the Arbitration Program, CPO/CTA special provisions, Foreign Futures and Options (Part 30) programs, and the tasks falling in the catch-all category "other" (which includes NFA disciplinary proceedings and anti-money laundering programs).

For the written reviews conducted, DSIO does not rigorously follow government audit or other recognized quality standards; however, we identified no requirement that it do so. Consistently following quality standards would permit DSIO to uniformly report NFA's performance over time and facilitate recommendation follow-up.

With regard to reporting, we found no evidence that DSIO's reports were distributed to the Commission or made public. Six of ten written reviews were not distributed to NFA in final; the other four were distributed to NFA in final after the arrival of the current DSIO Director. Always providing final written reviews to NFA would permit DSIO to better communicate and prioritize findings and recommendations, to better document NFA's receipt of findings and recommendations, and would permit NFA to commit to corrective actions. While the Commission may obtain any DSIO report, we believe furnishing the Commission with final written reviews of NFA would be the better practice.

Follow-up of recommendations. Since August 2015, DSIO has closed out recommendations in four written reviews under the scope of our audit (i.e., the ones that were given to NFA). However, NFA expressed concerns regarding recommendations contained in two of the four reviews. It appears there was confusion, possibly on both sides, as to what was intended. We will be taking a look at this in the next year. We hope CFTC will be precise in any advice given, and NFA will respond precisely to any suggestions CFTC may have.

As for the rest of the reports prior to August 2015, DSIO discussed recommendations with NFA on an ongoing basis but did not formally track or otherwise document the follow-up process through recommendation closeout. DSIO does not preserve a status log of recommendations made to NFA.

The impact of NFA's efforts on CFTC staffing levels. Finally, we learned that NFA's services are essential for performing tasks beyond the CFTC's and DSIO's resources, and therefore the agency leverages NFA staff to a great extent to perform its regulatory oversight of registrants. NFA is funded through member fees and assessments. NFA pays for CFTC's oversight services; the fee is remitted to the U.S. Treasury. Nevertheless, we believe NFA should evaluate whether it may be able to obtain audit and review services more cheaply.

We issued five recommendations designed to improve CFTC's oversight of NFA:

1. Approve a plan for NFA to examine Swap Dealer members for financial requirements after the Commission adopts financial capital rules.

2. Adopt written standards for reviews of NFA, including a periodic schedule for completion.

3. Evaluate NFA's performance of delegated tasks related to the Arbitration Program, CPO/CTA special provisions, Foreign Futures and Options, and "other," or:

    - Following a study of costs, require NFA to submit its eight program areas to engagements (as scheduled) by an independent public accountant (IPA) or other suitable entity whenever it would be cost-effective for the NFA or for CFTC.

4. Furnish all final written reviews and audits to NFA and to the Commission and revisit disclosure policies.

5. Establish a system for tracking status and closing recommendations.

Management generally concurred with the recommendations, had taken corrective action(s), or planned to take corrective action(s).

- Review of the Cost-Benefit Consideration for the Margin Rule on Uncleared Swaps

The Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") was signed into law on July 21, 2010. Among its many provisions, Dodd-Frank mandated the promulgation of rules establishing margin requirements for uncleared swaps. In December 2015, the CFTC finalized its rule ("the Margin Rule") implementing the mandate. The CFTC is required by law to consider the costs and benefits of new rules. A thorough consideration of costs and benefits based on rigorous economic analysis informs regulators, Congress, and the public of the likely effects of a policy change.

Our report concluded that the CFTC lacks an institutional commitment to robust cost-benefit consideration. The cost-benefit consideration for the CFTC's Margin Rule exemplifies this shortcoming. The CFTC's cost-benefit consideration lacks a clear discussion of the market failure justifying regulatory intervention. It lightly refers to the 2007-2008 financial crisis and asserts without scrutiny that the Margin Rule will reduce systemic risk.

It makes no attempt to discern the magnitude of the risk reduction or to quantify any costs other than the cost of maintaining margin collateral. Most importantly, the cost-benefit consideration elides numerous issues and

unintended consequences that might undercut the asserted systemic risk-mitigating effects of margin or increase the burdens on market participants.

In addition, the agency's data infrastructure is inadequate, particularly with respect to the market for uncleared swaps. This inadequacy precludes a convincing analysis of costs and benefits, as well as a retrospective review of the rule's efficacy. It also hampers regulatory oversight more generally.

Based on our review, we made the following recommendations:

1. When considering the costs and benefits of a proposed rule, the CFTC should establish a baseline understanding of the marketplace; specify the market failure justifying regulatory intervention; consider whether the market failure stems from existing regulations; and apply assumptions symmetrically across policy options. The CFTC should attempt to identify unintended consequences and strive to quantify costs and benefits. Moreover, the CFTC should engage in periodic retrospective analysis to monitor the cost-effectiveness of the rule. Because the substantive economic issues highlighted in our review are all amenable to in-depth economic research, we reaffirm our recommendation that the Office of the Chief Economist ("OCE") encourage long-term academic research, by its own staff and by outside economists, to increase understanding of CFTC-regulated markets.

2. The CFTC should focus resources on improving its data infrastructure, particularly with regard to uncleared swaps. With respect to rulemakings in particular, the CFTC should strive to identify, early in the rulemaking process, the data that will be needed to establish a baseline understanding of the market, to estimate the effects of potential policy choices, and to conduct retrospective analysis for policy effectiveness.

- Lean Labor Audit of Division of Clearing and Risk and Division of Market Oversight Functions

Lean labor focuses on the workforce and its interaction with other resources required for output. It seeks out inefficiencies such as overproduction, waiting, and unused employee potential to maximize the value of human capital assets. Our objective was to assess the effectiveness of balancing labor and workload for CFTC's Division of Market Oversight, which is charged with key financial oversight duties. DMO oversees the derivatives markets to ensure that prices accurately reflect the forces of supply and demand and are free of disruptive activity. DMO examines exchanges and data repositories to ensure compliance with applicable core principles. DMO evaluates new applications for designated contract markets (DCMs), swap execution facilities (SEFs), and swap data repositories (SDRs), and foreign boards of trade (FBOTs), and makes recommendations to the Commission to approve or deny applications. DMO also periodically examines existing designated DCMs, SEFs, and SDRs, to ensure compliance with applicable core principles, as well as CEA and Commission regulatory requirements.

DMO evaluates new DCM and SEF products to ensure they are not susceptible to manipulation as well as proposed DCM and SEF rules to ensure compliance with applicable provisions of the Commodity Exchange Act (CEA) and Commission regulations. DMO is also responsible for all aspects of swap data reporting, including ensuring compliance with reporting requirements by registered entities and swap counterparties. This project was ongoing at the close of the reporting period.

We examined five DMO operating units: Data and Reporting, Product Review, Market Review, Compliance, and Chief Counsel. We observed that each DMO unit specified a purpose directly linked to the Commodity Exchange Act (CEA) and CFTC mission statement.[2] We observed that DMO units conduct work as described by DMO management; however, we identified repetition in DMO processes where project management principles can be applied broadly. DMO has an opportunity to enhance basic project management competencies for managing work plans within budgets; tools, standard operating procedures (tasks); and timelines for project completion (schedule and

2 "The mission of the Commodity Futures Trading Commission (CFTC) is to foster open, transparent, competitive, and financially sound markets. By working to avoid systemic risk, the Commission aims to protect market users and their funds, consumers, and the public from fraud, manipulation, and abusive practices related to derivatives and other products that are subject to the Commodity Exchange Act (CEA)" (http://www.cftc.gov/About/MissionResponsibilities/index.htm, last visited May 14, 2018).

actual time). In addition, our analysis of unit staffing further noted opportunities for lowering costs. Most notable were opportunities to reevaluate staffing mix as it relates to unit purpose. Specifically, we noted the absence of journeyman career ladder staff, management analysts, paralegals, or other suitable professionals who we believe could complete tasks currently performed by higher paid attorneys.

We asked CFTC to consider six changes designed to increase efficiency:

1. Establish leadership commitment to develop a Lean culture;

2. Seek Lean/project management early adopters, support with training, and share their experience;

3. Standardize project management and metadata requirements. Deployed tools such as SharePoint and/or MicroStrategy that can be used more robustly to monitor work;

4. Define useful standard operating procedures for work units;

5. Require the use of payroll project codes to capture actual work time for outputs, and review the results in order to establish performance expectations;

6. Reevaluate and restructure unit workforce staffing through attrition and/or retirement options to lower costs

- Inspection and Evaluation of Certain Stress Testing Processes at CFTC

In June 2017 we initiated an inspection of CFTC's stress-testing capabilities within the Division of Clearing and Risk (DCR). This inspection was motivated by concerns conveyed to us by DCR staff regarding mismanagement of efforts to develop a stress-testing program that incorporates both cleared and uncleared products across major asset classes. Due to personnel and operational sensitivities raised during our fieldwork, in October 2017 we distributed a summary memo to the Commission and met with the Commissioners. In December 2017 we offered a discussion draft to the Commission, and again met with the Chairman and Commissioners, as well as relevant agency management. We expect to complete this report, including a description of the agency's response, prior to the close of FY 2018.

- Customer Protection Outreach Whitepaper

This CFTC Office of Inspector General white paper, initiated during FY 2018, explores where CFTC could target education initiatives based on complaint and enforcement trends compared with current outreach efforts by CFTC's Office of Customer Education and Outreach. We examine the location and volume of complaints and allegations tracked by CFTC's Division of Enforcement (DOE) (hot spots for fraud and other violations); and existing Customer Education and Outreach travel, as well as historic SmartCheck website statistics. This project was ongoing at the close of the reporting period.

Office of Inspector General
Federal Deposit Insurance Corporation

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.

Background

The Federal Deposit Insurance Corporation (FDIC) was created by the Congress in 1933 as an independent agency to maintain stability and public confidence in the nation's banking system by insuring deposits and independently regulating state-chartered, non-member banks. According to most recent data, the FDIC insures more than $7 trillion in deposits at more than 5,700 banks and savings associations, and promotes the safety and soundness of these institutions by identifying, monitoring, and addressing risks to which they are exposed. The FDIC is the primary federal regulator for about 3,640 of the insured institutions. An equally important role for the FDIC is as Receiver for failed institutions—that is, upon closure of an institution by its chartering authority—the state for state-chartered institutions, and the Office of the Comptroller of the Currency for national banks and federal savings associations—the FDIC is responsible for resolving the institution and managing and disposing of its remaining assets.

The FDIC Office of Inspector General (OIG) is an independent and objective oversight unit established under the Inspector General (IG) Act of 1978, as amended. 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. We have continued to undertake work in support of that mission since issuance of the last CIGFO annual report.

With respect to failed bank work, our office conducts material loss reviews in cases where losses to the Deposit Insurance Fund (DIF) meet the threshold outlined in Section 38(k) of the Federal Deposit Insurance Act, as amended. We perform failed bank reviews of all failures of FDIC-supervised institutions under the mandatory loss threshold to determine whether unusual circumstances exist warranting an in-depth review of the failure. We issued two material loss reviews during the past year. Additionally, we issued the results of a review of the FDIC's Claims Administration System's Functionality and the FDIC's Processes for Responding to Breaches of Personally Identifiable Information.

Importantly, also in connection with matters affecting the broader financial sector, in February 2018, our Office published its assessment of the Top Management and Performance Challenges Facing the FDIC. This assessment was based on our extensive oversight work and research relating to reports by other oversight bodies, review of academic and other relevant literature, perspectives from Government agencies and officials, and information from private sector entities.

We have also sustained strong investigative efforts to combat financial institution fraud at or affecting both open and closed financial institutions. Our cases reflect the cooperative efforts of OIG investigators, FDIC divisions and offices, other OIGs, U.S. Attorneys' Offices, and others in the law enforcement community throughout the country. 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.

Finally, over the past year, we continued to coordinate with our financial IG counterparts on issues of mutual interest. As a member of CIGFO, the FDIC OIG is also participating in the joint project related to the Financial Stability Oversight Council's Monitoring of International Financial Regulatory Proposals and Developments.

Additional information on our work during the past year is presented below.

****

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

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

First NBC exhibited many of the characteristics of bank failures that we identified in prior material loss reviews and other reviews of the FDIC's supervision program: a dominant official with broad lending authority and limited Board of Directors oversight; rapid growth funded by high-cost deposits; and large lending relationships and concentrations without adequate risk management controls to mitigate the risks.

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

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

We made two recommendations in this report and management concurred.

Material Loss Review of the Failure of Seaway Bank and Trust Company

Our material loss review of the failure of Seaway Bank and Trust Company, Chicago, Illinois, examined an institution that failed on January 27, 2017, resulting in a $57.2 million loss to the DIF. The scope of our review included 2009 through Seaway's failure. Reviewing this period allowed us to evaluate Seaway's history before and after it acquired assets from two failed banks and changes that occurred to Seaway's Board of Directors and management.

We concluded that Seaway failed as a result of poor corporate governance and risk management practices. The Board and management were unable to effectively address a number of problems that began escalating, following the death of the bank's long-time Chairman in April 2013. Among other concerns, examiners uncovered accounting problems during the 2013 examination related to the assets Seaway acquired in 2010 and 2011 from the FDIC as Receiver.

The FDIC conducted examination activities, as required, and properly implemented applicable Prompt Corrective Action provisions. However, we concluded that it would have been prudent for the FDIC to have participated in a 2012 state examination of Seaway or conducted a separate visitation in 2012 to assess Seaway's accounting for the acquired failed bank assets. While it was permissible by FDIC Rules and Regulations to forego participation in the state examination, in our opinion, the FDIC missed an opportunity to see firsthand how the institution was managing and accounting for its acquisition of failed bank assets at a critical time.

Claims Administration System (CAS) Functionality

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

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

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

CAS improved timeliness of insurance determinations compared to the FDIC's predecessor system. The FDIC's goal is to provide depositors at failed institutions with access to their insured funds within 1 or 2 business days of failure. Although the FDIC had never failed to meet this timeliness standard, CAS may not be able to meet the FDIC's goal for the largest institutions due to the volume and complexity of large bank deposit platforms. In such cases, the FDIC may withhold a portion of the failed institution's deposits until an insurance determination can be made.

Regarding accuracy in making insurance determinations, CAS reduced the risk of inaccurate insurance determinations as compared to the FDIC's predecessor system by decreasing the opportunity for human error. The FDIC believes that CAS capabilities and procedures provide reasonable assurance of the accuracy of insurance determinations.

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

The FDIC's Processes for Responding to Breaches of Personally Identifiable Information (PII)

Implementing proper controls to safeguard personally identifiable information (PII) and respond to breaches when they occur is critical to maintaining stability and public confidence in the nation's financial system and protecting consumers from financial harm. We initiated an audit of the FDIC's processes for dealing with breaches of PII 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. Our review sample included 18 of 54 suspected or confirmed breaches involving PII that the FDIC discovered during the period January 1, 2015 through December 1, 2016. The breaches we reviewed potentially affected over 113,000 individuals.

The FDIC had established formal processes for evaluating the risk of harm to individuals potentially affected by a breach involving PII and providing notification and services to those individuals, when appropriate. However, the implementation of these processes was not adequate. Specifically:

> **FDIC Did Not Complete Key Breach Investigation Activities and Notify Affected Individuals Timely.** The FDIC did not complete key breach investigation activities (i.e., impact/risk assessments and/or convene the Data Breach Management Team or DBMT) within the timeframes established in the FDIC's Data Breach Handling Guide (DBHG) for 13 of 18 suspected or confirmed breaches that we reviewed. In addition, the FDIC did not notify potentially affected individuals in a timely manner for the incidents we reviewed. It

took an average of 288 days (more than 9 months) from the date the FDIC discovered the breaches to the date that the FDIC began to notify individuals.

FDIC Did Not Adequately Document Key Assessments and Decisions. Our review of 18 suspected or confirmed breaches found that Incident Risk Analysis (IRA) forms did not clearly explain the rationale behind the overall impact/risk levels assigned to the incidents. Some IRA forms were not substantially complete prior to convening the DBMT. The underlying analysis used to support assigned impact/risk levels for three breaches was inconsistent with the methodology in the DBHG. The overall risk ratings recorded in the IRA forms for five breaches were not consistent with the risk mitigation actions taken by the FDIC.

FDIC Needed to Strengthen Controls Over the DBMT. Although the DBHG described the role and activities of the DBMT, the FDIC had not established a formal charter or similar mechanism for the DBMT that defined its purpose, scope, governance structure, and key operating procedures. The FDIC had also not developed a process for briefing DBMT members on the outcome of their recommended actions to leverage lessons learned and promote consistency. The FDIC also did not provide DBMT members with specialized training to help ensure successful implementation of their responsibilities.

Not Track and Report Key Breach Response Metrics. The DBHG identified key categories of qualitative and quantitative metrics for benchmarking, tailoring, and continuously improving the FDIC's breach prevention and response capabilities. However, the FDIC generally did not track or report the metrics in the DBHG for the suspected or confirmed breaches we reviewed.

We made seven recommendations and the FDIC concurred with them.

Top Management and Performance Challenges

Under the Reports Consolidation Act of 2000, the OIG identifies the management and performance challenges facing the FDIC and provides its assessment to the Corporation for inclusion in the FDIC's annual performance and accountability report. This year we identified seven areas representing the most significant challenges for the FDIC, a number of which have implications to the broader financial sector and ways to improve financial oversight:

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

The identification of these challenges helps the FDIC and other policymakers identify the primary risks at the agency, and provides guidance for our Office to focus its attention and work efforts, as shown in the following summaries of each of these challenges.

