SEMIANNUAL REPORT TO CONGRESS

October 1, 2016–March 31, 2017

Office of Inspector General

Board of Governors of the Federal Reserve System

Consumer Financial Protection Bureau

SEMIANNUAL REPORT TO CONGRESS

October 1, 2016–March 31, 2017

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

Message From the Inspector General

Mark Bialek
Inspector General

For this semiannual period, given new statutory requirements under the Inspector General Empowerment Act of 2016, we are widening the window into our work by summarizing more investigative results and reports with unimplemented recommendations (appendix B and appendix C, respectively). This increased transparency aligns with our dedication to being *the* trusted oversight agency of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB). To be trusted means, in part, showing a clear connection between our work and our mission, vision, and values.

This reporting period, we reviewed financial controls related to the Board's financial statements and the CFPB's purchase and travel card programs, as well as information security controls at the Board and the CFPB. We also recommended actions both agencies could take to improve their processes and culture. How can the Board encourage its staff to share divergent views so it can make more-informed decisions related to financial institution supervision in light of multiple perspectives? How can the CFPB mitigate the risk of conflicts of interest with its vendors, or enhance its administration of advisory committees? What can the Board do to maximize the effectiveness of its monitoring of emerging risks at large financial institutions? These questions cut to the heart of the effectiveness of our agencies' operations, and our answers, with actionable recommendations for improvement, shed light on how operations can improve, for the agencies themselves, and for the public, Congress, and other stakeholders.

This report also describes closed investigations we previously did not make public that involved allegations of misconduct by senior government employees. In addition, our investigators continue to get results for our agencies: Over the past 6 months, we have received 331 Hotline complaints; opened 17 investigations; and seen our work result in 6 persons referred to the U.S. Department of Justice for criminal prosecution; 5 indictments; $8,009,552 in criminal

fines, restitution, and special assessments; and $638,000,000 in civil judgments.

We also unveiled our new strategic plan and are committed to looking inward and being transparent about our major goals:

1. Make a Difference: Deliver results that promote agency excellence.
2. Cultivate Great Teams: Promote a diverse, skilled, and engaged workforce and foster an inclusive, collaborative environment.
3. Build Bridges: Optimize external stakeholder engagement.
4. Work Better: Advance organizational effectiveness and model a culture of continuous improvement.

We believe that our strategic plan encourages our agencies and other stakeholders to hold us accountable as an organization, and it gives us a benchmark by which to hold ourselves accountable as well.

Finally, I thank the OIG staff, who deserve congratulations for the great work they do every day and whose dedication to promoting economy, efficiency, and effectiveness and to rooting out fraud, waste, and abuse is second to none.

Sincerely,

Mark Bialek
Inspector General
April 28, 2017

Contents

Highlights

The Office of Inspector General (OIG) continued to promote the integrity, economy, efficiency, and effectiveness of the programs and operations of the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB). The following are highlights of our work during this semiannual reporting period.

Audits, Evaluations, and Inspections

14 reports issued	**6** Board **8** CFPB
60 recommendations closed	**31** Board **29** CFPB

Willingness to Share Divergent Views About Large Financial Institution Supervision Activities. Employees' willingness to share views varies by Federal Reserve Bank and among supervision teams at the same Reserve Bank. Leadership and management approaches play a major role in influencing employees' comfort level in sharing views.

The CFPB's Contract Award Controls and Processes. The CFPB generally complies with contract award laws, regulations, and agency policies and procedures, but some reviews and approvals were overlooked or not documented as required, and other controls and processes can be improved.

The CFPB's Controls for Identifying and Avoiding Conflicts of Interest Related to Vendor Activities. The CFPB can strengthen its controls for identifying and avoiding potential conflicts of interest associated with using vendors to support fair lending compliance and enforcement analysis. The agency should also evaluate whether to perform more fair lending enforcement analysis internally.

The Board's Use of Continuous Monitoring as a Supervisory Tool. Although the Board and the Reserve Banks have multiple documents that address the expectations for certain aspects of continuous monitoring, the Board has not issued guidance that harmonizes these expectations across its supervisory portfolios and the Reserve Banks.

The Board's Information Security Program. The Board has taken several steps to mature its information security program to ensure that it is consistent with Federal Information Security Modernization Act of 2014 (FISMA) requirements. However, the Board's information security program needs several improvements in the areas of risk management, identity and access management, security and privacy training, and incident response.

The CFPB's Information Security Program. The CFPB has taken several steps to mature its information security program to ensure that it is consistent with FISMA requirements. However, the CFPB's information security program needs several improvements in the areas of risk management, identity and access management, and contingency planning.

Investigations

17
cases opened

21
cases closed

6
matters for prosecutorial consideration

5
indictments

$8,009,552
in criminal fines, restitution, and special assessments

$638,000,000
in civil judgments

Multiple Former Pierce Commercial Bank Officials Indicted for Conspiracy and Bank Fraud. Four former Pierce Commercial Bank officials were indicted in the Western District of Washington in Tacoma for conspiracy to make false statements on loan applications and to commit bank fraud. Along with three other branch employees, the individuals knowingly made false statements overvaluing property on home loan applications. The fraudulent scheme contributed to the failure of the bank, which caused the Deposit Insurance Fund (DIF) about $24.8 million in losses.

Former Employee at the Federal Reserve Board Pleads Guilty to Unlawful Conversion of Government Property. A Communications Analyst pleaded guilty to unlawful conversion of government property, was sentenced to 12 months' probation, and was fined $5,000 for installing unauthorized software on a Board server to connect to a Bitcoin network in order to earn bitcoins.

Introduction

Congress established the OIG as the independent oversight authority for the Board and the CFPB. In fulfilling this responsibility, the OIG conducts audits, evaluations, investigations, and other reviews related to Board and CFPB programs and operations. By law, OIGs are not authorized to perform agency program functions.

In accordance with the Inspector General Act of 1978, as amended, our office has the following responsibilities:

- to conduct and supervise independent and objective audits, evaluations, investigations, and other reviews related to Board and CFPB programs and operations in order to promote economy, efficiency, and effectiveness within the Board and the CFPB
- to help prevent and detect fraud, waste, abuse, and mismanagement in Board and CFPB programs and operations
- to review existing and proposed legislation and regulations in order to make recommendations regarding possible improvements to Board and CFPB programs and operations
- to keep the Board of Governors, the Director of the CFPB, and Congress fully and currently informed

Congress has also mandated additional responsibilities that influence the OIG's priorities, including the following:

- Section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act; 12 U.S.C. § 1831o(k)), requires that the OIG review Board-supervised financial institutions that failed when the failure resulted in a material loss to the DIF and that we report on the failure within 6 months. Section 38(k) also requires that the OIG conduct an in-depth review of any nonmaterial losses to the DIF that exhibit unusual circumstances.
- The Federal Reserve Act, as amended by the USA PATRIOT Act of 2001 (12 U.S.C. § 248(q)), grants the Board certain

federal law enforcement authorities. Our office performs the external oversight function for the Board's law enforcement program.

- The Federal Information Security Modernization Act of 2014 (FISMA; 44 U.S.C. § 3555) established a legislative mandate for ensuring the effectiveness of information security controls over resources that support federal operations and assets. In accordance with FISMA requirements, we perform annual independent reviews of the Board's and the CFPB's information security programs and practices, including the effectiveness of security controls and techniques for selected information systems.
- The Improper Payments Information Act of 2002, as amended (IPIA; 31 U.S.C. § 3321 note), requires agency heads to periodically review and identify programs and activities that may be susceptible to significant improper payments. The CFPB has determined that its Consumer Financial Civil Penalty Fund is subject to IPIA. The Improper Payments Elimination and Recovery Act of 2010 requires our office to determine each fiscal year whether the agency is in compliance with IPIA.
- Section 211(f) of the Dodd-Frank Act (12 U.S.C. § 5391(f)) requires that the OIG review and report on the Board's supervision of any covered financial company that is placed into receivership. The OIG is to evaluate the effectiveness of the Board's supervision, identify any acts or omissions by the Board that contributed to or could have prevented the company's receivership status, and recommend appropriate administrative or legislative action.
- Section 989E of the Dodd-Frank Act (5 U.S.C. app. 3 § 11 note) established the Council of Inspectors General on Financial Oversight (CIGFO), which is required to meet at least quarterly to share information and discuss the ongoing work of each Inspector General (IG), with a focus on concerns that may apply to the broader financial sector and ways to

improve financial oversight.[1] Additionally, CIGFO is required to report annually about the IGs' concerns and recommendations, as well as issues that may apply to the broader financial sector. CIGFO also can convene a working group of its members to evaluate the effectiveness and internal operations of the Financial Stability Oversight Council, which was created by the Dodd-Frank Act and is charged with identifying threats to the nation's financial stability, promoting market discipline, and responding to emerging risks to the stability of the nation's financial system.

- The Government Charge Card Abuse Prevention Act of 2012 (5 U.S.C. § 5701 note and 41 U.S.C. § 1909(d)) requires our office to conduct periodic risk assessments and audits of the CFPB's purchase card, convenience check, and travel card programs to identify and analyze risks of illegal, improper, or erroneous purchases and payments.
- Section 11B of the Federal Reserve Act (12 U.S.C. § 248(b)) mandates annual independent audits of the financial statements of each Federal Reserve Bank and of the Board. The Board performs the accounting function for the Federal Financial Institutions Examination Council (FFIEC), and we oversee the annual financial statement audits of the Board and of the FFIEC.[2] Under the Dodd-Frank Act, the U.S. Government Accountability Office performs the financial statement audit of the CFPB.
- The Digital Accountability and Transparency Act of 2014 (DATA Act; 31 U.S.C. § 6101 note) requires agencies to report

1. CIGFO comprises the IGs of the Board and the CFPB, the Commodity Futures Trading Commission, the U.S. Department of Housing and Urban Development, the U.S. Department of the Treasury, the Federal Deposit Insurance Corporation, the Federal Housing Finance Agency, the National Credit Union Administration, the U.S. Securities and Exchange Commission, and the Office of the Special Inspector General for the Troubled Asset Relief Program.
2. The FFIEC is a formal interagency body empowered (1) to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the CFPB and (2) to make recommendations to promote uniformity in the supervision of financial institutions.

financial and payment data in accordance with data standards established by the U.S. Department of the Treasury (Treasury) and the Office of Management and Budget. The CFPB has determined that its Consumer Financial Civil Penalty Fund is subject to the DATA Act and that only one specific DATA Act requirement, section 3(b), applies to the Bureau Fund. The DATA Act requires our office to review a statistically valid sample of the data submitted by the agency and report on its completeness, timeliness, quality, and accuracy and the agency's implementation and use of the data standards.

Audits, Evaluations, and Inspections

Audits assess aspects of the economy, efficiency, and effectiveness of Board and CFPB programs and operations. For example, the OIG oversees audits of the Board's financial statements and conducts audits of (1) the efficiency and effectiveness of the Board's and the CFPB's processes and internal controls over their programs and operations; (2) the adequacy of controls and security measures governing these agencies' financial and management information systems and their safeguarding of assets and sensitive information; and (3) compliance with applicable laws and regulations related to the agencies' financial, administrative, and program operations. OIG audits are performed in accordance with the *Government Auditing Standards* established by the Comptroller General of the United States.

Inspections and evaluations include program evaluations and legislatively mandated reviews of failed financial institutions supervised by the Board. Inspections are often narrowly focused on particular issues or topics and provide time-critical analyses. Evaluations are generally focused on the effectiveness of specific programs or functions. OIG inspections and evaluations are performed according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

The information below summarizes OIG audit and evaluation work completed during the reporting period.

Board of Governors of the Federal Reserve System

Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities

2016-SR-B-014 **November 14, 2016**

We initiated this evaluation in response to a written request from the Director of the Board's Division of Banking Supervision and Regulation and the Board's General Counsel. Our objectives were (1) to assess the methods for Federal Reserve System decisionmakers to obtain material information necessary to ensure that decisions and conclusions resulting from supervisory activities at Large Institution Supervision Coordinating Committee (LISCC) firms and large banking organizations (LBOs) are appropriate, supported by the record, and consistent with applicable policies and (2) to determine whether there are adequate channels for System decisionmakers to be aware of supervision employees' divergent views about material issues regarding LISCC firms and LBOs.

We found that employees' willingness to share views varies by Reserve Bank and among supervision teams at the same Reserve Bank. We also found that leadership and management approaches play a major role in influencing employees' comfort level in sharing views. We identified five root causes for employees' reticence to share their views; addressing these root causes will likely improve the flow of information to decisionmakers. In addition, we describe several leadership behaviors and processes currently employed by the leadership at certain Reserve Banks that appear particularly effective in helping to convince Reserve Bank supervision employees that it is both safe and worthwhile to share their views.