Emerging Cybersecurity Risks at Insured Financial Institutions

Cybersecurity is a significant concern for the banking industry because of the industry's use of and reliance on technology – not only in bank operations, but also as an interface with customers. It has become one of the most

critical challenges facing the financial services sector due to the frequency and increasing sophistication of cyber-attacks. The FDIC has a significant financial interest in mitigating cybersecurity risks at insured banks. If a bank fails, the FDIC will need to step in and may have to fund the losses from the DIF.

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

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

Management of Information Security and Privacy Programs

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

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

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

We will continue to perform the annual review of the FDIC's information security program and practices pursuant to the Federal Information Security Modernization Act. We also have work planned in specific areas of the FDIC's information security program.

Utilizing Threat Information to Mitigate Risk in the Banking Sector

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

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

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

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

Readiness for Banking Crises

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

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

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

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

Enterprise Risk Management Practices

Enterprise Risk Management (ERM) is a decision-making tool that assists federal leaders in anticipating and managing risks at an agency, and helps to consider and compare multiple risks and how they present challenges and opportunities when viewed across the organization. According to OMB guidance, ERM is beneficial because

it addresses a fundamental organizational issue: the need for information about major risks to flow both vertically (i.e., up and down the organization) and horizontally (i.e., across its organizational units) to improve the quality of decision-making. When implemented effectively, ERM seeks to open channels of communication, so that managers have access to the information they need to make sound decisions. ERM can also help executives recognize how risks interact (i.e., how one risk can exacerbate or offset another risk). Further, ERM examines the interaction of risk treatments (actions taken to address a risk), such as acceptance or avoidance. We intend to conduct an evaluation of the effectiveness of the FDIC ERM Program.

Acquisition Management and Oversight

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

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

In our work, we have noted several shortcomings in contractor oversight, which can lead to delays and cost overruns. In our report entitled ***The FDIC's Failed Bank Data Services Project*** (March 2017), we reviewed a 10-year, $295 million project related to the transition of the management of failed financial institution data from one contractor to another. Our review focused on transition costs of approximately $24.4 million. The audit concluded that transition milestones were not met, resulting in a one year delay. Further, transition costs, while less than projected in the approval, were greater than the initial estimates at contract inception, by $14.5 million. We concluded that the reasons for the increase were that the FDIC faced challenges related to defining contract requirements, coordinating contracting and program office personnel, and establishing implementation milestones.

We are conducting an evaluation to review the FDIC's current contract oversight management program.

Measuring Costs and Benefits of FDIC Regulations

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

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

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

FDIC OIG Investigations Seek to Ensure Integrity in the Financial Services Sector

OIG investigations over the past months continued to complement our audit and evaluation work. Our investigative results over the 12 months ending March 31, 2018 included the following: 96 indictments; 35 arrests; 92 convictions; and potential monetary recoveries (fines, restitution, and asset forfeitures) of nearly $378 million.

Our office is committed to partnerships with other OIGs, the Department of Justice (DOJ), the Federal Bureau of Investigation, and other state and local law enforcement agencies in pursuing criminal acts in open and closed banks and helping to deter fraud, waste, and abuse. The OIG also actively participates in many financial fraud working groups nationwide to keep current with new threats and fraudulent schemes that can undermine the integrity of the FDIC's operations and the financial services industry as a whole.

Our current cases involve fraud and other misconduct on the part of senior bank officials, and include commercial loan and mortgage fraud exposed by turmoil in the housing, commercial real estate, and lending industries. The perpetrators of such crimes can be those very individuals entrusted with governance responsibilities at the institutions—directors and bank officers. In other cases, parties providing professional services to the banks and customers, others working inside the bank, and customers themselves are principals in fraudulent schemes.

The FDIC OIG's Office of Investigations also continues to identify emerging financial fraud schemes that affect FDIC-supervised and insured institutions. Our relationships with DOJ's Money Laundering and Asset Recovery Section, and DOJ's Fraud Section and Anti-Trust Division have allowed us to play a lead role in money laundering and foreign currency exchange rate manipulation investigations. We also work with other agencies, including the Small Business Administration, Department of Housing and Urban Development, and the Department of Agriculture, to identify fraud in the guaranteed loan portfolios of FDIC-supervised institutions. These investigations are important, as large-scale fraud schemes can significantly affect the financial industry and the financial condition of the institutions the FDIC supervises and insures.

Several case examples from the past year follow:

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

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

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

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

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

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

Banamex USA Enters into a Non-Prosecution Agreement and Agrees to Forfeit $97.44 Million

Banamex USA (BUSA) agreed to forfeit $97.44 million and entered into a non-prosecution agreement (NPA) to resolve an investigation into BUSA's Bank Secrecy Act (BSA) violations.

In its agreement with DOJ, BUSA admitted to criminal violations by willfully failing to maintain an effective anti-money laundering compliance program with appropriate policies, procedures, and controls to guard against money laundering and willfully failing to file Suspicious Activity Reports (SARs). According to admissions contained in the agreement and the accompanying statement of facts, from at least 2007 until at least 2012, BUSA processed more than 30 million remittance transactions to Mexico with a total value of more than $8.8 billion. During the same period, BUSA's monitoring system issued more than 18,000 alerts involving more than $142 million in potentially suspicious remittance transactions. BUSA, however, conducted fewer than 10 investigations and filed only 9 SARs in connection with these 18,000-plus alerts, filing no SARs on remittance transactions between 2010 and 2012. BUSA also admitted that, for several years, BUSA recognized that it should have improved its monitoring of money services business remittances but failed to do so.

BUSA employed a limited and manual transaction monitoring system, running only two scenarios to identify suspicious activity on the millions of remittance transactions it processed. These two scenarios produced paper reports that were intended to be reviewed by hand by the two employees assigned to perform the BSA functions of the bank, in addition to time-consuming non-BSA responsibilities. As BUSA began to expand its remittance processing business in 2006, BUSA understood the need to enhance its anti-money laundering efforts, yet failed to make necessary improvements to its transaction monitoring controls or to add staffing resources.

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

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

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

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

Additional information on the work of the FDIC OIG may be found at www.fdicoig.gov

Office of Inspector General
The Federal Housing Finance Agency

Created by the Housing and Economic Recovery Act of 2008 (HERA), the Federal Housing Finance Agency (FHFA or Agency) supervises and regulates (1) the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Mortgage Corporation (Freddie Mac) (the Enterprises), (2) the Federal Home Loan Banks (FHLBanks) (collectively, the regulated entities), and (3) the FHLBanks' fiscal agent, the Office of Finance. Since September 2008, FHFA has also served as conservator for the Enterprises. As of year-end 2017, the Enterprises, together, reported approximately $5.4 trillion in assets and more than $5.3 trillion in debt. The FHLBanks collectively reported roughly $1.1 trillion in assets.

Also created by HERA, the FHFA Office of Inspector General (OIG) conducts, supervises, and coordinates audits, evaluations, investigations, and other activities relating to the programs and operations of FHFA. OIG promotes economy, efficiency, and effectiveness and protects FHFA and the entities it supervises and regulates against fraud, waste, and abuse, thereby contributing to the liquidity and stability of the nation's housing finance system, and protecting the interests of the American taxpayers. We accomplish this mission by providing independent, relevant, timely, and transparent oversight of the Agency to promote accountability, integrity, economy, and efficiency; advising the Director of the Agency and Congress; informing the public; and engaging in robust enforcement efforts to protect the interests of American taxpayers.

Background

OIG focuses its resources on programs and operations that pose the greatest financial, governance, and/or reputational risk to the Agency, the Enterprises, and the FHLBanks to best leverage its resources to strengthen oversight. We use an integrated approach to identify these programs and operations of greatest risk and publish an annual risk-based ***Audit, Evaluation, and Compliance Plan*** that describes FHFA's and OIG's roles and missions, explains our risk-based methodology for developing this plan, provides insight into particular risks within four areas, and generally discusses areas where we will focus our audit, evaluation, and compliance resources during the coming year (see OIG, Audit, Evaluation, and Compliance Plan - March 2018). In addition to our risk-based work plan, OIG completes work required to fulfill its statutory mandates.

An integral part of OIG's oversight is to identify and assess FHFA's top management and performance challenges and to align our work with these challenges. In October 2017, we updated our assessment of FHFA's major management and performance challenges. We noted that these challenges all carried over from prior years and, if not addressed, could adversely affect FHFA's accomplishment of its mission. (See OIG, Fiscal Year 2018 Management and Performance Challenges). During this reporting period, OIG continued to focus much of its oversight activities on identifying vulnerabilities in these areas and recommending meaningful actions that the Agency could take to mitigate these risks and remediate identified deficiencies. These challenges include:

- **Conservatorship Operations – Improve Oversight of Matters Delegated to the Enterprises and Strengthen Internal Review Processes for Non-Delegated Matters.** Since September 2008, FHFA has administered two conservatorships of unprecedented scope and undetermined duration. When then-Secretary of the Treasury Henry Paulson announced the conservatorships of the Enterprises in September 2008, he explained that they were meant to be a "time out" during which the Enterprises would be stabilized, enabling the "new Congress and the next Administration [to] decide what role government in general, and these entities in particular, should play in the housing market." The current FHFA Director has echoed that view, recognizing that conservatorship "cannot [and] should not be a permanent state" for the Enterprises. However, putting the Enterprises into conservatorships has proven to be far easier than taking them out, and the "time out" period for the conservatorships is now in its 10th year.

  While in conservatorship, the Enterprises have required almost $191.5 billion in financial investment from the Department of the Treasury (Treasury) to avert their insolvency and, through March 2018, the Enterprises have paid to the Treasury more than $278.7 billion in dividends on its investment. Despite their high leverage, diminished capital, conservatorship status, and uncertain future, the Enterprises have grown in size since being placed into conservatorship in 2008 and, according to FHFA, their combined market share of newly issued mortgage-backed securities is more than 60%.

  Although market conditions have improved and the Enterprises have paid dividends on Treasury's investments, the Enterprises' future profitability cannot be assured for these reasons: the wind down of their retained investment portfolios and reduction in net interest income; reduction in the value of the Enterprises' deferred tax assets due to recent federal corporate tax reform (considered by FHFA to be a short-term consequence); the level of guarantee fees they will be able to charge and keep; the future performance of their business segments; and the significant uncertainties involving key market drivers, such as mortgage rates, homes prices, and credit standards.

  Under HERA, FHFA's actions as conservator are not subject to judicial review or intervention, nor are they subject to procedural safeguards that are ordinarily applicable to regulatory activities such as rulemaking. As conservator of the Enterprises, FHFA exercises control over trillions of dollars in assets and billions of dollars in revenue and makes business and policy decisions that influence and affect the entire mortgage finance industry.

- **Supervision of the Regulated Entities – Upgrade Supervision of the Enterprises and Continue Robust Supervision of the FHLBanks.** As discussed earlier, FHFA plays a unique role as both conservator and supervisor for the Enterprises and as supervisor for the FHLBank System. FHFA has repeatedly stated that effective supervision of the FHLBanks and the Enterprises is critical to ensuring their safety and soundness. The Federal Home Loan Bank Act requires each FHLBank to be examined at least annually, and the Federal Housing Enterprises Financial Safety and Soundness Act of 1992, as amended, requires FHFA to conduct annual on-site examinations of each Enterprise. FHFA's annual examination program assesses the financial safety and soundness and overall risk management practices of each Enterprise through ongoing monitoring, targeted examinations, and risk assessments.

- **Information Technology Security – Enhance Oversight of Cybersecurity at the Regulated Entities and Ensure an Effective Information Security Program at FHFA.** Security of information technology (IT) and IT systems continues to be a preeminent issue for businesses and individuals alike. The regulated entities, like most modern institutions, rely on complex IT systems to conduct almost every aspect of their work. These IT systems manage processes to guarantee and purchase loans, supporting more than $5 trillion in Fannie Mae and Freddie Mac mortgage assets, and store, process, and transmit financial data and personally identifiable information (PII). Both Enterprises and the FHLBanks have been the subject of cyberattacks, though none caused significant harm. All entities regulated by FHFA acknowledge that the substantial precautions put into place to protect their IT systems might be vulnerable, and penetration of those systems poses a material risk to their business operations. Further, the Enterprises are increasingly relying on third-party service providers, which requires the sharing of sensitive information between Enterprise and third-party systems.

- **Counterparties and Third Parties– Enhance Oversight of the Enterprises' Relationships with Counterparties and Third Parties.** The Enterprises rely heavily on counterparties and third parties for a wide array of professional services, including mortgage origination and servicing. That reliance exposes the Enterprises to counterparty risk—the risk that the counterparty will not meet its contractual obligations. FHFA has delegated to the Enterprises the management of their relationships with counterparties, and FHFA reviews that management largely through its supervisory activities. As participants in the mortgage market change, counterparties can affect the risks to be managed by Fannie Mae and Freddie Mac. In recent years, the Enterprises' businesses have changed dramatically in terms of the types of institutions originating and selling mortgages to them and servicing mortgages on their behalf.

Examples of OIG's Oversight Accomplishments: Audit, Evaluation, and Compliance Activities

Conservatorship Operations

Corporate Governance: Review and Resolution of Conflicts of Interest Involving Fannie Mae's Senior Executive Officers Highlight the Need for Closer Attention to Governance Issues by FHFA (EVL-2018-001; January 31, 2018)

FHFA, as conservator, has delegated to each Enterprise responsibility for a significant portion of day-to-day management and risk management controls. For this governance approach to succeed, FHFA must be confident that the Enterprises' directors and committees are properly exercising the powers they have been given and fulfilling their responsibilities. In an earlier completed administrative investigation, we reviewed the policies, procedures, and codes that make up Fannie Mae's process for conflicts of interest involving senior executive officers (SEOs). In this evaluation, OIG assessed FHFA's oversight of this conflicts process.

We first sought to understand whether Fannie Mae's governance documents reserved to either the Board of Directors (Board) or the Nominating and Corporate Governance Committee (NGC or Committee) the authority to resolve conflicts of interest issues involving SEOs. The NGC Charter charges the NGC with reviewing activities of Designated Executive Officers—also called SEOs—that "may result in a potential or actual conflict of interest" under the Conflict of Interest Policy (COI Policy) or Conflict of Interest Procedure (COI Procedure). The Charter also states that the NGC is responsible for interpreting the COI Policy and COI Procedure where the interpretation relates to the Fannie Mae Chief Executive Officer (CEO), who is also an SEO.

Fannie Mae's COI Policy and COI Procedure—drafted by the office responsible for assisting the NGC in fulfilling its duties, Fannie Mae's Office of Compliance and Ethics (FM Ethics)—state that the NGC is responsible for "approving" conflict of interest requests from SEOs. The COI Procedure sets forth a clear, unambiguous procedure that must be used by FM Ethics to escalate all conflicts requests involving SEOs to the NGC for resolution by the NGC.

To understand the practice followed by the NGC to resolve SEO potential conflicts of interest, we interviewed the NGC Chair (an NGC member since December 2008 and chair since October 2015) and he provided two conflicting explanations of the NGC's practice. We sought to determine what practice, if any, had been consistently followed by the NGC over a five-year period between January 2012 and December 2016 with respect to SEOs. We identified 57 potential conflicts involving SEOs. Of these 57 potential conflicts involving SEOs, we found:

- For 24 of the 57 potential conflicts (42%), FM Ethics presented the potential conflict and its recommended determination to the NGC for its determination.

- For 16 of the 57 (28%), FM Ethics determined, on its own, whether a conflict involving an SEO existed, and, where it found a conflict, took steps to address it and subsequently notified the NGC of its determination. We found no evidence that any NGC member: asked FM Ethics to explain why it presented some SEO potential conflicts to the NGC for its resolution, but retained and resolved other potential SEO conflicts and subsequently notified the NGC of its determination; pressed FM Ethics to explain the basis of its authority to resolve conflicts determinations for SEOs; provided direction to FM Ethics about its role in resolving SEO

conflicts; or raised the potential inconsistencies between its duties under the Charter and its duties under the COI Procedure with the Board and asked the Board to clarify its responsibilities.

- For 17 of the 57 (30%), FM Ethics determined, on its own, whether a potential conflict of interest involving an SEO existed and took steps to resolve any conflict that it identified. We found no evidence that FM Ethics ever notified the NGC of any of these 17 conflicts disclosures or determinations, which deprived the NGC of its ability to satisfy its duties under its Charter.

We also looked at FHFA's oversight of the NGC's review of conflicts of interest involving SEOs. While we found that FHFA employees attended NGC meetings at which FM Ethics presented conflicts questions involving SEOs to the NGC for its determinations and notified the NGC of its decisions regarding SEO conflicts requests, we found no evidence that FHFA employees identified the lack of consistent approach and process in the resolution of these conflicts or escalated those issues to senior FHFA management. We also found no evidence that FHFA's senior management was aware of these issues until we brought them to FHFA's attention.

Based on our review, we found failures, both by Fannie Mae's NGC and by FHFA, which created a weakness in Fannie Mae's risk management structure. Without enhancements to the NGC's oversight, there is a significant risk that the NGC will continue to fall short in exercising its governance responsibilities. FHFA agreed with our eight recommendations to address these shortcomings.

Audit of FHFA's Oversight of Fannie Mae's Compliance with the Required Risk Mitigants of Automated Underwriting, Mortgage Insurance, and Homeownership Education for its Purchases of Mortgages with a 97% LTV (AUD-2018-003; issued March 8, 2018) ***and Audit of FHFA's Oversight of Freddie Mac's Compliance with the Required Risk Mitigants of Automated Underwriting, Mortgage Insurance, and Homeownership Education for its Purchases of Mortgages with a 97% LTV*** (AUD-2018-004; March 8, 2018))

For more than 20 years, successive administrations agreed that a barrier to homeownership for low- and moderate-income people was a significant down payment, and they promoted solutions to reduce that barrier to increase accessibility to homeownership. Numerous studies have found that saving enough cash for a down payment and other up-front closing costs is the greatest barrier that low-income and minority families face when considering homeownership.