Our report contains recommendations designed to increase employees' willingness to share their views and improve the flow of information to decisionmakers regarding the supervision of large financial institutions. The Board concurred with our recommendations.

The Board Can Improve Documentation of Office of Foreign Assets Control Examinations

2017-SR-B-003 **March 15, 2017**

We evaluated the Board's supervision activities for foreign banking organizations following high-profile enforcement actions related to Office of Foreign Assets Control (OFAC) violations. From 2010 to 2014, OFAC issued seven civil money penalties totaling almost $1.7 billion and the Board issued four civil money penalties totaling $788 million related to U.S. sanctions programs. Our objective was to assess the Board's approach to evaluating foreign banking organizations' OFAC compliance programs.

The OFAC examinations we reviewed did not always include documentation to adequately explain the rationale for the examination approach or the basis for conclusions. Although the *Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations* includes guidance on what to include in examination workpapers and the *Bank Secrecy Act/Anti-Money Laundering Examination Manual* includes OFAC examination procedures, there are no guidance or minimum expectations specific to how OFAC examinations should be documented. We also found data reliability concerns in the National Examination Database regarding whether OFAC compliance had been reviewed. These data reliability concerns may have occurred because there is no established definition of what it means to review OFAC compliance and because Reserve Banks do not have consistent data entry procedures. In addition, the National Examination Database does not capture data that would indicate the extent of coverage of OFAC examinations.

Our report contains recommendations designed to strengthen the Board's supervision of OFAC compliance. The Board concurred with our recommendations.

The Board Can Improve the Effectiveness of Continuous Monitoring as a Supervisory Tool

2017-SR-B-005 **March 29, 2017**

We assessed the effectiveness of continuous monitoring as a supervisory activity for large, complex financial institutions, including LISCC firms and LBOs.

Although the Board and the Reserve Banks have multiple documents that address the expectations for certain aspects of continuous monitoring, the Board has not issued guidance that harmonizes these expectations across its supervisory portfolios and the Reserve Banks. Such guidance could outline the preferred analytical approach and documentation practices for this activity across the LISCC and LBO supervisory portfolios and minimize the variability that we noted for continuous monitoring activities across the Reserve Banks we visited. Although we noted certain best practices for executing continuous monitoring during our evaluation, those practices have not been broadly implemented across the Federal Reserve System. As a result, supervisory guidance issued by the Board could help to foster more consistent execution of this supervisory activity throughout the Federal Reserve System and maximize its effectiveness.

Our report contains recommendations to improve the effectiveness of continuous monitoring. The Board concurred with our recommendations.

2016 Audit of the Board's Information Security Program

2016-IT-B-013 **November 10, 2016**

FISMA requires IGs to conduct an annual, independent evaluation of their respective agencies' information security programs and practices. In support of FISMA independent evaluation requirements, the U.S. Department of Homeland Security (DHS) issued guidance to IGs on FISMA reporting for 2016. The guidance directs IGs to evaluate the performance of agencies' information security programs across eight areas. The guidance also references a five-level maturity model for IGs to use in assessing agencies' information security continuous monitoring and incident response programs. In accordance with these requirements, we reviewed the Board's information security program. Specifically, we evaluated the effectiveness of the Board's (1) security controls and techniques and (2) information security policies, procedures, and practices.

We found that the Board has taken several steps to mature its information security program to ensure that the program is consistent with FISMA requirements. For instance, we found that the Board has implemented an enterprisewide information security continuous monitoring lessons-learned process as well as

strengthened its system-level vulnerability management practices. However, we identified several improvements needed in the Board's information security program in the areas of risk management, identity and access management, security and privacy training, and incident response. Specifically, we found that the Board can strengthen its risk management program by ensuring that Board divisions are consistently implementing the organization's risk management processes related to security controls assessment, security planning, and authorization. In addition, we continued to find instances of Board sensitive information that was not appropriately restricted within the organization's enterprisewide collaboration tool. We also noted that the Board had not evaluated the effectiveness of its security and privacy awareness training program in 2016. Finally, we found that the Board can strengthen its incident response capabilities by transitioning to a Trusted Internet Connections network provider and utilizing services offered through DHS's EINSTEIN program for intrusion detection and prevention.

Our report includes recommendations to strengthen the Board's information security program in the areas of risk management, identity and access management, security and privacy training, and incident response. The Board concurred with our recommendations.

Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2016 and 2015, and Independent Auditors' Reports

2017-FMIC-B-002 **March 7, 2017**

We contracted with an independent public accounting firm to audit the financial statements of the Board and to audit the Board's internal control over financial reporting. The contract requires the audits of the financial statements to be performed in accordance with the auditing standards generally accepted in the United States of America, the standards applicable to financial audits in the *Government Auditing Standards* issued by the Comptroller General of the United States, and the auditing standards of the Public Company Accounting Oversight Board. The contract also requires the audit of internal control over financial reporting to be performed in accordance with the attestation standards established by the

American Institute of Certified Public Accountants and with the auditing standards of the Public Company Accounting Oversight Board. We reviewed and monitored the work of the independent public accounting firm to ensure compliance with applicable standards and the contract.

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the Board as of December 31, 2016 and 2015, and the results of its operations and its cash flows for the years then ended in conformity with accounting principles generally accepted in the United States of America. Also, in the auditors' opinion, the Board maintained, in all material respects, effective internal control over financial reporting as of December 31, 2016, based on the criteria established in *Internal Control—Integrated Framework* (2013) by the Committee of Sponsoring Organizations of the Treadway Commission. The auditors' report on compliance and other matters disclosed no instances of noncompliance or other matters.

Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2016 and 2015, and Independent Auditors' Reports

2017-FMIC-B-001 **March 1, 2017**

The Board performs the accounting function for the FFIEC, and we contract with an independent public accounting firm to annually audit the financial statements of the FFIEC. The contract requires the audits to be performed in accordance with auditing standards generally accepted in the United States of America and in accordance with the auditing standards applicable to financial audits in the *Government Auditing Standards* issued by the Comptroller General of the United States. We reviewed and monitored the work of the independent public accounting firm to ensure compliance with applicable standards and the contract.

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the FFIEC as of December 31, 2016 and 2015, and the results of operations and cash flows for the years then ended in conformity with accounting principles generally accepted in the United States of America. The auditors' report on internal control over financial reporting

and on compliance and other matters disclosed no instances of noncompliance or other matters.

Consumer Financial Protection Bureau

The CFPB Can Strengthen Contract Award Controls and Administrative Processes

2017-FMIC-C-007 **March 30, 2017**

We assessed the CFPB's compliance with the *Federal Acquisition Regulation* and CFPB policy related to the contract solicitation, selection, and award processes, as well as the effectiveness of the CFPB's associated internal controls. This audit was a follow-on to our 2015 audit of the CFPB's contract management processes.[3]

We found the CFPB to be generally compliant with applicable laws, regulations, and CFPB policies and procedures related to contract preaward and award process controls. We noted, however, that on some occasions, reviews and approvals were overlooked or not documented as required by the *Federal Acquisition Regulation* or CFPB policy. The Procurement Office can improve its contract file documentation by consistently including evidence that acquisition planning documents have been reviewed and approved and that conflict of interest documents for evaluation team members were signed. The CFPB can also improve the documentation used to support price reasonableness determinations for sole-source contracts and improve Routing and Review Slip documentation. We also found that there were opportunities to expand the use of digital signatures in the acquisition process. Lastly, the Procurement Office can capture and monitor acquisition lead-time data as a performance measure and better inform program offices by enhancing communications and training.

Our report contains recommendations designed to strengthen the CFPB's internal control environment during acquisition planning, improve contract file documentation, and better use performance goals and communicate with program offices during the acquisition process. The CFPB concurred with our recommendations.

3. Office of Inspector General, *The CFPB Can Enhance Its Contract Management Processes and Related Controls*, OIG Report 2015-FMIC-C-014, September 2, 2015.

The CFPB Can Strengthen Its Controls for Identifying and Avoiding Conflicts of Interest Related to Vendor Activities

2017-SR-C-004 **March 15, 2017**

We assessed whether the CFPB effectively mitigates the risk of potential conflicts of interest associated with using vendors to support fair lending compliance and enforcement analysis. We focused on a contract for fair lending enforcement analysis and expert witness services. Our scope did not include identifying potential or actual conflicts of interest related to the CFPB's fair lending supervision contracts, and our findings are not reflective of all CFPB contracting practices.

We found that the CFPB can strengthen its controls for identifying and avoiding potential conflicts of interest by (1) ensuring that vendors comply with existing documentation requirements; (2) clarifying roles and responsibilities; and (3) better facilitating vendor disclosure of potential conflicts, or affirmation that no conflicts exist, at the issuance of each task order. In addition, although the CFPB currently performs some fair lending enforcement analysis internally, we found that the CFPB should evaluate the potential costs and benefits of performing more fair lending enforcement analysis internally.

Our report contains recommendations designed to strengthen the CFPB's identification and avoidance of potential conflicts of interest and to reduce the agency's exposure to operational and reputational risk. The CFPB concurred with our recommendations.

2016 Audit of the CFPB's Information Security Program

2016-IT-C-012 **November 10, 2016**

FISMA requires IGs to conduct an annual, independent evaluation of their respective agencies' information security programs and practices. In support of FISMA independent evaluation requirements, DHS issued guidance to IGs on FISMA reporting for 2016. The guidance directs IGs to evaluate the performance of agencies' information security programs across eight areas. The guidance also references a five-level maturity model for IGs to use in assessing agencies' information security continuous monitoring and incident response programs. Consistent with

these requirements, we reviewed the CFPB's information security program. Our audit objectives were to evaluate the effectiveness of the CFPB's (1) security controls and techniques and (2) information security policies, procedures, and practices.

We found that the CFPB has taken several steps to mature its information security program to ensure that it is consistent with FISMA requirements. For instance, we found that both the CFPB's information security continuous monitoring and incident response programs were operating at an overall maturity of level 3 (*consistently implemented*), primarily due to enhancements in the agency's automation capabilities. However, we identified several improvements needed in the CFPB's information security program in the areas of risk management, identity and access management, and contingency planning. Specifically, we noted that the CFPB can strengthen its risk management program by formalizing its insider threat activities and evaluating options to develop an agencywide insider threat program that leverages planned activities around data loss prevention. Related to the management of insider threat risks, signed rules of behavior documents were not in place for several privileged users who were not consistently resubmitting user access forms to validate the need for their elevated access privileges. We also noted that the CFPB has not completed an agencywide business impact analysis to guide its contingency planning activities, nor has it fully updated its continuity of operations plan to reflect the transition of its information technology infrastructure from Treasury.

Our report includes recommendations to strengthen the CFPB's information security program in the areas of insider threat activities, privileged users, and contingency planning activities. The CFPB concurred with our recommendations.

The CFPB's Advisory Committees Help Inform Agency Activities, but Advisory Committees' Administration Should Be Enhanced

2016-MO-C-016 **November 30, 2016**

We conducted an audit of the CFPB's activities related to its four advisory committees, which provide expert advice on specific issues related to the CFPB's mission. Our objectives were (1) to assess the CFPB's compliance with applicable laws and regulations

as they relate to advisory committees, (2) to assess the CFPB's administration of the advisory committees, and (3) to evaluate the CFPB's advisory committees' effectiveness in informing the CFPB's activities.

Overall, we found that the CFPB advisory committees were generally effective and were operating in compliance with applicable laws and regulations for the period we reviewed. We also found that the CFPB should improve its administration of advisory committee activities. Specifically, the Office of Advisory Board and Councils and the Office of Research can improve their administrative processes by formally tracking the clearance process of documents before dissemination to advisory committee members, determining an optimal method to identify conflict of interests for certain members, retaining application materials, posting summaries of advisory committee meetings to the CFPB's Advisory groups webpage, and centrally retaining advisory committee expenditure information. In addition, we found that assessing advisory committee effectiveness can assist the CFPB in determining whether the committees provide the agency with information and perspectives that help inform agency activities.

Our report contains recommendations designed to improve the CFPB's administrative processes and to establish the formal monitoring of the effectiveness of advisory committee activities. The CFPB concurred with our recommendations.

Evaluation of the CFPB's Implementation of the Digital Accountability and Transparency Act of 2014

2016-FMIC-C-015 **November 30, 2016**

The DATA Act aims to help policymakers and taxpayers track federal spending by requiring agencies to make accessible consistent data on expenditures and contract information. The CFPB determined that the act applies in full to its Consumer Financial Civil Penalty Fund and in part to its Bureau Fund. Our audit objective was to gain an understanding of the processes, systems, and controls that the CFPB has implemented, or plans to implement, to report financial and spending data as required by the DATA Act.