As conservator, FHFA issued an expectation to the Enterprises in May 2014 to "Work to increase access to mortgage credit for creditworthy borrowers, consistent with the full extent of applicable credit requirements and risk-management practices." Later that year, in October 2014, the FHFA Director announced that FHFA was working with the Enterprises to develop sensible and responsible guidelines for mortgages with loan-to-value (LTV) ratios between 95% and 97% (high LTV mortgages) to increase access for creditworthy but lower-wealth borrowers.

After reviewing proposals received from Fannie Mae and Freddie Mac, FHFA staff prepared a memorandum in early December 2014 recommending that the FHFA Director approve the high LTV mortgage programs proposed by the Enterprises. The memorandum acknowledged that "historical performance demonstrates that higher LTV loans can have higher risks than lower LTV loans and can have higher loss severities," but asserted that these higher risks can be safely offset by thoughtful compensating factors and risk mitigants, including automated underwriting, private mortgage insurance, and pre-purchase homeownership education. The Staff Memorandum identified an additional control: FHFA's ongoing oversight of Enterprise purchases of high LTV mortgages. The FHFA Director accepted the staff recommendation and approved the programs.

OIG completed two audits, one of Fannie Mae and one of Freddie Mac, to assess FHFA's oversight of each Enterprise's implementation of their 97% LTV mortgage program. As part of assessing FHFA's oversight, we obtained (through FHFA) and analyzed each Enterprise's data on 97% LTV mortgages purchased by the Enterprise and whether those mortgages conformed to three FHFA-required credit terms: (1) automated underwriting, (2) mortgage insurance, and (3) homeownership education.

Our analysis of data provided by the Enterprises, through FHFA, found a high rate of compliance for the mortgages purchased by the Enterprises under their 97% LTV mortgage programs.

Based on our inquiries to FHFA and Fannie Mae, and our analysis of the data provided by the Enterprise, we found that Fannie Mae purchased 74,700 mortgages from December 2014 to December 2016, under the approved 97% LTV mortgage program. Of those mortgages purchased, all were underwritten using an automated underwriting system and all but two loans utilized mortgage insurance or another credit enhancement. Regarding homeownership education, which was required for only about a fourth of the 97% LTV mortgage purchases, we found that Fannie Mae relied on the lenders' representations and warranties to determine whether this requirement was met. Fannie Mae quality control reviews of purchased loans found exceptions with homeownership education in 3% of loans sampled where homeownership education was a requirement. Fannie Mae advised us that it implemented a "fatal" rule in its Loan Delivery system, requiring lenders to confirm that pre-purchase homeownership education has been completed, when required, or the mortgage will be rejected.

Based on our inquiries to FHFA and Freddie Mac, and our analysis of the data provided by the Enterprise, we found that Freddie Mac purchased 19,628 mortgages from December 2014 to December 2016, under the approved 97% LTV mortgage program. Of those mortgages purchased, all were underwritten using an approved method of underwriting and contained information from the lender about required mortgage insurance or another credit enhancement. Regarding homeownership education, we found a compliance rate of 98%. Freddie Mac advised us that the Enterprise is developing and implementing additional business rules to: (1) improve the accuracy of lenders' recording of homeownership education information in its Selling System and (2) enforce the homeownership education requirement.

We found that FHFA's oversight and supervision of the Enterprises' 97% LTV mortgage programs, which focused on the Enterprises' credit risk management, did not directly address compliance with the three risk mitigants that were the scope of our audits. While we made no recommendations in our audit reports, we advised FHFA that in view of the increasing volume of 97% LTV mortgages purchased by the Enterprises, it would be prudent for FHFA to conduct supervisory activities over their 97% LTV mortgage programs, consistent with the recognition by FHFA that such activities are "an important oversight control."

Supervision of the Regulated Entities

FHFA Requires the Enterprises' Internal Audit Functions to Validate Remediation of Serious Deficiencies but Provides No Guidance and Imposes No Preconditions on Examiners' Use of that Validation Work (EVL-2018-002; issued March 28, 2018)

When FHFA conducts supervisory activities, it may identify significant deficiencies related to risk management, risk exposure, or violations of laws, regulations, or orders affecting the performance or condition of a regulated entity. Among these "adverse examination findings" are matters requiring attention (MRAs), which consist of either "critical supervisory matters (the highest priority) that pose substantial risk to the safety and soundness of the regulated entity" or "deficiencies," which if not corrected, could "escalate and potentially negatively affect" the regulated entity.

FHFA expects the Enterprises to take corrective action to remediate MRAs. When Enterprise management determines that it has completed remediation of an MRA, FHFA expects the Enterprise's internal audit (IA) functions to review the corrective action and "validate" that remediation has been fully implemented as intended. The Enterprise then submits a closure package to FHFA that contains documentation of IA's validation work. Based on a review of the closure package, and any other follow-up examination work that FHFA may conduct, FHFA determines whether the MRA has been satisfactorily addressed and notifies the Enterprise of its determination.

In a 2016 evaluation, OIG found that some FHFA examiners appeared to have accepted MRA validation work conducted by the Enterprises' IA functions without evidence of independent analysis. During this reporting period, we completed two follow-up evaluations. In one report, we reviewed internal guidance and standards for reliance

on the Enterprises' IA functions when examiners assess the remediation of MRAs. We compared FHFA guidance to guidance issued by the Office of the Comptroller of the Currency (OCC) and the Board of Governors of the Federal Reserve System (Federal Reserve), and interviewed FHFA officials and staff. OCC and Federal Reserve guidance direct their respective examiners to periodically assess and conclude on the overall effectiveness or strength of the IA functions at their regulated financial institutions. Federal Reserve guidance permits reliance on IA MRA follow-up only when the Federal Reserve has rated the institution's IA function as effective overall. We found, however, that FHFA has not concluded on the overall effectiveness of the Enterprises' IA functions and has no present plans to do so. As a result, we concluded that FHFA examiners lack assurance of the overall quality, reliability, competency, and objectivity of the Enterprises' IA function when they use IA validation work.

In addition, we found that FHFA guidance does not address whether, or the circumstances under which, FHFA examiners may rely on, accept, or otherwise use information, analyses, or conclusions provided by an Enterprise's IA function when determining whether an Enterprise has satisfactorily remediated an MRA. Accordingly, examiners are given wide discretion to determine whether and to what extent to rely on, accept, or otherwise use IA validation work as a basis to close MRAs. In our view, such discretion to use IA validation work to close MRAs, without a predicate supervisory conclusion on the overall effectiveness of the IA function, creates the risk that FHFA's assessment of the adequacy of Enterprise remediation will be impaired.

We made three recommendations to FHFA to address these shortcomings. FHFA agreed with one recommendation and disagreed with two. FHFA agreed to issue more detailed examiner guidance regarding the use of IA work in assessment of Enterprise remediation of MRAs. FHFA did not agree to conclude periodically on the overall effectiveness of the Enterprises' IA functions and did not agree to direct that examiners can use IA work to assess MRA remediation only if FHFA has concluded that the IA function is effective overall.

The Gap in FHFA's Quality Control Review Program Increases the Risk of Inaccurate Conclusions in its Reports of Examination of Fannie Mae and Freddie Mac (EVL-2017-006; issued August 17, 2017)

Each year, FHFA supervises the Enterprises through targeted examinations and ongoing monitoring activities. At the conclusion of each annual supervisory cycle, FHFA prepares and transmits a report of examination (ROE) to the board of directors for each Enterprise. The annual ROE constitutes FHFA's "primary work product that communicates . . . the cumulative results of [FHFA's] supervisory activities conducted during the annual examination cycle." Each ROE also contains numerical ratings that FHFA assigns for seven component areas, a rating system known as CAMELSO. In addition, FHFA assigns a composite rating for each Enterprise's overall safety, soundness, and risk management practices.

In this evaluation, we reviewed FHFA's processes for assigning CAMELSO ratings to the Enterprises and documenting the bases for those ratings. We found that FHFA examination managers prepare a draft ROE narrative that contains a proposed rating for each CAMELSO component within their purview. The examination managers then submit their draft narratives to the examiner-in-charge (EIC), who edits the narratives and compiles them into a draft ROE for the cognizant Deputy Director's approval.

During our fieldwork, we learned that the independent quality control review program, which was intended to confirm that examination findings and conclusions are adequately supported before communicated to the Enterprises, did not meet the requirements established by FHFA in a 2013 supervision directive. Instead of performing a quality control review of the ROEs or the CAMELSO ratings before either was transmitted to an Enterprise, as required by the 2013 directive, quality control reviews were performed of certain examination findings and conclusions.

According to an FHFA official, these quality control reviews made it unnecessary to perform quality control reviews of the ROEs and the CAMELSO ratings because the information on which they were based had already been subjected to quality control review. We found, however, that quality control reviews were not performed for ongoing monitoring activities that did not result in findings communicated to the Enterprises in writing. We determined that the ROEs issued to the Enterprises for the 2015 supervisory cycle contained conclusions derived from ongoing monitoring activities that had not been subject to a quality control review, which increased the risk that an ROE may inaccurately report that an Enterprise is meeting supervisory expectations or making progress in addressing weaknesses.

FHFA agreed with our recommendation to enhance its quality control review program to reach all conclusions from ongoing monitoring activities and represented that it would amend its quality control review guidance.

Information Technology Security

FHFA Failed to Complete Non-MRA Supervisory Activities Related to Cybersecurity Risks at Fannie Mae Planned for the 2016 Examination Cycle (AUD-2017-010; issued September 27, 2017) and ***FHFA Did Not Complete All Planned Supervisory Activities Related to Cybersecurity Risks at Freddie Mac for the 2016 Examination Cycle*** (AUD-2017-011; issued September 27, 2017)

The Enterprises store, process, and transmit significant amounts of financial data and PII in connection with their mission to support the secondary mortgage market. FHFA recognizes that cybersecurity is a significant risk for both Enterprises in light of the frequency and sophistication of attacks on information technology systems of financial institutions. In its 2015 Performance and Accountability Report (PAR), the Agency represented that: "A key objective of FHFA's supervisory work will continue to be the effective oversight of how each Enterprise manages cyber risks and addresses vulnerabilities."

OIG completed separate audits addressing aspects of FHFA's supervision of cybersecurity risks for Fannie Mae and Freddie Mac during the 2016 examination cycle. The audits had two objectives. First, we sought to determine whether the supervisory activities planned by FHFA relating to each Enterprise's cybersecurity risks for the 2016 examination cycle addressed the cybersecurity risks highlighted in its risk assessments and supervisory strategies for the Enterprises, applying the standard adopted by FHFA. Second, we sought to determine whether cybersecurity-related planned supervisory activities for the 2016 examination cycle were completed during that cycle in light of FHFA's representations in its 2015 PAR that "a key objective of FHFA's supervisory work" during 2016 would be oversight of how the Enterprises managed their cyber risk and addressed vulnerabilities.

For Fannie Mae, we found that FHFA did not establish a link in its supervisory planning documents to the risks it identified in its Operational Risk Assessment for the 2016 examination cycle. We were not able to confirm whether all the risks identified in that Operational Risk Assessment could be tracked to planned cybersecurity supervisory activities. We also could not determine whether the planned supervisory activities addressed the risks FHFA considered the most critical for the Enterprise because FHFA did not identify which risks were the most critical in either the Operational Risk Assessment or the Supervisory Strategy.

We found that FHFA did not complete any of its supervisory activities relating to Fannie Mae's current cybersecurity risks planned for the 2016 examination cycle during that cycle. As revised at mid-year, those planned activities included one targeted examination and three ongoing monitoring activities. We determined that FHFA did complete its ongoing monitoring of Fannie Mae's remediation of three cybersecurity-related MRAs issued in prior years. We could not reconcile FHFA's representations that cybersecurity supervisory activities would be a key objective of FHFA's supervisory work during the 2016 supervisory cycle with the Agency's inability to complete any of the four planned supervisory activities relating to Fannie Mae's cybersecurity risks during the 2016 examination cycle.

As part of this audit, we reviewed an August 2016 memorandum by FHFA staff to explain the reasons for the mid-year revisions to the 2016 supervisory plan which reported: "a number of staffing and structural changes in 2016... directly impacted execution of the 2016 examination plan." That memorandum stated that all ongoing monitoring activities and targeted examinations for 2016 were "descoped due to the limited time available due to the focus on MRA closure."

A reasonable inference from this memorandum is that FHFA staff held the view that FHFA lacked a sufficient complement of examiners to adequately perform its supervisory responsibilities for the Enterprises. We raised the same concern in an audit issued in September 2016, in which we found that FHFA failed to conduct and complete more than half of its planned targeted examinations of Fannie Mae for the 2012 to 2015 examination cycles and completed no targeted examinations planned for the 2015 examination cycle before the 2015 ROE issued. We reported that the reason repeatedly provided by FHFA examiners and the then-current EIC for this failure was

resource constraints, notwithstanding the consistent position of FHFA senior leadership that the Agency had an adequate complement of examiners to meet its supervisory responsibilities for the Enterprises. Our findings in this 2017 audit—that FHFA completed none of its planned supervisory activities for the 2016 examination cycle relating to Fannie Mae's management of its cybersecurity risks—caused us to renew the caution we issued previously:

> For a federal financial regulator, responsible for supervising two Enterprises that together own or guarantee more than $5 trillion in mortgage assets and operate in conservatorship, to fail to complete a substantial number of planned targeted examinations, including failure to complete any of its 2015 planned targeted examinations for Fannie Mae within the 2015 supervisory cycle, is an unsound supervisory practice and strategy.

We also found that FHFA's failure to complete any of its planned supervisory activities during 2016 relating to Fannie Mae's management of cybersecurity risk (other than closing MRAs issued in prior years) meant that it had no findings to report in the section of the 2016 ROE entitled "Information Security and Cyber-Security." Lacking supervisory information relating to the management of information security risks to report in the ROE, FHFA summarized the conclusions reached by Fannie Mae's IA function and by a contractor retained by Fannie Mae to perform a cyber risk assessment. We warned that there is a significant risk that FHFA's inability to complete any of its planned supervisory activities relating to Fannie Mae's management of its cybersecurity risks and reliance on conclusions reached by Fannie Mae's IA and its contractor deprived Fannie Mae's Board of Directors with information necessary to execute the cyber risk management responsibilities delegated to it by FHFA.

For Freddie Mac, we also found that FHFA did not establish a link between the objectives of the planned supervisory activities and the cybersecurity risks. However, we were able to link the cybersecurity risks identified in the Operational Risk Assessment to the objectives for three of the five non-MRA planned cybersecurity supervisory activities for this cycle. However, we were not able to link the stated objectives for two of the five planned supervisory activities to cybersecurity risks identified in the Operational Risk Assessment for Freddie Mac. For the 2016 examination cycle, FHFA planned two targeted examinations at Freddie Mac, three ongoing monitoring activities relating to cybersecurity risks at Freddie Mac, and one other ongoing monitoring activity regarding Freddie Mac's effort to remediate an MRA issued by FHFA in a prior year. We found that FHFA did not complete one of its planned targeted examinations until after the 2016 ROE issued on March 10, 2017, and deferred the other. We also found that FHFA completed the three planned ongoing monitoring activities relating to cybersecurity risks at Freddie Mac as well as the planned MRA remediation ongoing monitoring activity.

In response to our specific recommendations to address the shortcomings identified in our audits, FHFA agreed that cybersecurity is a significant area for risk management by the Enterprises and is a critical component of FHFA's supervision of the Enterprises. FHFA represented that it was working to improve its supervision protocols and processes to more effectively identify cybersecurity risks and address them in FHFA's examination activities and identified a number of planned corrective actions.

Counterparties and Third Parties

FHFA Should Improve its Administration of the Suspended Counterparty Program (COM-2017-005; issued July 31, 2017)

The Enterprises and the FHLBanks have adopted counterparty risk management programs designed to protect them from excessive financial loss caused by deterioration in a counterparty's financial condition. FHFA adopted the Suspended Counterparty Program in June 2012 to augment the regulated entities' programs and provide them with additional protection from the financial and reputational risks posed by individuals and businesses with a history of engaging in fraudulent conduct.

FHFA promulgated interim and final rules requiring each regulated entity to refer to FHFA a current or former counterparty or an affiliate that has been convicted of, or sanctioned administratively for, engaging in mortgage-related fraud or other financial misconduct within the last three years (covered misconduct). The interim and final rules also limit FHFA's authority to suspend a current and former counterparty or an affiliate to a three-year period after a conviction or administrative sanction was imposed for covered misconduct.

OIG assessed the FHFA Office of General Counsel's (OGC) administration of the Suspended Counterparty Program to determine whether the program is achieving its stated objective. We found deficiencies in OGC's administration of the program, the remediation of which could enable the program to effectively limit the regulated entities' exposure to the risks inherent in doing business with counterparties found to have engaged in covered misconduct. As of December 31, 2016, OGC had a backlog of 424 referrals from other agencies, the majority of which had been pending for a year or more. OGC's failure to resolve referrals on a timely basis is consequential: we identified five instances in which OGC did not resolve referrals within a three-year period after a finding of covered misconduct, which precluded the suspending official from determining whether the counterparty should be suspended under the Suspended Counterparty Program. Further, we found the length of three suspensions fell short of the periods called for in the Agency's internal guidelines and that the Agency did not document the mitigating factors that support the shorter suspensions, in contravention of FHFA's Records Management Policy.

We recommended that FHFA establish a plan to reduce the Suspended Counterparty Program backlog and document its reasons for any departures from the suspension periods prescribed in its guidelines. FHFA agreed with our recommendations.

FHFA Should Address the Potential Disparity Between the Statutory Requirement for Fraud Reporting and its Implementing Regulation and Advisory Bulletin (COM-2018-002; issued March 23, 2018)

Fannie Mae and Freddie Mac face the risk of fraud from various actors in the mortgage market, including originators, counterparties, and insiders. Fraud may subject the Enterprises to significant financial, operational, legal, or reputational harm. For this reason, the Enterprises are subject to fraud reporting requirements prescribed by statute, regulation, and guidance issued by FHFA.

OIG assessed FHFA's oversight of the Enterprises' reporting of actual or potential fraud. We found a potential disparity between the fraud reporting requirement in the statute and that in the Agency's regulation and guidance. By statute, an Enterprise must "timely report" to the Agency each occurrence involving the purchase or sale of a loan or financial instrument when the Enterprise discovers fraud or "suspects a possible fraud." The statute also insulates a regulated entity from all liability in connection with making a "good faith" report. FHFA's implementing regulation defines "possible fraud" to require an Enterprise to conduct and complete an inquiry and develop a "reasonable belief" of its existence. The inquiry built into FHFA's definition of "possible fraud" appears to contemplate a higher reporting threshold than the statutory direction to "timely report" a suspicion of possible fraud.

We are mindful of the deference to be given an agency's construction of a statute that the agency administers where the statute is ambiguous and the agency's position is reasonable. Given that the fraud reporting requirement is contained in a statute intended to restore confidence in the Enterprises and strengthen regulatory oversight, we questioned whether an interpretation that appears to weaken the statutory requirement to timely report suspected possible fraud is reasonable.

FHFA's implementing regulation requires an Enterprise to report "immediately" fraud and suspicion of possible fraud with significant impact. FHFA's definition of "possible fraud" caused the Enterprises to conduct inquiries, which may have delayed reporting of possible fraud with potential significant impact. One Enterprise notified the Agency after conducting a six-week inquiry and was unable to state when, during its inquiry, it determined that the fraud allegations warranted "immediate" reporting. We were not able to determine, from the record, whether the Enterprise's "immediate notification" was timely (i.e., within one reporting day).

Examples of OIG Investigative Accomplishments

OIG is vested with statutory law enforcement authority that is exercised by the Office of Investigations (OI). Depending on the type of misconduct uncovered, OI investigations may result in criminal charges, civil complaints, and/or administrative sanctions and decisions. Civil claims can lead to settlements or verdicts with restitutions, fines, penalties, forfeitures, assessments, and exclusion of individuals or entities from participation in federal programs. Criminal charges filed against individuals or entities may result in plea agreements or trials, incarceration, restitution,

fines, and penalties. OI is staffed with special agents (SAs), investigative counsels (ICs), analysts, and attorney advisors. To increase FHFA-OIG's effectiveness, four of OIG's attorney-investigators have been appointed as Special Assistant U.S. Attorneys (SAUSAs) in several judicial districts throughout the country. They have been assigned criminal matters arising from OI's investigations in the districts where they have been appointed and have pursued these investigations to conviction and sentencing.

Civil Cases

OI continued to actively participate in residential mortgage-backed securities (RMBS) investigations by working closely with U.S. Attorneys' offices to investigate allegations of fraud committed by financial institutions and individuals in connection with RMBS. OI SAs and attorneys reviewed evidence produced by various parties, conducted witness interviews, provided strategic litigation advice, and briefed other law enforcement agencies on the operations of the RMBS market.

In March 2018, the Department of Justice (DOJ) reached agreement with Barclays Capital, Inc. (Barclays) to settle a civil action filed in December 2016 in which the United States sought civil penalties for alleged conduct related to Barclays' underwriting and issuance of RMBS between 2005 and 2007. Barclays will pay the United States $2 billion in civil penalties in exchange for dismissal of the Amended Complaint. Agreement has also been reached with the two former Barclays executives who were named as defendants in the suit: Paul Menefee, who served as Barclays' head banker on its subprime RMBS securitizations, and John Carroll, who served as Barclays' head trader for subprime loan acquisitions. In exchange for dismissal of the claims against them, Menefee and Carroll agreed to pay the United States the combined sum of $2 million in civil penalties.

The scheme alleged in the complaint involved 36 RMBS deals in which over $31 billion worth of subprime and Alt-A mortgage loans were securitized, more than half of which defaulted. The complaint alleged that in publicly filed offering documents and in direct communications with investors and rating agencies, Barclays systematically and intentionally misrepresented key characteristics of the loans it included in these RMBS deals. In general, the borrowers whose loans backed these deals were significantly less creditworthy than Barclays represented, and these loans defaulted at exceptionally high rates early in the life of the deals. In addition, as alleged in the complaint, the mortgaged properties were systematically worth less than what Barclays represented to investors.

Criminal Cases

40-Year Prison Sentence, More than $180 Million Forfeiture Order for Former Chief Financial Officer of Resort Development; JPMorgan Chase Bank Former Senior Loan Officer Sentenced, Florida

Last year, we reported that David Schwarz, the former Chief Financial Officer and partial owner of Cay Clubs Resorts and Marinas (Cay Clubs), was convicted in March 2017 after a jury trial on charges of conspiracy to commit bank fraud, bank fraud, and interference with the administration of Internal Revenue laws. Cay Clubs marketed vacation rental units for 17 locations in Florida, Las Vegas, and the Caribbean and raised more than $300 million from investors by promising to develop dilapidated properties into luxury resorts. Cay Clubs incentivized investors by promising an upfront "leaseback" payment of 15-20% of the unit sales price at the time of closing. These incentives were concealed from the lenders and the Enterprises. As Cay Clubs experienced financial difficulties, Schwarz conspired with others at Cay Clubs to recruit insiders as straw buyers to obtain mortgages on Cay Clubs condominiums. The loan proceeds were then diverted to the failing Cay Clubs Company and to pay out investor leaseback payments.

In a related case Ross Pickard pled guilty in May 2017 to conspiracy to commit loan and credit application fraud for his role in this scheme. According to the plea agreement, Pickard was a senior loan officer at JP Morgan Chase Bank. He conspired with others in a scheme to defraud the bank by completing, certifying, and submitting mortgage loan applications on behalf of borrowers that contained false and fraudulent statements. The false statements included, but were not limited to, false occupancy, overinflated income and assets, as well as the understated liabilities. By relying on Pickard's false and fraudulent statements on the loan applications, JP Morgan Chase was induced into funding mortgage loans for otherwise unqualified borrowers.

In May 2017, Schwarz was sentenced to 480 months in prison, 5 years of supervised release, and ordered forfeiture of cash and real property of over $304 million. An amended restitution order was filed during July 2017, ordering Schwarz's total restitution of over $181 million. Both the forfeiture and restitution were ordered jointly and severally with co-conspirators. In August 2017, Pickard was sentenced to 36 months in prison, 36 months of supervised release, and ordered to pay over $33 million in restitution and roughly $470,000 in forfeiture for his role in this scheme, which caused losses to Fannie Mae and Freddie Mac of more than $11 million dollars.

Three Found Guilty After Trial in $10 Million Nationwide Loan Modification Scheme; Sentenced to Prison Terms of up to 20 Years; Restitution Ordered up to $10.2 Million, Virginia

In July 2017, Sammy Araya, Michael Henderson, and Jen Seko were sentenced to a combined 39 years in prison after their convictions by a federal jury for their roles in a nationwide, multi-year mortgage modification fraud scheme that victimized hundreds of homeowners out of at least $10 million. Araya, Henderson, and Seko were sentenced to 240 months, 144 months, and 84 months in prison, respectively, and 36 months of supervised release. Restitution hearings were held between August and September 2017, where each co-defendant was jointly and severally ordered restitution, ranging from $9 to $10.2 million.

According to court records and evidence presented at trial, Araya, Henderson, and Seko operated a large-scale scam that victimized vulnerable individuals and families across the country for several years. The conspirators sent targeted mass mailers to homeowners facing foreclosure through Seko's company, Seko Direct Marketing. The mailers referenced federal programs designed to help struggling homeowners and were titled "Notice of Mortgage Relief," among other misleading titles. The mailers listed various toll-free telephone numbers for the homeowners to call for assistance. When a victim homeowner called the toll-free number listed on the mailer, a member of the conspiracy posing as a "customer service representative" would answer the phone and collect financial information from the victim. Henderson served as one of the purported "customer service representatives" and helped to distribute the money collected by the scam, while Araya was the mastermind and principal beneficiary of the fraudulent operation.

After being contacted by another member of the conspiracy and told that their mortgage modification had been approved, the victim homeowners would be told that their lender required a "reinstatement fee," usually in the amount of thousands of dollars. Victims were also told that they were required to make several "trial" mortgage modification payments. After these so-called "trial payments" were completed, their modification would be complete, and their new lower mortgage payment would become permanent for the life of the loan. In reality, however, the members of the conspiracy were simply diverting the victims' payments for their own personal benefit, without doing anything to assist in modifying the victims' mortgages. Araya used the proceeds of the fraud to purchase expensive vehicles, a racehorse, luxury goods, personal travel, and a reality television show he produced called "Make It Rain.TV."

This scheme had devastating consequences for the victim homeowners, all of whom were already in a precarious financial position. Many victims suffered substantially greater financial hardship after falling victim to this conspiracy than they were already facing when they entered into the fraudulent agreements with the conspirators. In many cases, the lenders ultimately foreclosed on the victims' homes after the victims had been induced to make their "trial" mortgage payments to the members of the conspiracy rather than to their lenders. In addition to the millions stolen from struggling homeowners, the scheme resulted in an estimated $3.8 million in losses to financial institutions and approximately $1.1 million in potential losses to the Enterprises.

In related cases, in June 2017, Nicholas Estilow and Sabrina Rafo were sentenced for their roles in this scheme. Estilow and Rafo were sentenced to 80 and 60 months in prison, respectively, and 3 years of supervised release. Both defendants were additionally ordered restitution of over $3.6 million and forfeiture of over $9.3 million, jointly and severally.

Three Found Guilty in Builder Bailout Fraud Scheme Trial, Illinois

In October 2017, Theodore Wojtas, Jr., Karin Ganser, and David Belconis were convicted by a federal jury on charges of wire fraud and mail fraud for their participation in a mortgage fraud scheme involving the marketing and sale

of condominiums at a 50-acre development known as The Woods at Countryside in Palatine, Illinois (the Woods). Belconis was additionally convicted on charges of false statements.

The co-defendants used an assortment of advertising methods and sales pitches—on air, online, in writing, and at live presentations—to falsely promote the purchase of condominiums at the Woods as a means to financial independence and wealth, enticing prospective condominium buyers with substantial, unsustainable financial incentives, including down payment refunds and up to three years' worth of mortgage payments, maintenance costs, and property tax payments.

Additionally, the co-defendants colluded to misrepresent and conceal material facts from banks and mortgage lenders to fraudulently induce them to approve non-conforming loans to unqualified buyers, thereby exposing lenders and the Enterprises to millions of dollars in potential losses. The Enterprises purchased over $32 million in mortgage loans that had been made to condominium buyers at the Woods. The fraud scheme caused more than $16 million in losses to banks, mortgage lenders, and the Enterprises, whose combined losses are over $1.3 million.

Former Settlement Agent Sentenced After Guilty Trial Verdict, New Jersey

In March 2018, Mark Andreotti was sentenced to 144 months in prison, 5 years of supervised release, and ordered to pay over $2.1 million in restitution. Andreotti was previously convicted at trial on charges of bank fraud, conspiracy to commit bank fraud, tax evasion, and failure to file tax returns.

According to documents filed in this case and evidence presented at trial, Andreotti submitted a loan application to a bank requesting $625,000 to refinance his home mortgage. Andreotti, who owned and operated Metropolitan Title and Abstract (Metropolitan), used Metropolitan as the settlement agent on the transaction. After the bank transferred the $625,000 for the refinance to Metropolitan's escrow account, Andreotti spent the money on other expenses instead of paying off the first mortgage on the house.

Later, Andreotti conspired with another individual who worked as a real estate attorney to obtain $480,000 by claiming that the money would be used to refinance the mortgage on the attorney's house. After the bank transferred the money for the refinance to Metropolitan's escrow account, Andreotti kept $110,000 for himself before transferring the remaining funds to the other conspirator.

This scheme resulted in at least $1.1 million in losses to financial institutions and Fannie Mae.

Office of Inspector General U.S. Department of Housing and Urban Development

The U.S. Department of Housing and Urban Development (HUD) Inspector General is one of the original 12 Inspectors General authorized under the Inspector General Act of 1978. The HUD Office of Inspector General (OIG) strives to make a difference in HUD's performance and accountability. HUD OIG has a strong commitment to its statutory mission of detecting and preventing fraud, waste, and abuse and promoting the effectiveness and efficiency of government operations.

While organizationally located within HUD, HUD OIG operates independently with separate budget authority. Its independence allows for clear and objective reporting to HUD's Secretary and Congress. HUD's primary mission is to improve housing and expand opportunities for families seeking to improve their quality of life. HUD does this through a variety of housing and community development programs aimed at helping Americans nationwide obtain affordable housing. These programs are funded through a $46.9 billion annual congressional appropriation.

In addition, within HUD are the Federal Housing Administration (FHA) and Government National Mortgage Association (Ginnie Mae). FHA provides mortgage insurance for single-family homes, multifamily properties, nursing homes, and hospitals. FHA is self-funded through mortgage insurance premiums and receives limited congressional funding. FHA generated more than $1.2 trillion in insured loans in fiscal year 2017, and Ginnie Mae securitized almost $2 trillion in mortgage-backed securities. A majority of the mortgage-backed securities are FHA-insured mortgages.

Ginnie Mae guarantees the timely payment of principal and interest on mortgage-backed securities to institutional investors worldwide. These securities, or "pools" of mortgage loans, are used as collateral for the issuance of securities. Mortgage-backed securities are commonly referred to as "pass-through" certificates because the principal and interest of the underlying loans are passed through to investors. Ginnie Mae guarantees only securities backed by mortgage loans insured by government agencies, including FHA, the U.S. Department of Veterans Affairs, HUD's Office of Public and Indian Housing, and the U.S. Department of Agriculture's Rural Development. Ginnie Mae offers the only mortgage-backed securities carrying the full faith and credit guaranty of the United States Government, which means that its investors are guaranteed payment of principal and interest in full and on time.

While there are other HUD programs that are vulnerable to fraud and abuse, HUD OIG spends considerable time on the FHA program because of the changes in the mortgage industry, Ginnie Mae's increased reliance on contractors, and the increase of nonbanks as Ginnie Mae issuers.

While FHA's market share is moving downward, FHA continues to be a dominant factor in the mortgage market. In testimony, the Inspector General stated that OIG continues to have concerns regarding the ability of FHA's and Ginnie Mae's systems and infrastructure to adequately meet their requirements and perform their services.

These concerns were also expressed by OIG to FHA and Ginnie Mae through audits and comments on proposed rule changes. Some of these are longstanding issues that were highlighted in OIG's work products from as far back as the early to mid-1990s.

As an example, after 6 years of being below the statutorily required minimum capital ratio of 2 percent, the FHA Mutual Mortgage Insurance fund has 3 years of being above the required minimum.

OIG continues to have concerns that an increase in demand on the FHA and U.S. Department of Veterans Affairs programs will have collateral implications for the integrity of the Ginnie Mae mortgage-backed securities program, including the potential for increases in fraud in that program. Ginnie Mae securities are the only mortgage-backed securities to carry the full faith and credit guaranty of the United States. In addition, if an issuer fails to make the required pass-through payment of principal and interest to mortgage-backed securities investors, Ginnie Mae is required to assume responsibility for it by defaulting the issuers and assuming control of the issuers' mortgage-backed securities pools.

A significant problem facing FHA and the lenders it works with was the decreasing home values of foreclosed-on properties. FHA's sale of foreclosed-on properties continues to have returns of less than 50 percent of FHA's expenditures on the mortgage. These issues reinforce the importance for FHA-approved lenders to maintain solid underwriting standards and quality control processes to withstand severe adverse economic conditions.

Over the years, HUD OIG has continued to report on the mediocre underwriting efforts and quality control processes of some FHA-approved lenders. Based on the results of the mortgage loan origination and underwriting initiative, HUD OIG again partnered with the U.S. Department of Justice's Civil Division, as well as a number of U.S. Attorneys' Offices and HUD's Office of General Counsel, to investigate FHA-approved lenders for potential fraud and to facilitate litigation under the False Claims Act and other statutes when warranted. OIG's reviews focused on FHA's mortgage lenders that posed the greatest risk regarding their compliance with FHA's underwriting requirements and their quality control processes. HUD OIG staff will continue assisting in these efforts into fiscal year 2018.

In recent years, HUD OIG has enhanced its efforts to identify and investigate civil fraud and pursue civil actions and administrative sanctions, frequently combining efforts from its multiple disciplines to create teams of auditors, special agents, attorneys, and data analysts to conduct civil investigations. The central hub to these efforts is HUD OIG's Joint Civil Fraud Division, a distinct team of forensic auditors and special agents dedicated to investigating fraud and pursuing civil and administrative remedies.

HUD OIG's joint civil fraud teams work closely with the U.S. Department of Justice, U.S. Attorney's Offices, HUD's Office of General Counsel, and local prosecutors to pursue civil remedies under a variety of statutes and regulations, including the False Claims Act; Program Fraud Civil Remedies Act; and Financial Institutions Reform, Recovery, and Enforcement Act. HUD OIG also works with HUD's Departmental Enforcement Center to pursue debarments, suspensions, and limited denials of participation when appropriate.