The DATA Act requires IGs to issue a report to Congress assessing a statistical sample of spending data submitted by the agency and its implementation of the data standards. However, CIGIE identified a timing anomaly for this requirement. The DATA Act states that the first IG report is due to Congress in November 2016; however, the act did not require federal agencies to report spending data until May 2017. As a result, CIGIE encouraged IGs to undertake DATA Act readiness reviews of their respective agencies well in advance of the November 2017 report. Our report is in response to CIGIE's suggestion.

Overall, we identified activities that will help the CFPB successfully implement the DATA Act requirements. We believe that the CFPB's success in implementing the DATA Act requirements will depend in part on (1) the effective execution of its implementation efforts; (2) the finalized designation of a senior accountable official; and (3) the clear documentation of the roles and responsibilities of the Bureau of the Fiscal Service, Administrative Resource Center. Our report contains no recommendations.

The CFPB's Civil Penalty Fund Is in Compliance With the Improper Payments Information Act of 2002, as Amended

2017-FMIC-C-006 **March 29, 2017**

We assessed whether the CFPB is in compliance with IPIA, which requires agency heads to periodically review and identify all programs and activities that may be susceptible to significant improper payments. The CFPB determined that its Consumer Financial Civil Penalty Fund is subject to IPIA. The Consumer Financial Civil Penalty Fund contains money that the CFPB collects from judicial and administrative actions against people or companies that violate federal consumer financial law. Funds may be used to pay victims or for consumer education, financial literacy programs, and program administration costs. For fiscal year 2016, total disbursements from the Consumer Financial Civil Penalty Fund were approximately $54 million.

We determined that the CFPB complied with the two applicable requirements of IPIA for fiscal year 2016 as they relate to the Consumer Financial Civil Penalty Fund. We made no recommendations in our report.

Fiscal Year 2016 Risk Assessment of the CFPB's Purchase Card Program

February 1, 2017

As required by the Government Charge Card Abuse Prevention Act of 2012, we conducted a risk assessment of the CFPB's purchase card program to determine the frequency and scope of future audits. The results of the risk assessment show that the risk of illegal, improper, or erroneous use in the CFPB's purchase card program is *low*. As a result, we will not include an audit of the CFPB's purchase card program in the OIG's 2017 annual audit plan.

Fiscal Year 2016 Risk Assessment of the CFPB's Travel Card Program

February 1, 2017

As required by the Government Charge Card Abuse Prevention Act of 2012, we conducted a risk assessment of the CFPB's travel card program to determine the frequency and scope of future audits. The results of the risk assessment show that the risk of illegal, improper, or erroneous use in the CFPB's travel card program is *medium*.

Although a risk level of *medium* means that the risk is likely to occur, such risk would be expected to have a limited impact on current operations and long-term objectives. In addition, we completed an audit of the travel card program in June 2016. As a result, we will not include an audit of the travel card program in the OIG's 2017 annual audit plan.

Failed State Member Bank Reviews

Material Loss Reviews

Section 38(k) of the Federal Deposit Insurance Act, as amended, requires that the IG of the appropriate federal banking agency complete a review of the agency's supervision of a failed institution and issue a report within 6 months of notification from the Federal Deposit Insurance Corporation (FDIC) OIG that the projected loss to the DIF is material. Under section 38(k), a material loss to the DIF is defined as an estimated loss in excess of $50 million.

The material loss review provisions of section 38(k) require that the IG do the following:

- review the institution's supervision, including the agency's implementation of prompt corrective action
- ascertain why the institution's problems resulted in a material loss to the DIF
- make recommendations for preventing any such loss in the future

No state member bank failures occurred during the reporting period that required us to initiate a material loss review.

Nonmaterial Loss Reviews

The Federal Deposit Insurance Act, as amended, requires the IG of the appropriate federal banking agency to semiannually report certain information on financial institutions that incurred nonmaterial losses to the DIF and that failed during the respective 6-month period.

When bank failures result in nonmaterial losses to the DIF, the IG is required to determine (1) the grounds identified by the federal

banking agency or the state bank supervisor for appointing the FDIC as receiver and (2) whether the losses to the DIF present unusual circumstances that would warrant in-depth reviews. Generally, the in-depth review process is the same as that for material loss reviews, but in-depth reviews are not subject to the 6-month reporting deadline.

The IG must semiannually report the completion dates for each such review. If an in-depth review is not warranted, the IG is required to explain this determination. In general, we consider a loss to the DIF to present unusual circumstances if the conditions associated with the bank's deterioration, ultimate closure, and supervision were not addressed in any of our prior bank failure reports, or if there was potential fraud.

We completed our initial review of the Allied Bank failure and identified a series of unusual circumstances that warrant an in-depth review (table 1). We initiated our in-depth review in February 2017 and will summarize the results of that review in an upcoming semiannual report to Congress.

Table 1: Nonmaterial State Member Bank Failure During the Reporting Period[a]

State member bank	Location	Asset size (millions)	DIF projected loss (millions)	Closure date	OIG summary of state's grounds for receivership	OIG determination
Allied Bank	Mulberry, Arkansas	$66.3	$6.9	09/23/2016	Unsafe and unsound condition	Circumstances warrant an in-depth review, which commenced on 02/09/2017

a. Allied Bank failed on September 23, 2016, a week before the close of the prior semiannual reporting period. Given the timing of the failure, we had not been advised of the estimated loss to the DIF associated with the failure before the close of the prior semiannual reporting period. We made our determination to conduct an in-depth review of this failure during this reporting period.

Investigations

The OIG's Office of Investigations conducts investigations of criminal, civil, and administrative wrongdoing by Board and CFPB employees, as well as investigations of alleged misconduct or criminal activity that affects the Board's or the CFPB's ability to effectively supervise and regulate the financial community. The OIG operates under statutory law enforcement authority granted by the U.S. Attorney General, which vests our Special Agents with the authority to carry firearms, to seek and execute search and arrest warrants, and to make arrests without a warrant in certain circumstances. OIG investigations are conducted in compliance with CIGIE's *Quality Standards for Investigations* and the *Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority*.

During this period, the Office of Investigations met with other financial OIGs to discuss matters of mutual interest, joint investigative operations, joint training opportunities, and hotline operations. The office also met with officials at both the Board and the CFPB to discuss investigative operations and the investigative process.