HUD OIG's internal joint efforts, in conjunction with those of other enforcement groups, result in civil outcomes that are meant to help HUD recover from unwarranted damages sustained due to fraud.

This year, HUD OIG is highlighting four areas of concern related to the financial market as follows:

1. The Joint Civil Fraud Division recovered more than $200 million in settlement agreements from lenders.

2. OIG issued a disclaimer of opinion on Ginnie Mae's fiscal years 2016 and 2017 financial statements.

3. Fiscal year 2017 examples of the Office of Investigation's closed mortgage fraud cases with restitutions in excess of $300 million.

4. The Office of Evaluation issued a brief on the ever-increasing number of nonbanks as Ginnie Mae issuers.

1. Joint Civil Fraud

- HUD OIG assisted the U.S. Department of Justice, Washington, DC, and the U.S. Attorney's Office, Eastern District of Michigan, in the civil investigation of United Shore Financial Services, LLC. United Shore is a Federal Housing Administration (FHA)-approved mortgage lender with its principal place of business located in Troy, MI.

  On December 28, 2016, United Shore entered into a settlement agreement with the Federal Government to pay $48 million to avoid lengthy litigation of certain civil claims the Government stated that it had against United Shore. As part of the settlement, United Shore agreed that it engaged in certain conduct in connection with its origination, underwriting, quality control, and endorsement of single-family residential mortgage loans insured by FHA. As a result of United Shore's conduct, HUD insured loans approved by United Shore that were not eligible for FHA mortgage insurance under the direct endorsement program and that HUD would not otherwise have insured.

- HUD OIG, in coordination with the U.S. Department of Justice's Civil Division and the U.S. Attorney's Office for the Northern District of Illinois' Eastern Division, conducted a joint review of the former president and founder of MDR Mortgage Corporation in Palatine, IL.

  On November 23, 2016, a judgment of more than $10 million was entered against the former president and founder of MDR Mortgage in favor of the U.S. Government. Of the more than $10 million judgment, HUD's loss totaled more than $3.4 million.

- HUD OIG assisted DOJ and the U.S. Attorney's Offices, District of New Jersey, District of Minnesota, and Southern District of Florida, in the civil investigation of PHH Corporation, PHH Mortgage Corporation (PHHMC), and PHH Home Loans, LLC (PHHHL), collectively referred to as PHH.

  On August 3, 2017, PHH entered into a settlement agreement with the Federal Government to pay $65 million in a combined settlement amount. The United States attributed $45.5 million to PHHMC and $19.5 million to PHHHL. PHH agreed that it engaged in certain conduct related to FHA-insured mortgages in connection with PHHMC's and PHHHL's origination, underwriting, endorsement, and quality control of single-family residential mortgage loans insured by FHA between January 1, 2006, and December 31, 2011, that resulted in claims for payment submitted to FHA on or before June 30, 2013. The settlement agreement was neither an admission of liability by PHH nor a concession by the United States that its claims were not well founded.

- HUD OIG assisted DOJ, Washington, DC, and the U.S. Attorney's Office for the Middle District of Florida in a civil investigation of Financial Freedom Acquisition, a division of CIT Bank, N.A. Financial Freedom was originally owned by IndyMac Bank until its failure in 2008, when the Federal Deposit Insurance Corporation was appointed as conservator. On March 18, 2009, OneWest Bank, N.A., based in Pasadena, CA, acquired the assets of Financial Freedom. On August 3, 2015, CIT Group acquired OneWest Bank, including Financial Freedom. The home equity conversion mortgage (HECM) servicing operations for Financial Freedom were located in Austin, TX.

  On May 16, 2017, Financial Freedom entered into a settlement agreement with the Federal Government to pay nearly $68.3 million to avoid the delay, uncertainty, inconvenience, and expense of lengthy litigation. Financial Freedom also had paid HUD more than $21 million related to the covered conduct through HUD's Supplemental Claims system, for a total settlement value of nearly $89.3 million. The Federal Government alleged that Financial Freedom sought to obtain insurance payments for debenture interest from HUD and did not disclose on the insurance claim forms that the lender was not eligible for such interest payments. The settlement was neither an admission of liability by Financial Freedom nor a concession by the United States that its claims were not well founded.

  As a result of Financial Freedom's conduct, lenders on relevant home equity conversion mortgages (HECM) obtained additional debenture interest that they were not entitled to receive. HUD incurred substantial losses

when it paid additional debenture interest on HECM claims on the loans covered by the settlement agreement. Of the nearly $89.3 million settlement, FHA received $41 million, and the remaining amount was paid to other Federal entities.

2. Ginnie Mae's Disclaimer for the Fourth Consecutive Year

HUD OIG audited Ginnie Mae's fiscal years 2017 and 2016 (restated) financial statements, including its report on Ginnie Mae's internal control and test of compliance with selected provisions of laws and regulations applicable to Ginnie Mae.

In fiscal year 2017, for the fourth consecutive year, OIG was unable to obtain sufficient, appropriate evidence to express an opinion on the fairness of the $3.6 billion (net of allowance) in nonpooled loan assets from Ginnie Mae's defaulted issuers' portfolio as of September 30, 2017. Ginnie Mae also continued to improperly account for FHA reimbursable costs as an expense instead of capitalizing them. Additionally, critical information needed to perform the audit was not provided in sufficient time to audit the guaranty asset and guaranty liability financial statement line items. The combination of these unresolved issues for a number of years was both material and pervasive because it impacted multiple financial statement line items across all of Ginnie Mae's basic financial statements.

As a result of the scope limitation in OIG's audit work and the effects of material weaknesses in internal control, OIG has not been able to obtain sufficient, appropriate evidence to provide a basis for an audit opinion on Ginnie Mae's fiscal years 2017 and 2016 (restated) financial statements. Based on the results of its work, OIG identified four material weaknesses, one significant deficiency, and one reportable noncompliance with selected provisions of laws and regulations.

3. Office of Investigation's Fiscal Year 2017 Examples of Closed Mortgage Fraud Cases

- Seven employees of a mortgage modification company were sentenced in U.S. District Court in connection with earlier guilty pleas to conspiracy to commit mail fraud, wire fraud, and misprision of a felony. Collectively, the defendants were sentenced to more than 26 years imprisonment and ordered to pay more than $2.4 million in restitution to the victims. The defendants jointly operated a series of California-based companies that falsely purported to provide home loan modification services to many homeowners in exchange for upfront fees. To induce homeowners to pay these fees, the defendants told the homeowners they had been approved for modifications on extremely favorable terms, the modification already had been negotiated with the homeowners' lenders, and they would receive financial assistance under various government relief programs. None of those promises were true, and few homeowners received any type of mortgage loan modification through the defendants' companies. HUD OIG; the United States Postal Inspection Service; the Federal Bureau of Investigation (FBI); the Special Inspector General for the Troubled Asset Relief Program (SIGTARP); the Federal Housing Finance Agency (FHFA) OIG; and the U.S. Department of Homeland Security, Investigations, conducted this investigation.

- Seven employees of an FHA-insured lender were sentenced in U.S. District Court for their earlier guilty pleas to conspiracy and wire fraud for their roles in a mortgage fraud conspiracy. Collectively, the defendants were sentenced to a total of 17 years of probation and ordered to pay almost $57 million in restitution to FHA. The employees participated in a mortgage fraud scheme by accepting, processing, and submitting fraudulent loan applications for as many as 189 FHA-insured mortgages that contained false information pertaining to borrower income, assets, employment, rental payments, and other credit worthiness documentation. HUD OIG and the FBI conducted this investigation.

- Five codefendants were sentenced in U.S. District Court following their convictions of mail fraud, wire fraud, and conspiracy. Collectively, the defendants were sentenced to 10 years in jail and ordered to pay more than $1.8 million in restitution to FHA and $3.1 million to various victims. The codefendants recruited individuals to purchase renovated houses owned by development companies and falsified income and asset information in

order for borrowers to qualify for the home loans. The defendants then received substantial payments from the proceeds of the sales. HUD OIG and the FBI conducted this investigation.

- In a civil judgement filed in U.S. District Court, the founder of a mortgage company was ordered to pay the government $10.3 million for violations of the False Claims Act. The owner submitted false verification forms showing that the HUD-approved loan correspondent was not involved in any proceeding "that could result in or has resulted in a criminal conviction, debarment, limited denial of participation, suspension or civil monetary penalty," when he was under indictment. FHA realized losses of more than $3.4 million when 237 FHA-insured loans defaulted. HUD OIG conducted this investigation.

- Ten employees of a mortgage modification company were sentenced in U.S. District Court in connection with earlier guilty pleas to and convictions of wire fraud, mail fraud, and conspiracy to commit wire fraud. Collectively, the defendants were sentenced to more than 104 years imprisonment and ordered to pay more than $10.2 million in restitution to the victims. The conspirators targeted distressed homeowners, making misrepresentations to induce them to make payments of thousands of dollars each in exchange for supposed mortgage modification assistance. The defendants did nothing to modify the mortgages and used the victims' payments for their own personal benefit. Victims suffered losses exceeding $11 million. HUD OIG, SIGTARP, the United States Postal Inspection Service, and FHFA OIG conducted this investigation.

- A Federal jury found two lenders, their president, and a senior vice president liable for violations of the False Claims Act and the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 for misrepresentations in connection with the FHA program. A Federal judge in U.S. District Court ordered the defendants to pay more than $298.5 million to FHA for those violations. The lenders originated loans through branches not approved by HUD, made false certifications to HUD regarding branch operations, submitted fictitious quality control reports to HUD, and failed to disclose that the company had been sanctioned by regulators and that some employees had felony convictions. HUD OIG, the HUD Office of General Counsel, and the U.S. Attorney's Office conducted this investigation.

4. Office of Evaluation Brief on the Ever-Increasing Number of Nonbanks as Ginnie Mae Issuers

By the end of fiscal year 2016, Ginnie Mae had made guaranties on loans with a remaining principal balance (RPB) of approximately $1.73 trillion.[3] Through these guaranties, Ginnie Mae facilitates capital inflows to the U.S. housing market. Since 2010, Ginnie Mae's RPB has grown by approximately 62 percent. During this time, Ginnie Mae's business has increasingly relied on nonbanks, which now represent a majority of issuances annually.[4] As OIG and Ginnie Mae have previously noted, the increase in the number of nonbank issuers and their complexity present a challenge for monitoring efforts. OIG is highlighting monitoring challenges so HUD leadership is aware of and can be better prepared to address them. It is imperative that Ginnie Mae has the appropriate staffing with the skills, knowledge, and abilities to monitor nonbanks. OIG is focusing on Ginnie Mae's capacity to monitor nonbanks with an ongoing audit.

During preliminary work, OIG found that Ginnie Mae's organizational structure and staff levels have not kept pace with the growth and changes in the mortgage industry. OIG believes this poses a greater risk to Ginnie Mae's ability to properly monitor and mitigate the risks posed by nonbanks than whether its compliance reviews ensure that nonbank issuers service loans in accordance with its rules and requirements. If the final audit results confirm this condition, it will correspond with the finding of a fall 2016 study self-initiated by Ginnie Mae.[5]

3 A guaranty is a formal pledge to pay another person's debt or to perform another person's obligation in the case of default.

4 The U.S. Government Accountability Office has defined banks as "bank holding companies, financial holding companies, savings and loan holding companies, insured depository institutions, and credit unions, including any subsidiaries or affiliates of these types of institutions." Nonbanks are any other entities.

5 KPMG LLP conducted a business process reengineering study and delivered its results to Ginnie Mae on September 26, 2016. KPMG concluded that understaffing creates "…an impaired ability for Ginnie Mae to monitor its Issuers for sources of risk that could impair investor confidence in the Ginnie Mae Mortgage-Backed Security (MBS), to resolve Issuer failures effectively and with minimal cost and disruption, and to support the government mortgage finance system by allowing a competitive market to flourish." KPMG found that contractors account for 68 percent of the full-time employees performing Ginnie Mae core competencies and 84 percent of all Ginnie Mae full-time employees. When KPMG benchmarked Ginnie Mae staffing, KPMG determined that the Ginnie Mae workforce difference, when compared to similarly situated entities, was 582, meaning that Ginnie Mae staffing would be approximately 1,434 rather than 852 if it were staffed at a level comparable to similarly situated entities.

Beyond this audit, OIG will regularly collect and analyze data to focus on Ginnie Mae's most pressing challenges. OIG analytics are intended to identify trouble spots before they become another event like Taylor, Bean & Whitaker. OIG looks forward to continuing a productive relationship and furthering its role in helping HUD and Ginnie Mae identify risks and overcome challenges to their missions.

The tasks before HUD OIG continue to be daunting. Challenges remaining include

- Addressing the elements of fraud that were involved in the collapse of the mortgage market and monitoring the rollout of new FHA loan products to reduce exploitation of program vulnerabilities.

- Combating perpetrators of fraud, including those who have migrated from the subprime markets, who seek to exploit FHA loan programs.

- The emergence of certain aspects of seller-funded downpayment assistance by nonprofits and State housing finance agencies.

The consequences of the mortgage crisis, its worldwide economic implications, and the resulting pressures placed on HUD and HUD OIG come at a time when HUD has had significant new leadership responsibilities. Over the last 8 years, HUD has also been focused on rebuilding communities devastated by disasters, such as Lower Manhattan post-September 11 and Hurricanes Katrina, Rita, and Wilma, which have added tens of billions of dollars in new program funds, requiring quick distribution and keen oversight. The devastating hurricanes and floods in late 2017 that hit Houston, Florida, Puerto Rico, and the Virgin Islands and the wild fires in California increased the demand on HUD OIG's resources. HUD OIG continues to work closely with the Department as it implements the funding for recovery from these natural disasters.

Office of Inspector General National Credit Union Administration

The NCUA OIG promotes the economy, efficiency, and effectiveness of NCUA programs and operations and detects and deters fraud, waste, and abuse, thereby supporting the NCUA's mission of providing, through regulation and supervision, a safe and sound credit union system that promotes confidence in the national system of cooperative credit.

Agency Overview

The National Credit Union Administration (NCUA) is responsible for chartering, insuring, and supervising federal credit unions and administering the National Credit Union Share Insurance Fund (Share Insurance Fund). The agency also manages the Operating Fund,[6] the Community Development Revolving Loan Fund,[7] and the Central Liquidity Facility.[8]

Credit unions are member-owned, not-for-profit cooperative financial institutions formed to permit members to save, borrow, and obtain related financial services. NCUA charters and supervises federal credit unions, and insures accounts in federal and most state-chartered credit unions across the country through the Share Insurance Fund, a federal fund backed by the full faith and credit of the United States government.

In September 2017, the NCUA Board voted to close the Temporary Corporate Credit Union Stabilization Fund and transfer its remaining assets and obligations into the Share Insurance Fund. The Stabilization Fund was created in May 2009 as a revolving fund in the U.S. Treasury that gave NCUA flexibility to manage costs to the credit union system resulting from losses on faulty mortgage-backed securities purchased by five failed corporate credit unions that NCUA liquidated during the financial crisis.

The agency's mission is to provide through regulation and supervision, a safe and sound credit union system that promotes confidence in the national system of cooperative credit. The agency also has a vision to protect consumer rights and member deposits. Finally, NCUA is further dedicated to upholding the integrity, objectivity, and independence of credit union oversight. The agency implements initiatives designed to meet these goals.

6 The Operating Fund was created by the Federal Credit Union Act of 1934. It was established as a revolving fund in the United States Treasury under the management of the NCUA Board for the purpose of providing administration and service to the federal credit union system. A significant majority of the Operating Fund's revenue is comprised of operating fees paid by federal credit unions. Each federal credit union is required to pay this fee based on its prior year asset balances and rates set by the NCUA Board.

7 The NCUA's Community Development Revolving Loan Fund, which was established by Congress, makes loans and Technical Assistance Grants to low-income designated credit unions.

8 The Central Liquidity Facility is a mixed-ownership government corporation the purpose of which is to supply emergency loans to member credit unions.

Major NCUA Programs

Supervision

The agency's supervision program is designed to ensure the safety and soundness of the credit union system. NCUA supervises credit unions through annual examinations, regulatory enforcement, providing guidance in regulations and letters, and taking supervisory and administrative actions as necessary.

NCUA's Office of National Examinations and Supervision oversees examination and supervision issues related to consumer credit unions with assets greater than $10 billion and all corporate credit unions. Due to the relative size of their insured share base, they are deemed systemically important to the Share Insurance Fund. In addition, under the Dodd-Frank Act, the Bureau of Consumer Financial Protection (BCFP) has the authority to examine compliance with certain consumer laws and regulations by credit unions with assets over $10 billion.

Insurance

The NCUA administers the Share Insurance Fund, which provides insurance for deposits held at federally-insured natural person and corporate credit unions nationwide, up to $250,000 per depositor. The fund is capitalized by credit unions.

Credit Union Resources and Expansion

The NCUA's Office of Credit Union Resources and Expansion (CURE) supports credit union growth and development, including providing support to low-income credit unions, minority credit unions, and any credit union seeking assistance with chartering, charter conversions, by-law amendments, field of membership expansion requests, and low-income designations. CURE also provides access to online training and resources, grants and loans, and a program for preserving and growing minority institutions.

Consumer Protection

The NCUA's Office of Consumer Financial Protection (OCFP) is responsible for consumer protection in the areas of fair lending examinations, member complaints, and financial literacy. OCFP consults with the BCFP, which has supervisory authority over credit unions with assets of $10 billion or more. BCFP also can request to accompany NCUA on examinations of other credit unions. In addition to consolidating consumer protection examination functions within the agency, OCFP responds to inquiries from credit unions, their members, and consumers involving consumer protection and share insurance matters. Additionally, the office processes member complaints filed against federal credit unions.

Asset Management

The NCUA's Asset Management and Assistance Center (AMAC) conducts credit union liquidations and performs management and recovery of assets. AMAC assists agency regional offices with the review of large complex loan portfolios and actual or potential bond claims. AMAC also participates extensively in the operational phases of conservatorships and records reconstruction. AMAC's purpose is to minimize costs to the Share Insurance Fund and to credit union members.

Office of Minority and Women Inclusion

The NCUA formed the Office of Minority and Women Inclusion in January 2011, in accordance with the Dodd-Frank Act. The office is responsible for all matters relating to measuring, monitoring, and establishing policies for diversity in the agency's management, employment, and business activities. It is also responsible for measuring, monitoring, and providing guidance about diversity for the agency's regulated entities, excluding the enforcement of statutes, regulations, and executive orders pertaining to civil rights.

Office of Continuity and Security Management

The Office of Continuity and Security Management evaluates and manages security and continuity programs across NCUA and its regional offices. The office is responsible for continuity of operations, emergency planning and response, critical infrastructure and resource protection, cyber threat and intelligence analysis, insider threats and counterintelligence, facility security, and personnel security.

The NCUA Office of Inspector General

The 1988 amendments to the Inspector General Act of 1978 (IG Act) established IGs in 33 designated federal entities (DFEs), including the NCUA.[9] The NCUA Inspector General (IG) is appointed by, reports to, and is under the general supervision of a three-member presidentially appointed Board. Currently, one seat on the NCUA Board is vacant. Staffing for the OIG consists of ten employees: the IG, the Deputy IG, the Counsel to the IG/Assistant IG for Investigations, the Director of Investigations, five auditors, and an office manager. The OIG promotes the economy, efficiency, and effectiveness of agency programs and operations, and detects and deters fraud, waste, and abuse, thereby supporting the NCUA's mission of facilitating the availability of credit union services to all eligible consumers through a regulatory environment that fosters a safe and sound credit union system. The OIG supports this mission by conducting independent audits, investigations, and other activities, and by keeping the NCUA Board and the Congress fully and currently informed of its work.

Recent Work

In accordance with section 989(a)(2)(B) of the Dodd-Frank Act, the following highlights OIG work that focuses on issues particular to the NCUA but that also could be instructive for the broader financial sector.

Audit of the NCUA Information Technology Examination Program's Oversight of Credit Union Cybersecurity Programs

We issued an audit report on September 28, 2017, regarding NCUA's information technology examination program's oversight of federally insured credit unions' cybersecurity programs. Our audit concluded that the NCUA provided significant oversight of credit unions' cybersecurity programs, with the NCUA assessing credit unions' compliance with most National Institute of Standards and Technology (NIST) cybersecurity framework control guidelines. For examinations of federally insured credit unions with assets greater than $250 million, the NCUA required examiners to review credit unions' compliance with credit union member information security requirements and credit union compliance with electronic banking authentication guidance, which together covered 64 percent of NIST guidelines. The examination process also included an optional expanded review of a credit union's overall information security program. Performing this optional review addressed 91 percent of NIST guidelines.

We recommended that the NCUA implement an Automated Cybersecurity Examination Tool (ACET) that it had developed to increase and standardize examiners' reviews of credit union cybersecurity programs. NCUA's ACET was based on an assessment developed by the Federal Financial Institutions Examination Council (FFIEC) in 2015 and updated in 2017. The NCUA's ACET includes nearly 500 control measures and suggested steps for validating whether a credit union meets each of the control measures. We concluded that this expanded review of credit unions' cybersecurity programs would result in examiners assessing compliance with all NIST cybersecurity framework guidelines.

The NCUA agreed with our recommendation and issued a letter to credit unions in December 2017 indicating that it would begin implementing the ACET to improve and standardize its supervision related to cybersecurity. The NCUA already has required ACET for examinations of credit unions with over $1 billion in assets, and plans to require ACET for examinations of all federally insured credit unions by December 2018.

9 5 U.S.C. app. § 8G.

Conflict of Interest Investigation

After a referral from FSOC, we investigated a potential conflict of interest involving the NCUA Chairman. He participated in a vote, as a member of FSOC, to rescind FSOC's determination that material financial distress of American International Group (AIG) could pose a threat to U.S. financial stability, which removed AIG from the requirement of enhanced supervision by the Board of Governors of the Federal Reserve. At the time of the vote, he owned AIG stock worth approximately $7,500 and AIG warrants worth approximately $1,200.

We learned during our investigation that the Office of Government Ethics (OGE) believed that because the Chairman owned warrants, under 18 U.S.C. § 208, Acts affecting a personal financial interest, he could have a nonexempt financial interest that could have been affected by his participation in the vote regarding AIG. Our investigation found that the Chairman believed at the time of the vote that his AIG holdings fell under the OGE's de minimis exemption for publicly traded securities whose aggregate market value does not exceed $15,000, and therefore, as a result, he did not need to recuse himself from the FSOC vote. The Chairman asserted that warrants are treated the same as stock by securities lawyers and accountants and that warrants are publicly traded instruments, and also noted that the OGE has not provided any written guidance regarding the treatment of warrants. The Department of Justice declined prosecution of this case in January 2018.

Office of Inspector General
U. S. Securities and Exchange Commission

The U.S. Securities and Exchange Commission (SEC or agency) Office of Inspector General (OIG) promotes the integrity, efficiency, and effectiveness of the critical programs and operations of the SEC and operates independently of the agency to help prevent and detect fraud, waste, and abuse in those programs and operations, through audits, evaluations, investigations, and other reviews.

I. Background

The SEC's mission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. The SEC strives to promote a market environment that is worthy of the public's trust and characterized by transparency and integrity. Its core values consist of integrity, excellence, accountability, effectiveness, teamwork, and fairness. The SEC's strategic goals are to establish and maintain an effective regulatory environment; foster and enforce compliance with the Federal securities laws; facilitate access to the information investors need to make informed investment decisions; and enhance the Commission's performance through effective alignment and management of human, information, and financial capital.

The SEC is responsible for overseeing the nation's securities markets and certain primary participants, including broker-dealers, investment companies, investment advisers (IAs), clearing agencies, transfer agents, credit rating agencies, and securities exchanges, as well as organizations such as the Financial Industry Regulatory Authority, Municipal Securities Rulemaking Board, and the Public Company Accounting Oversight Board. Under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act), the agency's jurisdiction was expanded to include certain participants in the derivatives markets, private fund advisers, and municipal advisors.

The SEC's headquarters are in Washington, DC, and the agency has 11 regional offices located throughout the country. The agency's functional responsibilities are organized into 5 divisions and 25 offices, and the regional offices are primarily responsible for investigating and litigating potential violations of the securities laws. The offices also have examination staff to inspect regulated entities such as IAs, investment companies, and broker-dealers.

The SEC OIG was established as an independent office within the SEC in 1989 under the Inspector General Act of 1978, as amended (IG Act). The SEC OIG's mission is to promote the integrity, efficiency, and effectiveness of the SEC's critical programs and operations. The SEC OIG prevents and detects fraud, waste, and abuse through audits, evaluations, investigations, and other reviews related to SEC programs and operations.

The SEC OIG Office of Audits conducts, coordinates, and supervises independent audits and evaluations of the SEC's programs and operations at its headquarters and 11 regional offices. These audits and evaluations are based on risk and materiality, known or perceived vulnerabilities and inefficiencies, and information received from the Congress, SEC staff, the U.S. Government Accountability Office, and the public.

The SEC OIG Office of Investigations performs investigations into allegations of criminal, civil, and administrative violations involving SEC programs and operations by SEC employees, contractors, and outside entities. These investigations may result in criminal prosecutions, fines, civil penalties, administrative sanctions, and personnel actions. The Office of Investigations also identifies vulnerabilities, deficiencies, and wrongdoing that could negatively impact the SEC's program and operations.

In addition to the responsibilities set forth in the IG Act, Section 966 of the Dodd-Frank Act required the SEC OIG to establish a suggestion program for SEC employees. The SEC OIG established its SEC Employee Suggestion Program in September 2010. Under this program, the OIG receives, reviews, and processes suggestions from agency employees for improvements in the SEC's work efficiency, effectiveness, and productivity, and use of its resources, as well as allegations by employees of waste, abuse, misconduct, or mismanagement within the SEC.

II. SEC OIG Work Related to the Broader Financial Sector

In accordance with Section 989E(a)(2)(B)(i) of the Dodd-Frank Act, below is a discussion of the SEC OIG's completed and ongoing work, focusing on issues that may apply to the broader financial sector.

Completed Work

Audit of the Office of Compliance Inspections and Examinations' Investment Adviser Examination Completion Process, Report No. 541, July 21, 2017

The SEC's National Examination Program (NEP), conducted by the Office of Compliance Inspections and Examinations (OCIE), is risk-based and data-driven. As part of the NEP, OCIE examines SEC-registered entities, including about 12,000 IAs. According to the SEC's fiscal year (FY) 2016 Agency Financial Report, "OCIE uses the findings from these examinations to improve industry compliance, detect and prevent fraud, inform policy, and identify risks." We initiated this audit to assess the controls over OCIE's IA examination completion process and to follow-up on prior OIG recommendations.

We found that controls over OCIE's IA examination completion process are generally effective but improvements are needed. We reviewed documentation from all IA Corrective Action Reviews that OCIE approved between FYs 2015 and 2016 and closed in the Tracking and Reporting Examination National Documentation System as of November 22, 2016. We also reviewed documentation from a statistical sample of 240 of the 2,443 IA examinations that OCIE approved and closed in the Tracking and Reporting Examination National Documentation System during the same period. We did not find any deficiencies related to the IA CARs we reviewed. Moreover, we determined that OCIE has addressed prior OIG recommendations. However, we also identified deficiencies in OCIE's IA examination completion controls that warrant management's attention. Specifically, we found that two IA examination completion controls regarding control sheets and post-exam fieldwork lacked adequate segregation of duties; examiners did not always document preliminary exit interviews with examined IAs; and examiners either did not assign final risk ratings, or may have assigned final risk ratings inconsistently.

These deficiencies occurred because sufficiently robust policies and controls were not in place to prevent their occurrence. If OCIE does not appropriately review and consistently document IA examination results and risk assessments (1) examination work products may be more susceptible to error, (2) OCIE examiners' ability to sufficiently review prior examination findings and perform comprehensive risk assessments may be reduced, and (3) OCIE may not effectively consider the results of examinations during its evaluation of risk for future examinations. OCIE can improve its IA examination completion process and internal controls by updating or documenting policies and procedures consistent with the Standards for Internal Control in the Federal Government. During the audit, we also inquired about the status of (1) recommendations OCIE received in November 2016 from a consultant's efficiency study, and from an internal steering committee; and (2) plans to apply to the NEP the Government Accountability Office's Risk-Management Framework. We discussed with OCIE management, including the Acting Director, these other matters of interest, which did not warrant recommendations. We will continue to monitor these matters, as needed.

We issued a final report to the agency on July 21, 2017. To improve OCIE's IA examination completion process, we made three recommendations. We recommended that OCIE (1) design control activities related to the review and approval of examination work products to require adequate segregation of duties, (2) update NEP policies and procedures to more clearly define the requirements for documenting in the Tracking and Reporting Examination National Documentation System examination meetings and interviews, and (3) develop and disseminate to OCIE staff guidance for assigning final examination risk ratings before closing examinations. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

The report is available on our website at https://www.sec.gov/files/OIG_Final_Report_No._541-Audit_of_OCIE%27s_Investment_Adviser_Examination_Completion_Process_508_compliant_version_07-21-17.pdf.

Evaluation of the Division of Corporation Finance's Disclosure Review and Comment Letter Process, Report No. 542, September 13, 2017

In July 2016, some members of Congress requested that the SEC OIG and the Comptroller General of the Government Accountability Office jointly review the SEC's efforts to implement the agency's 2010 climate change guidance (SEC Release 33-9106), and assess the Division of Corporation Finance's (CF) comment letter process. Based on the request letter and our meeting with Congressional staff and the Government Accountability Office, the SEC OIG agreed to review and report on CF's disclosure review and comment letter process. In February 2018, the Government Accountability Office reported its observations related to disclosure requirements for climate change-related matters.

We found that CF established policies, procedures, and internal controls that provide overall guidance for how staff should conduct disclosure reviews and for how information, including comments, should be documented, tracked, and disseminated to companies and the public. We evaluated 95 of the more than 5,000 disclosure reviews conducted by CF staff in FY 2015, surveyed 325 CF disclosure review staff, and determined that staff generally complied with the established policies, procedures, and internal controls. In addition, more than 80 percent of survey respondents felt they (1) received sufficient training to conduct disclosure reviews, and (2) received or provided rationale for any proposed comments to companies that were waived or modified.

Although staff generally followed CF's disclosure review policies and procedures and the results of our survey of CF disclosure review staff were generally positive, we identified opportunities to improve CF's disclosure review documentation. Specifically, we found that examiners and reviewers did not always properly document comments before issuing comment letters to companies; some case files were incomplete as of the date CF issued a comment letter to a company; and examiners and reviewers inconsistently documented oral comments to companies.

These conditions may have occurred because there are no mechanisms or checks in place to ensure compliance with certain aspects of CF's policies, procedures, and internal controls for documenting written comments. In addition, guidance for documenting oral comments provided to companies is not detailed.

By not consistently or timely documenting written and oral comments, CF may not be able to fully and accurately explain the basis for its actions or adequately demonstrate that reviews were conducted effectively and that comments were appropriately reviewed before issuance. We also determined that the SEC's Office of Information Technology (OIT), in coordination with CF, did not establish or document the system security categorization or security controls for the Comment Letter Dissemination system. We discussed with management these other matters of interest, which did not warrant recommendations.

We issued a final report to the agency on September 13, 2017. To improve CF's disclosure review and comment letter process, we recommended that CF (1) establish a mechanism or control for CF staff to trace all comments provided to companies to examiner and reviewer reports before issuing comment letters; (2) establish a mechanism or control that ensures that CF staff follow policy to upload all examiner and reviewer reports to the internal workstation before issuing comment letters; and (3) establish detailed guidance on how examiners and reviewers should document oral comments provided to companies during disclosure reviews. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

The report is available on our website at https://www.sec.gov/files/Final-Report-Evaluation-of-Division-Corp-Fin-Disclosure-Review-and-Comment-Ltr.pdf.

Audit of the SEC's Progress in Enhancing and Redesigning the Electronic Data Gathering, Analysis, and Retrieval System, Report No. 544, September 28, 2017

The SEC's ability to fulfill its mission is, in part, dependent on the successful operation of the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. The SEC consistently spends more than $14 million a year on the EDGAR system, or about 6 percent of the agency's information technology budget. These costs cover both ongoing operations and enhancements to the current EDGAR system. Separately, since FY 2014, the agency has spent at least $3.4 million on efforts to redesign the EDGAR system. A disciplined process for managing the enhancements and redesign of the EDGAR system is necessary to ensure adequate system functionality and to avoid cost overruns and schedule delays in the SEC's efforts related to this mission-essential system.

Since 2014, the SEC has made several improvements in its planning and governance of the program to redesign the EDGAR system while continuously enhancing the system in operation. Our audit included reviewing a non-statistical sample of 6 of the 29 releases (or about 21 percent) deployed by the SEC to enhance the EDGAR system between October 1, 2013, and September 30, 2016. We also interviewed personnel and reviewed program documentation to assess the planning and governance of the SEC's EDGAR Redesign program.

We determined that (1) the SEC's governance of EDGAR system enhancements, including the governance and operation of the EDGAR Requirements Subcommittee and the EDGAR system enhancement lessons learned process, needs improvement; (2) OIT did not consistently manage the scope of EDGAR system releases to ensure SEC needs were achieved; (3) the SEC should improve its management of the EDGAR system engineering contract; (4) OIT did not fully and consistently implement EDGAR system enhancements in compliance with Federal and SEC change management controls; and (5) although the SEC has taken steps to improve its ability to develop and implement a new electronic disclosure system that meets agency needs, further improvements can strengthen the agency's EDGAR Redesign program governance and planning.

We issued our final report on September 28, 2017, and made nine recommendations, including that the SEC (1) more clearly define the EDGAR system governance structure; (2) enhance the relevant lessons learned process; (3) improve EDGAR system scope management processes; (4) ensure the EDGAR system engineering contractor complies with earned value management requirements and performance expectations; (5) update the EDGAR change management policies and procedures; and (6) address constraints impacting the timely completion, review, and approval of EDGAR Redesign program contract deliverables. Management concurred with all recommendations, which will be closed upon completion and verification of corrective action.

In addition, during our audit, two other matters of interest that did not warrant recommendations came to our attention. The first matter related to two systems the SEC used for enterprise configuration management, including to manage the configurations of the EDGAR system. We determined that OIT miscategorized one of the two systems and did not clearly define the other system as a component of the EDGAR system authorization boundary. The second matter related to potential negative impacts on system operations of ongoing EDGAR system enhancements resulting from rules adopted by the Commission. We discussed these matters with agency management for their consideration.

Because the audit report contains nonpublic information about the EDGAR system, only a redacted version of the report is available on our website at https://www.sec.gov/files/Audit-of-SECs-Progress-in-Enhancing-and-Redesigning-the-EDGAR-System.pdf.

Ongoing Work

Evaluation of the Office of Compliance Inspections and Examinations' Technology Controls Program

In recent years, the U.S. securities markets have been transformed by technological advances which have, among other things, substantially enhanced the speed, capacity, efficiency, and sophistication of the trading functions available to market participants. At the same time, technological advances have increased the risk of operational problems with automated systems, including failures, disruptions, delays, and intrusions.