Board of Governors of the Federal Reserve System

The Board is responsible for consolidated supervision of bank holding companies, including financial holding companies formed under the Gramm-Leach-Bliley Act. The Board also supervises state-chartered banks that are members of the Federal Reserve System. Under delegated authority from the Board, the Reserve Banks supervise bank holding companies and state member banks, and the Board's Division of Supervision and Regulation oversees the Reserve Banks' supervisory activities.

Our office's investigations concerning bank holding companies and state member banks typically involve allegations that holding company directors or officers falsified financial records, lied to or misled examiners, or obstructed examinations in a manner that

may have hindered the Board's ability to carry out its supervisory operations. Such activity may result in criminal violations, including false statements or obstruction of bank examinations. The following are examples from this reporting period of investigations into matters affecting the Board's ability to carry out its supervisory responsibilities.

Former Federal Reserve Board Employee Sentenced for Installing Unauthorized Software on a Board Server

A former Board employee was sentenced to 12 months' probation and fined $5,000 for installing unauthorized software on a Board server. The defendant pleaded guilty to one misdemeanor count of unlawful conversion of government property.

The defendant, a Communications Analyst, inappropriately used his access to a Board server to install unauthorized software to earn bitcoins. Bitcoins are earned as compensation when users allow their systems' computing power to be part of the structure that processes, verifies, and records bitcoin transactions. Due to the anonymity of the Bitcoin network, the Board-CFPB OIG was unable to conclusively determine the amount of bitcoins earned through the Board's server. The defendant also modified security safeguards to remotely access the server. When confronted by OIG agents, the defendant initially denied any knowledge of the wrongdoing but later remotely deleted the Bitcoin software in an effort to conceal his actions. Forensic analysis conducted by Board-CFPB OIG agents and the Federal Reserve System's National Incident Response Team confirmed the defendant's involvement, which resulted in his termination from the Board and ultimately led to his voluntary admission of guilt. The defendant's actions did not result in a loss of Board information, and the Board implemented security enhancements as a result of this incident.

The case was investigated by the Board-CFPB OIG and prosecuted by the U.S. Department of Justice's (DOJ) Computer Crime and Intellectual Property Section.

Former NOVA Bank Officers Sentenced for Conspiracy, False Statements, and Troubled Asset Relief Program Fraud

The former President of NOVA Bank was sentenced to 14 months in prison and was ordered to pay a $50,000 fine, and the former NOVA Bank Board Chairman was sentenced to 11 months in prison and was ordered to pay a $100,000 fine. Both individuals were involved in a fraud conspiracy to obtain $13.5 million in public Troubled Asset Relief Program funds for NOVA Bank. NOVA Bank's holding company, NOVA Financial Holdings, Inc., of Berwyn, Pennsylvania, is supervised and regulated by the Board.

This case was the result of a joint investigation by the Board-CFPB OIG, the FDIC OIG, the Federal Bureau of Investigation (FBI), the Special Inspector General for the Troubled Asset Relief Program (SIGTARP), Internal Revenue Service (IRS)–Criminal Investigation, and the U.S. Attorney's Office for the Eastern District of Pennsylvania.

Former Bank Senior Executive Vice President Sentenced for Failing to Report a Crime

A former One Bank & Trust Senior Executive Vice President was sentenced to 2 years of probation and 100 hours of community service for failing to report a crime. The defendant was also a Director at One Financial Corporation, which is the Board-supervised bank holding company for One Bank & Trust. The former bank executive pleaded guilty to misprision of a felony.

The defendant recommended approval of a $1.5 million line of credit for someone the defendant knew and arranged for the line of credit to be approved without going through the formal approval process. When the line of credit defaulted, the defendant and other former One Bank & Trust executives made false bank entries to hide the default from federal bank regulators. This default was then left off One Bank & Trust's Call Reports to prevent any additional regulatory scrutiny while the bank was soliciting over $10 million in Troubled Asset Relief Program funds. The borrower who defaulted was sentenced to a year and a day in federal prison after pleading guilty to money laundering.

This case was the result of a joint investigation by the Board-CFPB OIG, the FDIC OIG, IRS–Criminal Investigation, the FBI, SIGTARP, and the U.S. Attorney's Office for the Eastern District of Arkansas.

Former President and Chief Executive Officer of Farmers Exchange Bank Charged in Second Superseding Indictment

A former President and Chief Executive Officer of Farmers Exchange Bank was charged in a second superseding indictment with one or more counts of bank fraud; theft, embezzlement, or misapplication by a bank employee; false bank entries, reports, and transactions; false statements; wire fraud; and money laundering. This second superseding indictment amended some of the charges previously filed against the defendant and added additional charges, resulting in a 45-count indictment.

The defendant made false entries in the bank's books, reports, and statements with the intent to injure and defraud the bank and to deceive the agents and examiners appointed to examine the affairs of the bank, including the Board and the FDIC. Additionally, the indictment alleged that the defendant devised a scheme to defraud other FEB Bancshares, Inc., shareholders to obtain money by false and fraudulent pretenses and caused about $4.9 million to be transferred in interstate commerce through the Fedwire Transfer System in Dallas, Texas.

This is a joint investigation by the FDIC OIG, the Board-CFPB OIG, and the FBI, with prosecutorial support from the U.S. Attorney's Office for the Eastern District of Wisconsin.

Former Executive at Union Bank and Trust Company Pleaded Guilty to Theft of Bank Property

A former Assistant Vice President at Union Bank and Trust Company pleaded guilty to one count of theft of bank property. For about 12 years—from around 2000 to 2012—the defendant knowingly took about $200,000 from Union Bank and Trust in Evansville, Wisconsin, and used her position to cover up the theft. The Board-CFPB OIG investigated this matter to determine

whether any misrepresentations were made in an effort to obstruct the Board's supervision program.

This is a joint investigation by the Board-CFPB OIG and the FDIC OIG, with prosecutorial support from the U.S. Attorney's Office for the Western District of Wisconsin.

Multiple Former Pierce Commercial Bank Officials Indicted for Conspiracy and Bank Fraud

Multiple former Pierce Commercial Bank officials were indicted in the Western District of Washington in Tacoma for conspiracy to make false statements on loan applications and to commit bank fraud. Prior to the indictment, one individual—a Vice President and Loan Officer—entered into a plea agreement with the U.S. Attorney's Office in Tacoma. Two other subjects—a second Vice President and Loan Officer and another Loan Officer—pleaded guilty in federal court to bank fraud.