This transformation of the U.S. securities markets occurred in the absence of a formal regulatory structure governing the automated systems of key market participants. Before 2015, the SEC's oversight of securities markets technology was conducted primarily pursuant to a set of voluntary principles known as the SEC's Automation Review Policy (ARP) Statements. Through the agency's ARP inspection program, the SEC oversaw about 25 entities, including securities exchanges, clearing organizations, and electronic communication networks. The SEC's Market Regulation Division (now known as the Division of Trading and Markets) administered the ARP inspection program, yet at times, had difficulty ensuring entities implemented recommendations for improvement due to the voluntary nature of the program.

In 2004, the Government Accountability Office criticized the voluntary nature of the ARP inspection program and recommended that the SEC propose a rule to make the program mandatory. On February 3, 2015, the SEC adopted Regulation Systems Compliance and Integrity (SCI) to strengthen the technology infrastructure of the U.S. securities markets. Regulation SCI applies to 44 entities (referred to as SCI entities) that directly support the following 6 key securities market functions: (1) order routing, (2) trading, (3) clearance and settlement, (4) market data, (5) market regulation, and (6) market surveillance.

The SEC's Office of Compliance Inspections and Examinations (OCIE) Technology Controls Program (TCP) oversees SCI entities' compliance with Regulation SCI by performing risk- and initiative-based inspections. The SEC's Technology Risk-Assurance, Compliance, and Examination Report system maintains documents related to these inspections.

The OIG has initiated an evaluation of OCIE's TCP. The objective of the evaluation is to assess OCIE's TCP and determine whether the program provided effective oversight of entities' compliance with Regulation SCI. Specifically, we plan to review the controls, including systems, policies, and procedures, in place for monitoring Regulation SCI compliance; evaluate the TCP inspection process; and review OCIE's management and oversight of its CyberWatch contract.

We expect to issue a report summarizing our findings during 2018.

Evaluation of the SEC's Handling of, and Response to, Electronic Data Gathering, Analysis, and Retrieval System Vulnerabilities

On September 23, 2017, the SEC Chairman sent a letter to the SEC's Inspector General, requesting that the OIG review the agency's handling of, and response to, a software vulnerability in the Commission's EDGAR system that the Chairman disclosed in his September 20, 2017, Statement on Cybersecurity.

The EDGAR system is central to the agency's mission and is critical to the functioning of the capital markets. The primary purpose of the EDGAR system is to increase the efficiency and fairness of the securities market for the benefit of investors, corporations, and the economy by accelerating the receipt, acceptance, dissemination, and analysis of time-sensitive corporate information filed with the agency. The EDGAR system is a complex system with multiple subsystems and components, which includes a test filing component. The test filing component of the EDGAR system allows companies to test their ability to create a filing in an EDGAR-acceptable format before submitting the companies' official filing.

In his Statement on Cybersecurity, the Chairman stated, "In August 2017, the Commission learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading. Specifically, a software vulnerability in the test filing component of [the] EDGAR system, which was patched promptly after discovery, was

exploited and resulted in access to nonpublic information. It is believed the intrusion did not result in unauthorized access to personally identifiable information, jeopardize the operations of the Commission, or result in systemic risk." Later, however, in his October 4, 2017, testimony before the United States House of Representatives Committee on Financial Services, the Chairman testified that he was "informed that the EDGAR test filing accessed by third parties in connection with the 2016 intrusion contained the names, dates of birth, and social security numbers of two individuals."

In response to the Chairman's request, the OIG has initiated an evaluation of the SEC's handling of, and response to, EDGAR system vulnerabilities. Specifically, we will (1) determine whether the SEC established key controls to ensure EDGAR system incidents and vulnerabilities were identified and reported in a timely manner; (2) evaluate the operating effectiveness of the SEC's incident handling processes, including processes for detecting, analyzing, containing, and eradicating EDGAR system vulnerabilities; (3) determine whether the SEC adequately assessed the security of the EDGAR system, including security assessments conducted during the change management process; and (4) determine whether known EDGAR vulnerabilities were remediated in a timely manner.

We expect to issue a report summarizing our findings during 2018.

Obstruction of an SEC Investigation by a Financial Advisor (Case No. 16-0571-I)

The SEC OIG and the U.S. Department of Justice (DOJ) jointly investigated a financial advisor, resulting in the individual being charged with obstructing an SEC investigation. Specifically, it was alleged that the individual had an arrangement with an attorney whereby the individual's company would pay the attorney a referral fee that the individual knew violated Federal and state regulations. After the individual's company discovered the payments, stopped them, and directed the individual to have the attorney return the fees already paid, the individual continued paying the referral fee by secretly writing checks to the attorney out of private checking accounts. The individual later testified about the referral agreement during a formal SEC investigation of the referral payments. The individual repeatedly described the referral agreement in a manner that was designed to prevent the SEC from learning about the individual's secret payments to the attorney and never mentioned the checks written to the attorney out of the individual's personal accounts.

On January 20, 2017, the individual pled guilty to one count of Obstruction of Proceedings in violation of 18 U.S.C. § 1505. The individual also entered into a separate agreement with the SEC that, among other sanctions and penalties, bars the individual for life from working in the securities industry. On April 20, 2017, the individual was sentenced to 1 year of probation, with 4 months to be served in home detention. The individual was also ordered to pay a $4,000 fine and a $100 Special Assessment. The DOJ press release describing the case is available at https://www.justice.gov/usao-ma/pr/connecticutfinancial-advisor-agrees-plead-guilty-obstructingsec-investigation.

Special Inspector General for the Troubled Asset Relief Program

The Special Inspector General for the Troubled Asset Relief Program (SIGTARP) has the duty, among other things, to conduct, supervise, and coordinate audits and investigations of the purchase, management, and sale of assets under the Troubled Asset Relief Program (TARP) or as deemed appropriate by the Special Inspector General.

Background

SIGTARP is primarily a Federal law enforcement agency protecting the interests of the American people by investigating crime at financial institutions that received TARP funds or at other TARP recipients in housing programs. All TARP programs are intended to promote financial stability.

When first created, SIGTARP found that financial institution fraud had evolved from the insider self-dealing fraud that marked the savings and loan crisis, to escape detection from traditional fraud identification methods of self-reporting and regulator referrals. SIGTARP created an intelligence-driven approach and leveraged technological solutions to discover insider crimes at banks that previously went undetected. Now, 100 bankers have been charged with and 84 bankers have been convicted of a crime resulting from SIGTARP investigations.

SIGTARP is now applying its intelligence-driven approach to search for crime in TARP housing programs. TARP recipients include large mortgage servicers in the Making Home Affordable (MHA) Program, like Wells Fargo, Bank of America, and JPMorgan Chase.

SIGTARP assesses that the top threat in TARP today is unlawful conduct by any of the 130 banks and other financial institutions in TARP's $27.8 billion MHA Program, where, as of March 31, 2018, Treasury had spent $18.8 billion, and will spend up to $9 billion through 2023. With an uptick in enforcement actions against financial institutions in MHA, SIGTARP is shifting resources to counter this threat.

The Most Serious Management And Performance Challenges & Threats Of Fraud, Waste, & Abuse Facing The Government In TARP

SIGTARP identifies the most serious management and performance challenges and threats facing the Government in TARP. Our selection is based on the significance and duration of the challenge/threat to the mission of TARP and to Government interests; the risk of fraud or other crimes, waste or abuse; the impact on agencies in addition to Treasury; and Treasury's progress in mitigating the challenge/threat.

Risk of Fraud, Waste, and Abuse by Large Banks and Others in the Making Home Affordable Program (Until Sept. 2023)

Unlawful conduct by any of the 130 financial institutions in MHA is the top threat in TARP. As of March 31, 2018, Treasury had paid $18.8 billion and will pay up to an additional $9 billion. These are not automated payments, but require reporting to Treasury and compliance with the law and Treasury's rules. The largest ten servicers – Ocwen, Wells Fargo, JPMorgan Chase, Bank of America, Nationstar, Select Portfolio Servicing, CitiMortgage, OneWest/CIT, Bayview Loan Servicing, and Ditech Financial - stand to receive $7.9 billion of the remaining $9 billion. Currently, there are nearly one million homeowners in the program and there has been a recent uptick in enforcement actions against MHA institutions. Despite finding wrongdoing by these financial institutions, such as servicers canceling homeowners out of the program for missing three mortgage payments when the servicer erred in applying the payments, Treasury is scaling back its compliance reviews. This raises the risk of fraud, waste, and abuse going undetected. The risk of fraud, waste, and abuse also jeopardizes the GSEs, FHA, and Veterans Affairs that participate in MHA.

Risk of Corruption, Antitrust Violations, Price Fixing, and Fraud in the Hardest Hit Fund Blight Elimination Program (Until Dec. 2021)

The Blight Elimination Program has expanded exponentially since the first $50 million allocation in 2013 to the city of Detroit to demolish abandoned homes and apartments. Using $768 million, currently, 269 cities or counties either have demolished or plan to demolish blighted properties, of which 41 have not yet reported starting demolitions. As SIGTARP reported in a June 2016 audit, Treasury did not apply standard controls that exist in HUD's blight program or in other Federal awards/ grants. SIGTARP reported that there were no federal requirements for competition or standard limitations to only pay necessary and reasonable costs. Treasury only partially implemented 2 of SIGTARP's 20 recommendations, leaving the program open to antitrust violations, fraud, and waste. The program's heavy reliance on city/county officials often not under contract in the program also creates risk of corruption, collusion, and abuse. For example, in December 2015, SIGTARP reported abuse by city officials in Evansville, Indiana who wanted to expand a university's medical school, to a site of a Ford dealership. City officials evicted people on the proposed new Ford dealership site so the homes would qualify as "abandoned" in TARP, used TARP to pay for the demolitions, and moved the Ford dealership to the demolished lots.

Risk of Waste and Misuse of TARP Dollars by State Agencies for Their Own Administrative Expenses in the Hardest Hit Fund (Until 2022)

Treasury has budgeted $1.1 billion in TARP dollars for administrative expenses of 19 state agencies to distribute $8.7 billion through the Hardest Hit Fund (HHF). In 2016 and 2017, SIGTARP identified $11 million in wasteful and unnecessary spending not associated with TARP by state housing agencies, including for example: catered barbeques with Treasury employees, parties, country club events, leasing a Mercedes, cash bonuses, gym memberships, gifts, free parking, settlements and legal fees in discrimination cases and employee perks. In October 2017, SIGTARP opened an audit into travel, conferences, and other administrative expenses. Additionally, in March 2018, SIGTARP issued an audit that found that while Treasury has dedicated $1.1 billion in HHF funds to operating and administrative expenses, including contracts for lawyers, accountants, auditors, consultants, providers of equipment, information technology, communications, risk management, training, and marketing, there were no Federal requirements for competition - even though millions of dollars in contracts have been, and will be, awarded.

Risk of Asbestos Exposure, Contaminated Soil and Illegal Dumping in the Hardest Hit Fund Blight Elimination Program (Until Dec. 2021)

The Army Corps of Engineers (Corps) worked with SIGTARP to issue a report on behalf of SIGTARP warning that the standard protections for demolition programs typically present in demolition grant programs are not present in the HHF program. The Corps found that Treasury and state agencies have not applied industry standard safeguards that protect against the risk of asbestos exposure, illegal dumping of debris, and contaminated soil material filling the hole.

Treasury has not implemented the SIGTARP/Corps' recommendations, even to require basic documentation of proper asbestos abatement, certain inspections, landfill receipts for dumping, and receipts showing the purchase of clean dirt.

SIGTARP's Investigations Approach

SIGTARP gained expertise in investigating large institutions which resulted in significant DOJ enforcement actions against Goldman Sachs, Bank of America, JPMorgan Chase, Morgan Stanley, Ally Financial, Wilmington Trust, Sun Trust Bank, Fifth Third Bank, Jefferies & Co., and RBS Securities.

SIGTARP's law enforcement counters threats to public safety and Government interests by investigating criminal actors and working with the Justice Department to prosecute those criminal actors. With 246 people sentenced to prison resulting from a SIGTARP investigation, at an average prison sentence of nearly five years, the threat these crimes pose is significant. SIGTARP's ongoing criminal investigations of recipients of TARP dollars in TARP housing programs promote free and fair trade by improving the overall condition for competition, and counter threats to public safety and Government interests, including financial institution fraud, public corruption, antitrust (unfair competition), contract fraud, and organized crime:

Financial Institution Fraud: SIGTARP's highest priority is investigating banks and other financial institutions receiving TARP dollars in the Making Home Affordable Program. Our investigations into TARP banks have already resulted in 100 bankers charged with and 84 convicted of a crime. Our remaining investigative work in this area is focused on supporting the Justice Department in its efforts to prosecute TARP bankers. Work on the bank bailout for FY 2018 supports Justice Department prosecutions of individuals investigated by SIGTARP, such as international money laundering charges related to a TARP bank, that help identify and reduce vulnerabilities in the financial system while stopping abuses by illicit actors.

Public Corruption: The corruption of local officials threatens public safety and fair competition. State and local officials award contracts under the $768 million Hardest Hit Fund blight demolition program.

Antitrust Violations: Unfair competitive practices in TARP housing programs including contract steering, bid rigging and price fixing, threatens the quality of work, harms public safety, threatens fair competition, and results in higher costs.

Contract Fraud, False Claims/Theft or Bribery in TARP Programs: Demolition contractors and State agencies play key roles in administering HHF programs. Fraud in any of these risk areas harm Government interests and fair competition.

Organized Crime: Organized crime in the $768 million blight demolition program or in TARP banks threatens public safety, fair competition and harms Government interests.

Selected SIGTARP's Investigations Results (April 1, 2017 to March 31, 2018)

Wilmington Trust Corporation

After an extensive SIGTARP investigation into the $330 million TARP recipient bank, on May 3, 2018, a jury found all four Wilmington Trust senior bank officer defendants, President Robert V.A. Harra Jr., CFO David Gibson, CCO William North, and Controller Kevyn Rakowski, guilty on all charges including concealing from the Federal Reserve, the Securities and Exchange Commission (SEC) and the investing public, the total quantity of past due loans on its books. The bank was also charged but, during jury selection, on October 10, 2017, Wilmington Trust resolved its indictment with DOJ and forfeited $60 million. Three other Wilmington Trust bank officers have been convicted following SIGTARP's investigation, including Vice President Joseph Terranova, Delaware Market Officer Brian Bailey, and Loan Officer Pete Hayes. Co-conspirator and Dover real estate developer Michael Zimmerman (now deceased) was also indicted. Two other co-conspirators were sentenced to prison: James Ladio, the former CEO of MidCoast Community Bank was sentenced to prison and ordered to pay $700,000 restitution, and Salvatore Leone was sentenced to prison and ordered to pay $784,568.

Sonoma Valley Bank

In the last quarter of 2017, SIGTARP supported an eight-week jury trial, including having a SIGTARP agent testify at trial. The jury's verdicts resulted in the conviction of the bank's former CEO Sean Cutting and former Chief Loan Officer Brian Melland for conspiracy, bank fraud, wire fraud, money laundering, falsifying bank records, lying to bank regulators, and other crimes. The jury also found guilty co-conspirator David Lonich, an attorney for real estate developer Bijan Madjlessi, who had been indicted before his death in 2014. Sonoma Valley Bank failed in August 2010, resulting in $8.65 million in lost TARP dollars.

Saigon National Bank

In 2018, trials are scheduled for criminal charges resulting from a SIGTARP investigation. In December 2015, SIGTARP agents, with other Federal law enforcement authorities, arrested 15 defendants (and charged 20 defendants across three indictments) in Operation "Phantom Bank," an alleged money laundering scheme for international narcotics trafficking and proceeds; some through Saigon National Bank. A total of 25 defendants have been indicted. The 109-page Federal Racketeer-Influenced and Corrupt Organizations Act (RICO) indictment against former bank CEO and President Tu Chau "Bill" Lu and others alleges that Lu orchestrated the scheme to launder millions in drug proceeds.

Excel Bank

As a result of a SIGTARP investigation, in January 2018, Shaun Hayes, the controlling shareholder in Excel Bank's bank holding company pled guilty to bank fraud and misapplication of Excel Bank funds. Excel Bank's Executive Vice President at the time of the scheme, Tim Murphy, previously pled guilty to bank fraud. Hayes admitted that he helped set up a loan to a straw party and caused $906,000 of the proceeds of that loan to be paid to Centrue Bank to pay off a loan that he and his business associate, Michael Litz, had guaranteed, with Hayes' interest concealed from Excel Bank. Litz also pled guilty in January 2018. Excel Bank failed in October 2012, resulting in nearly $4 million in lost TARP dollars.

GulfSouth Private Bank

On June 28, 2017, the President of GulfSouth Private Bank, Anthony Atkins, was sentenced to more than five years in prison and ordered to pay $2.4 million for bank fraud. Bank Vice President Sam Cobb was also sentenced to prison. SIGTARP agents obtained cooperation from Atkins' co-conspirators who were bank customers; each pled guilty in 2013 and provided information to SIGTARP. SIGTARP agents arrested bankers Atkins and Cobb in December 2016. When the bank failed, taxpayers lost $7.5 million in TARP.

SIGTARP's Audit Approach

SIGTARP conducts audits over TARP housing programs, helping promote financial stewardship by the Government. Much of SIGTARP's audit work is at the request of members of Congress. SIGTARP specializes in forensic audits that follow the money, analyzing general ledgers, credit card statements, invoices, and receipts.

SIGTARP assists Treasury in these efforts by auditing and evaluating housing programs to determine whether the Government is receiving fair value for its money and that recipients are spending TARP funds appropriately to accomplish the stated goals. To promote financial stewardship, SIGTARP reports on fraud, waste, and abuse and makes recommendations to Treasury (which has oversight of all TARP programs) to recover wasteful spending and prevent future fraud, waste, and abuse.