From around July 2004 to July 2008, the coconspirators and others working at Pierce Commercial Bank solicited individuals, whether or not they were qualified, to apply for Pierce Commercial Bank home loans. The coconspirators then had uniform residential loan applications prepared based upon fraudulent representations with and without the borrowers' knowledge. The fraudulent scheme resulted in over 5,000 mortgage loans, representing over $1 billion in loan proceeds. Until it failed, Pierce Commercial Bank was regulated by the Board. The scheme contributed to the failure of the bank. Hundreds of the borrowers involved in the scheme defaulted on their loans, causing over $9.5 million in losses to Pierce Commercial Bank, secondary investors, the U.S. Department of Housing and Urban Development (HUD), and the U.S. Federal Housing Administration and $24.8 million in losses to the DIF.

This case is being prosecuted by the U.S. Attorney's Office for the Western District of Washington, with the investigative assistance of the FBI, the HUD OIG, the Federal Housing Finance Agency (FHFA) OIG, the Board-CFPB OIG, the FDIC OIG, SIGTARP, and IRS–Criminal Investigation.

Consumer Financial Protection Bureau

Title X of the Dodd-Frank Act created the CFPB to implement and enforce federal consumer financial law. The CFPB's five statutory objectives are (1) to provide consumers with critical information about financial transactions, (2) to protect consumers from unfair practices, (3) to identify and address outdated and unduly burdensome regulations, (4) to foster transparency and efficiency in consumer financial product and service markets and to facilitate access and innovation, and (5) to enforce federal consumer financial law without regard to the status of the person to promote fair competition.

The CFPB supervises large banks, thrifts, and credit unions with total assets of more than $10 billion and certain nonbank entities, regardless of size, including mortgage brokers, loan modification providers, payday lenders, consumer reporting agencies, debt collectors, and private education lenders. Additionally, with certain exceptions, the CFPB's enforcement jurisdiction generally extends to individuals or entities that are or have engaged in conduct that violates federal consumer financial law.

Our office's investigations concerning the CFPB's responsibilities typically involve allegations that company directors or officers provided falsified business data and financial records to the CFPB, lied to or misled examiners, or obstructed examinations in a manner that may have affected the CFPB's ability to carry out its supervisory responsibilities. Such activity may result in criminal violations, such as false statements or obstruction of examinations. The following is an example from this reporting period of an investigation into matters affecting the CFPB's ability to carry out its supervisory responsibilities.

Former Principal of Loan Modification Company Pleaded Guilty

An information and plea agreement were filed on one of the former principals of a loan modification company in the U.S. District of Utah for the individual's involvement in a fraudulent telemarketing sales and loan modification conspiracy. This information and plea agreement follow a 40-count federal indictment in the U.S. District of Utah in Salt Lake City charging six individuals with conspiracy,

mail fraud, wire fraud, telemarketing fraud, conspiracy to commit money laundering, and money laundering in an alleged scheme to market and sell home loan modification services under the guise of a law firm.

Around September 2011, the principal and others made false and misleading statements to potential customers in order to convince them to pay for loan modification services. Potential clients were led to believe they were contracting with a true law firm, that an attorney would be working with them individually, and that the attorney would negotiate a loan modification with their lender. Instead, clients were contacted by the defendant and minimum wage employees who were not supervised by lawyers and did not have the legal background or knowledge in working loan modifications.

This case was investigated by the Board-CFPB OIG, the FBI, IRS–Criminal Investigation, SIGTARP, and the FHFA OIG, with prosecutorial support from the U.S. Attorney's Office for the District of Utah.

Hotline

The OIG Hotline helps people report fraud, waste, abuse, or mismanagement related to the programs or operations of the Board and the CFPB. Hotline staff can be reached by phone, email, web form, fax, or mail. The OIG reviews all incoming Hotline communications, researches and analyzes the issues raised, and determines how best to address the complaints. During this reporting period, the Hotline received 331 complaints.

The OIG Hotline continued to receive complaints from individuals seeking information about or wanting to file noncriminal consumer complaints regarding consumer financial products and services. In these matters, Hotline staff members typically refer complainants to the consumer group of the appropriate federal regulator for the institution involved, such as the Office of the Comptroller of the Currency's (OCC) Customer Assistance Group or the CFPB Consumer Response team.

The OIG Hotline continued to receive a significant number of complaints involving suspicious solicitations invoking the name of the Federal Reserve or the Chair of the Board of Governors. Hotline staff members continue to advise all individuals that these phishing emails are solicitations that attempt to obtain the personal or financial information of the recipient and that neither the Board nor the Reserve Banks endorse or have any involvement in them. As appropriate, the OIG may investigate these complaints.

Legislative and Regulatory Review, Congressional and Media Activities, and CIGIE Participation

21
legislative items reviewed

4
regulatory items reviewed

16
responses to congressional members and staff

7
responses to media inquiries

Legislative and Regulatory Review

The Legal Services program serves as the independent legal counsel to the IG and OIG staff. Legal Services provides comprehensive legal advice, research, counseling, analysis, and representation in support of OIG audits, investigations, inspections, and evaluations as well as other professional, management, and administrative functions. Legal Services also keeps the IG and OIG staff aware of recent legal developments that may affect the OIG, the Board, and the CFPB.

In accordance with section 4(a)(2) of the Inspector General Act of 1978, as amended, Legal Services independently reviews newly enacted and proposed legislation and regulations to determine their potential effect on the economy and efficiency of the Board's and the CFPB's programs and operations. During this reporting period, Legal Services reviewed 21 legislative items and 4 regulatory items.

Congressional and Media Activities

The OIG communicates and coordinates with various congressional committees on issues of mutual interest. During this reporting period, we provided 16 responses to congressional members and staff concerning the Board and the CFPB. Additionally, we responded to 7 media inquiries.

CIGIE Participation

The IG is a member of CIGIE, which provides a forum for IGs from various government agencies to discuss governmentwide issues and shared concerns. Collectively, CIGIE's members work to improve government programs and operations. The IG also serves as a member of CIGIE's Legislation Committee and Investigations Committee. The Legislation Committee is the central point of information for legislative initiatives and congressional activities that may affect the community, such as proposed cybersecurity legislation that was reviewed during the reporting period. The Investigations Committee advises the IG community on issues involving criminal investigations, criminal investigations personnel, and criminal investigative guidelines.

The Assistant Inspector General for Information Technology, as the Chair of the Information Technology Committee of the Federal Audit Executive Council, works with information technology audit staff throughout the IG community and reports to the CIGIE Information Technology Committee on common information technology audit issues. The Associate Inspector General for Legal Services and the Legal Services staff attorneys are members of the Council of Counsels to the Inspector General.