State Housing Agencies Charged $3 Million in Unnecessary Expenses to the Hardest Hit Fund - August 2017

In an August 2017 audit, SIGTARP uncovered that several state agencies wasted or misused approximately $3 million for large barbeques (including with Treasury employees), parties, seafood lunches, cash bonuses, gifts, avoidable storage costs, backdated costs, employee perks, and rent/operating expenses unrelated to TARP.

Mismanagement of the Hardest Hit Fund in Georgia - October 2017

In an October 2017 audit, SIGTARP found that the Georgia agency mismanaged the HHF, jeopardizing the goals of the program. The mismanagement was subsequently estimated to have wasted $18.6 million.

Risk of Asbestos Exposure, Illegal Dumping, and Contaminated Soil Found in Federal Blight Elimination Program - November 2017

The Army Corps of Engineers issued a report on behalf of SIGTARP warning that the standard protections for demolition programs typically present in demolition grant programs are not present in the HHF program. The Corps identified environmental and safety risks and failures to follow industry best practices that could put residents at risk of exposure to hazardous materials, which include three high-risk areas: 1) proper removal and storage of asbestos and other hazardous material; 2) proper dumping of all debris and waste in appropriate landfills or recycling facilities; and 3) filling in the holes with only clean soil. These high-risk areas threaten HHF's goal of neighborhood stabilization, and carry a high risk of fraud, waste, abuse and environmental crimes

Most of the $9.6 Billion Hardest Hit Fund Has No Federal Competition Requirements for Contract Awards - March 2018

SIGTARP found that most of the $9.6 billion HHF program has no Federal requirements for competition, even though millions of dollars in contracts have been, and will be, awarded. The lack of Federal competition requirements is insufficient protection for fraud, waste, and abuse.

SIGTARP's Recoveries From Audits And Investigtions

SIGTARP continues to assess current and future operations to fulfill its mission and reduce spending, while supporting financial stewardship by providing recoveries to assist in funding the Government at the least cost over time. SIGTARP's investigations and audits have recovered $10 billion - a 35-times return on investment. Fiscal Year 2017 recoveries exceeded the Fiscal Year 2017 appropriated budget and already in Fiscal Year 2018, SIGTARP has recovered $104 million, including more than $90 million paid to the Government. This recovery to the government is almost triple SIGTARP's appropriated budget of $34 million.

Office of Inspector General Department of the Treasury

The Department of the Treasury Office of Inspector General performs independent, objective reviews of specific Treasury programs and operations with oversight responsibility for one federal banking agency – the Office of the Comptroller of the Currency. That federal banking agency supervises approximately 1,350 financial institutions.

Introduction

The Department of the Treasury (Treasury) Office of Inspector General (OIG) was established pursuant to the 1988 amendments to the Inspector General Act of 1978. The Treasury Inspector General is appointed by the President, with the advice and consent of the Senate. Treasury OIG performs independent, objective reviews of Treasury programs and operations, except for those of the Internal Revenue Service (IRS) and the Troubled Asset Relief Program (TARP), and keeps the Secretary of the Treasury and Congress fully informed. Treasury OIG is comprised of four divisions: (1) Office of Audit, (2) Office of Investigations, (3) Office of Counsel, and (4) Office of Management. Treasury OIG is headquartered in Washington, DC, and has an audit office in Boston, Massachusetts, and investigative offices in Greensboro, North Carolina; Houston, Texas; and Jacksonville, Florida.

Treasury OIG has oversight responsibility for the Office of the Comptroller of the Currency (OCC). OCC is responsible for approximately 943 national banks, 353 federal savings associations, and 50 federal branches of foreign banks. The total assets under supervision are $12 trillion, making up 68 percent of the total U.S. commercial banking assets. Treasury OIG also oversees four offices created by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) which are (1) the Office of Financial Research (OFR), (2) the Federal Insurance Office, (3) the Office of Minority and Women Inclusion within Treasury's Departmental Offices (DO), and (4) the Office of Minority and Women Inclusion within OCC. Additionally, Treasury OIG oversees Treasury's role related to the financial solvency of the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Mortgage Corporation (Freddie Mac) under the Housing and Economic Recovery Act of 2008 (HERA), to include Treasury's Senior Preferred Stock Purchase Agreements established for the purpose of maintaining the positive net worth of both entities. As of December 2017, the funding capacity available to the two entities is $254 billion covering future net worth deficiencies.

Treasury Management and Performance Challenges Related to Financial Regulation and Economic Recovery

In accordance with the Reports Consolidation Act of 2000, the Treasury Inspector General annually provides the Secretary of the Treasury with his perspective on the most serious management and performance challenges facing the Department. In a memorandum to the Secretary dated October 16, 2017, the Inspector General reported three management and performance challenges that were directed towards financial regulation and economic recovery. Those challenges are: Operating in an Uncertain Environment, Cyber Threats, and Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement.[10]

Operating in an Uncertain Environment

The proposed budget cuts and new requirements imposed by Executive Order (E.O.) 13781, ***Comprehensive Plan for Reorganizing the Executive Branch*** (March 13, 2017) create an uncertain environment that affect Treasury's operations. In its implementation of E.O. 13781 the Office of Management and Budget (OMB) required agencies to submit Agency Reform Plans to OMB concurrently with their fiscal year 2019 budget requests. These plans were to include proposals in four categories: eliminate activities; restructure or merge; improve organizational efficiency and effectiveness; and workforce management. After consideration of all Agency Reform Plans, OMB intends to work with agencies in developing crosscutting reform proposals that involve multiple agencies, which could include merging agencies, components, programs, or activities that have similar missions.

OMB's Government-wide Reform Plan may significantly impact the administration of Treasury's programs and operations. With looming uncertainties as to the impact of the plan, Treasury must plan for the potential long-term restructuring of certain functions or offices/bureaus and/or budget cuts. This may require Treasury to take immediate actions to achieve near-term cost savings while focusing its limited resources on programs that are in the highest need to citizens and/or where there is a unique Federal role such as in economic recovery.

Cyber Threats

Cybersecurity is a long-standing and serious challenge facing the Nation today. A reliable critical infrastructure, including information systems and networks, is vital to our national security and economic stability. Cyber threats are a persistent concern as Treasury's information systems are critical to the core functions of government and the Nation's financial infrastructure. As cyber threats continue to evolve and become more sophisticated and subtle, they pose an ongoing challenge for Treasury to fortify and safeguard its internal systems and operations and the financial sector it oversees.

Attempted cyber attacks against Federal agencies, including Treasury, and financial institutions are increasing in frequency and severity, and continue to evolve at an accelerated rate. Such attacks include distributed denial of service attacks, phishing or whaling attacks, fraudulent wire payments, malicious spam (malspam), and ransomware. Organized hacking groups leverage published and unpublished vulnerabilities and vary their methods to make attacks hard to detect and even harder to prevent. Criminal groups and nation-states are constantly seeking to steal information; commit fraud; and disrupt, degrade, or deny access to information systems.

Effective public-private coordination continues to be required to address the cyber threat against the Nation's critical infrastructure. In this regard, Treasury is looked upon to provide effective leadership to financial institutions in particular, and the financial sector in general, to strengthen awareness and preparedness against cyber threats.

10 The Treasury Inspector General's memorandum included one other challenge not directly related to financial regulation and economic recovery: Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments. The memorandum also discussed concerns about two matters: currency and coin production and documenting key activities and decisions.

Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement

Identifying, disrupting, and dismantling the financial networks that support terrorists, organized transnational crime, weapons of mass destruction proliferators, and other threats to international security continue to be a challenge. Treasury's Office of Terrorism and Financial Intelligence (TFI) is dedicated to disrupting the ability of terrorist organizations to fund such activities through intelligence analysis, sanctions, and international private-sector cooperation that identify donors, financiers, and facilitators funding terrorist organizations.

TFI's ability to effectively gather and analyze intelligence information on financial crimes and terrorism requires a stable cadre of staff. In the fall of 2017 there were concerns over TFI's ability to meet mission critical objectives due to multiple vacant key positions. Since that time, all but two positions have been filled. Because of TFI's complementary missions in intelligence gathering and coordination with international and domestic intelligence and law enforcement entities, stability and coordination within TFI is imperative to reduce duplication, enhance information gathering and intelligence analysis, and increase efficiency.

The Financial Crimes Enforcement Network (FinCEN) faces continuing challenges to enhance financial transparency and strengthen efforts to combat financial crime and collect, analyze, and report data on national and international threats. FinCEN has focused on enhancing enforcement efforts through compliance with the Bank Secrecy Act (BSA) in partnership with Federal banking regulators and law enforcement. Other areas of concern for FinCEN include the increasing use of (1) mobile devices for banking, internet banking, internet gaming, and peer-to-peer transactions; and (2) money service businesses, including virtual currency administrators and exchanges. FinCEN and other regulatory agencies will need to make sure that providers of these services who are covered by BSA understand their obligations to report information to FinCEN.

Completed and In-Progress Work on Financial Oversight

OFR's Procurement Activities – Government Purchase Cards

We initiated an audit of OFR's procurement activities. We reported that OFR purchase cardholders made split purchases, which is prohibited by the Federal Acquisition Regulation and Treasury's Office of the Procurement Executive *Charge Card Management Plan Purchase Card Program*. In addition, OFR's cardholder files were not in compliance with applicable documentation requirements due to a lack of training and understanding of the requirements. Consequently, the files did not provide a complete history of each transaction showing that informed decisions were made at each step of the process and proper approvals were obtained.

We recommended that OFR (1) work with Treasury DO's Purchase Card Program Coordinator to conduct a one-time purchase cardholder and approver refresher training on split purchase transactions, within 60 days; (2) develop and implement a policy to require OFR Approving Officials to review purchase card transactions for potential split purchases on a monthly basis when approving official duties are transferred to OFR employees in 2018; (3) share the results of our review of OFR's split purchases with its service provider, Treasury's Office of Budget and Travel (OBT); (4) review purchase cardholders' files to ensure that all documents required by policy and procedures are included in the files; (5) develop and implement a policy for storing and maintaining government purchase card transaction documentation in a centralized location; (6) conduct a one-time government purchase card cardholder and approver refresher training, within 60 days, on cardholder file documentation and retention requirements; and (7) share the results of findings related to OFR's documentation of government purchase card transactions with OBT.

Oversight of Servicers' Determination of In-Scope Borrowers Under the Amended Consent Orders

Expressing concern that one servicer under an amended foreclosure consent order failed to identify and send payments to 24,000 borrowers until after a private citizen contacted OCC, the Ranking Member of the House Committee on Financial Services asked the Treasury Inspector General and the Board of Governors of the Federal Reserve System/Consumer Financial Protection Bureau Inspector General to look into the matter. In response, we

initiated an audit to determine: (1) the facts and circumstances surrounding the increase in the population of the one servicer's in-scope borrowers; (2) the methodology used and procedures performed by OCC to test and validate the universe of in-scope borrowers and whether such borrowers were appropriately sent checks for the five servicers not covered in prior Treasury OIG reviews; (3) OCC's process for vetting any individual questions, complaints, or requests for appeal related to the in-scope population from borrowers; (4) any direction that OCC has provided to servicers outlining how the servicer should process questions, complaints, or requests to appeal the determination of the in-scope population that they receive from borrowers; and (5) what data gaps existed within servicers' systems that made it difficult to identify in-scope borrowers and whether such data gaps or system integration issues have been fixed.

We reported that OCC took immediate action to determine the total borrowers omitted from Citibank's in-scope population once the error was discovered and ensured checks were mailed to the affected borrowers in accordance with the Independent Foreclosure Review (IFR) payment agreement. We found that OCC's process for determining the in-scope population of borrowers was reasonable and consistent with the process reviewed in our prior audit of the amended consent orders (OIG-14-044; August 6, 2014). OCC identified system errors during its oversight of this process and directed the respective servicers to take corrective action. We also found that OCC had a borrower complaint process that sought to address borrowers' concerns regarding their in-scope status in a reasonable manner. Further, we found that all servicers reviewed by OCC had identified data gaps and/or system integration issues and took corrective actions to mitigate those issues. We made no recommendations to OCC as a result of our audit.

OCC's Supervision of Federal Branches of Foreign Banks (In Progress)

We initiated an audit of OCC's supervision of federal branches of foreign banks. The objective of this audit is to assess OCC's supervision of federal branches and agencies of foreign banking organizations operating in the United States.

OCC's Supervision of Wells Fargo Bank (In Progress)

We initiated an audit of OCC's supervision of Wells Fargo Bank's sales practices. The objectives of this audit are to assess (1) OCC's supervision of incentive-based compensation structures within Wells Fargo and (2) the timeliness and adequacy of OCC's supervisory and other actions taken related to Wells Fargo sales practices, including the opening of accounts.

OCC's Supervision Related to De-risking by Banks (In Progress)

We initiated an audit of OCC's supervisory impact on the practice of de-risking[11] by banks. The objectives of this audit are to determine (1) whether supervisory, examination, or other staff of the OCC have indirectly or directly caused banks to exit a line of business or to terminate a customer or correspondent account, and (2) under what authority OCC plans to limit, through guidance, the ability of banks to open or close correspondent or customer accounts, including a review of laws that govern account closings and OCC's authority to regulate account closings.

OFR's Procurement Activities – Contracts (In Progress)

We initiated an audit of OFR's procurement activities. The objectives of this audit are to determine if (1) OFR's procurement activities ensure that OFR effectively and efficiently acquires the goods and services needed to accomplish its mission and (2) these acquisitions are made in compliance with applicable procurement regulations.

OFR's Hiring Practices and Response to Federal Employee Viewpoint Survey Results (In Progress)

We initiated an audit of OFR's hiring practices and response to its Federal Employee Viewpoint Survey (FEVS) results. The objectives for this audit are to determine whether (1) OFR's hiring practices are in accordance with Office of Personnel Management, Treasury, OFR, and other Federal requirements; and (2) OFR's process for reviewing and responding to FEVS results are in accordance with Federal requirements including Treasury policies and procedures.

11 The Financial Action Task Force defines de-risking as the termination or restriction, by financial institutions, of business relationships with categories of customers.

Failed Bank Reviews

In 1991, Congress enacted the Federal Deposit Insurance Corporation Improvement Act (FDICIA) amending the Federal Deposit Insurance Act (FDIA). The amendments require that banking regulators take specified supervisory actions when they identify unsafe or unsound practices or conditions. Also added was a requirement that the Inspector General for the primary federal regulator of a failed financial institution conduct a material loss review when the estimated loss to the Deposit Insurance Fund is "material." FDIA, as amended by Dodd-Frank, defines the loss threshold amount to the Deposit Insurance Fund triggering a material loss review as a loss that exceeds $50 million for 2014 and thereafter (with a provision to temporarily raise the threshold to $75 million in certain circumstances). The act also requires a review of all bank failures with losses under these threshold amounts for the purposes of (1) ascertaining the grounds for appointing FDIC as receiver and (2) determining whether any unusual circumstances exist that might warrant a more in-depth review of the loss. As part of the material loss review, OIG auditors determine the causes of the failure and assess the supervision of the institution, including the implementation of the prompt corrective action (PCA) provisions of the act.[12] As appropriate, OIG auditors also make recommendations for preventing any such loss in the future.

From 2007 through May 2018, FDIC and other banking regulators closed 528 banks and federal savings associations. One hundred and forty-two (142) of these were Treasury-regulated financial institutions; in total, the estimated loss to FDIC's Deposit Insurance Fund for these failures was $36.4 billion. Of the 142 failures, 58 resulted in a material loss to the Deposit Insurance Fund, and our office performed the required reviews of these failures.

During the period covered by this annual report, we completed a material loss review of Guaranty Bank (Guaranty) located in Milwaukee, Wisconsin, whose failure in May 2017 resulted in a loss to the Deposit Insurance Fund estimated at $148.6 million. We determined that Guaranty failed primarily because of relaxed loan underwriting standards, poor risk management, and deficient supervision by the board of directors and bank management. Regarding supervision, we found that OCC examiners generally followed guidance in supervising Guaranty Bank; however, that supervision did not prevent a material loss to the Deposit Insurance Fund. We found that OCC did not adequately review (1) Guaranty's request for retention bonuses for PCA compliance prior to providing a determination of no supervisory objection,[13] and (2) the salaries of Guaranty's senior executives and therefore did not detect until 2017 that Guaranty gave yearly salary increases to senior executive officers which were prohibited by PCA. As a result, the bank paid $468,926 in bonuses and salary increases to senior executive officers in violation of PCA. We recommended that the Comptroller of the Currency develop and document examination procedures, for banks subject to PCA restrictions, that are designed to identify and track all types of compensation paid to executive officers as defined in 12 CFR 215 ***Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks,*** also known as Regulation O[14].

We also initiated a material loss review of Washington Federal Bank for Savings, Chicago, Illinois, whose failure in December 2017 resulted in a loss to the Deposit Insurance Fund estimated at $60.5 million.

12 Prompt corrective action is a framework of supervisory actions for insured institutions that are not adequately capitalized. It was intended to ensure that action is taken when an institution becomes financially troubled in order to prevent a failure or minimize the resulting losses. These actions become increasingly severe as the institution falls into lower capital categories. The capital categories are well-capitalized, adequately capitalized, undercapitalized, significantly undercapitalized, and critically undercapitalized.

13 OCC uses the term "no supervisory objection" to convey that they do not find a compelling supervisory or regulatory reason to deny the request. OCC does not consider an NSO an "approval."

14 The Regulation O definition of executive officer includes every vice president, unless that person was formally excluded from the decision-making process by the bank's bylaws or a resolution from the board of directors.