Peer Reviews

Government auditing and investigative standards require that our audit and investigative units be reviewed by a peer OIG organization every 3 years. Section 989C of the Dodd-Frank Act amended the Inspector General Act of 1978 to require that OIGs provide in their semiannual reports to Congress information about (1) peer reviews of their respective organizations and (2) their peer reviews of other OIGs. The following information addresses these Dodd-Frank Act requirements.

- In September 2014, the Tennessee Valley Authority OIG completed the latest peer review of our audit organization. We received a peer review rating of *pass*. There were no report recommendations, and we had no pending recommendations from previous peer reviews of our audit organization.
- In April 2016, the Special Inspector General for Afghanistan Reconstruction completed the latest peer review of our Office of Investigations and rated us as compliant. There were no report recommendations, and we had no pending recommendations from previous peer reviews of our investigations organization.

See our website for peer review reports of our organization.

Appendix A: Statistical Tables

Table A-1: Audit, Inspection, and Evaluation Reports Issued to the Board During the Reporting Period

Report title	Type of report
2016 Audit of the Board's Information Security Program	Audit
Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities	Evaluation
Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2016 and 2015, and Independent Auditors' Reports	Audit
Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2016 and 2015, and Independent Auditors' Reports	Audit
The Board Can Improve Documentation of Office of Foreign Assets Control Examinations	Evaluation
The Board Can Improve the Effectiveness of Continuous Monitoring as a Supervisory Tool	Evaluation

Total number of audit reports: 3
Total number of evaluation reports: 3

Table A-2: OIG Reports to the Board With Recommendations That Were Open During the Reporting Period[a]

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
Response to a Congressional Request Regarding the Economic Analysis Associated with Specified Rulemakings	06/11	2	2	–	03/17	–	2
Evaluation of Prompt Regulatory Action Implementation	09/11	1[b]	1	–	03/17	–	1
Security Control Review of the National Remote Access Services System (nonpublic report)	03/12	8	8	–	09/16	7	1
Security Control Review of the Board's Public Website (nonpublic report)	04/12	12	12	–	05/16	9	3
Security Control Review of the Aon Hewitt Employee Benefits System (nonpublic report)	09/12	8	8	–	01/17	8	–
Board Should Enhance Compliance with Small Entity Compliance Guide Requirements Contained in the Small Business Regulatory Enforcement Fairness Act of 1996	07/13	2	2	–	03/17	–	2
Security Control Review of a Third-party Commercial Data Exchange Service Used by the Board's Division of Banking Supervision and Regulation (nonpublic report)	08/13	11	11	–	02/17	11	–
The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control	09/13	1	1	–	02/17	–	1
Opportunities Exist to Achieve Operational Efficiencies in the Board's Management of Information Technology Services	02/14	2	2	–	03/17	2	–

See notes at end of table.

Table A-2: OIG Reports to the Board With Recommendations That Were Open During the Reporting Period[a] (continued)

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
Opportunities Exist for the Board to Improve Recordkeeping, Cost Estimation, and Cost Management Processes for the Martin Building Construction and Renovation Project	03/14	6	6	–	03/17	6	–
Enforcement Actions and Professional Liability Claims Against Institution-Affiliated Parties and Individuals Associated with Failed Institutions	07/14	3[b]	3	–	03/17	1	2
Opportunities Exist to Enhance the Board's Oversight of Future Complex Enforcement Actions	09/14	5	5	–	02/17	3	2
The Board Should Enhance Its Supervisory Processes as a Result of Lessons Learned From the Federal Reserve's Supervision of JPMorgan Chase & Company's Chief Investment Office	10/14	10	10	–	03/17	10	–
The Board Can Better Coordinate Its Contingency Planning and Continuity of Operations Program	10/14	4	4	–	03/17	4	–
Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle	12/14	3	3	–	03/17	2	1
Review of the Failure of Waccamaw Bank	03/15	5	5	–	02/17	3	2

See notes at end of table.

Table A-2: OIG Reports to the Board With Recommendations That Were Open During the Reporting Period[a] (continued)

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
The Board Can Enhance Its Diversity and Inclusion Efforts	03/15	11	11	–	03/17	11	–
Security Control Review of the Board's Consolidated Supervision Comparative Analysis, Planning and Execution System (nonpublic report)	09/15	3	3	–	–	–	3
The Board Identified Areas of Improvement for Its Supervisory Stress Testing Model Validation Activities, and Opportunities Exist for Further Enhancement	10/15	8	8	–	03/17	8	–
2015 Audit of the Board's Information Security Program	11/15	4	4	–	11/16	3	1
Security Control Review of the Board's Statistics and Reserves System (nonpublic report)	12/15	6	6	–	–	–	6
Review of the Failure of NBRS Financial	03/16	1	1	–	03/17	1	–
The Board Should Strengthen Controls to Safeguard Embargoed Sensitive Economic Information Provided to News Organizations	04/16	9	9	–	–	–	9
Security Control Review of the Board's Active Directory Implementation (nonpublic report)	05/16	10	10	–	–	–	10
2016 Audit of the Board's Information Security Program	11/16	9	9	–	–	–	9

See notes at end of table.

Table A-2: OIG Reports to the Board With Recommendations That Were Open During the Reporting Period[a] (continued)

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities	11/16	11	11	–	–	–	11
The Board Can Improve Documentation of Office of Foreign Assets Control Examinations	03/17	2	2	–	–	–	2
The Board Can Improve the Effectiveness of Continuous Monitoring as a Supervisory Tool	03/17	2	2	–	–	–	2

a. A recommendation is closed if (1) the corrective action has been taken; (2) the recommendation is no longer applicable; or (3) the appropriate oversight committee or administrator has determined, after reviewing the position of the OIG and division management, that no further action by the agency is warranted. A recommendation is open if (1) division management agrees with the recommendation and is in the process of taking corrective action or (2) division management disagrees with the recommendation and we have referred or are referring it to the appropriate oversight committee or administrator for a final decision.
b. These recommendations were directed jointly to the OCC, the FDIC, and the Board.

Table A-3: Audit, Inspection, and Evaluation Reports Issued to the CFPB During the Reporting Period

Report title	Type of report
2016 Audit of the CFPB's Information Security Program	Audit
The CFPB's Advisory Committees Help Inform Agency Activities, but Advisory Committees' Administration Should Be Enhanced	Audit
Evaluation of the CFPB's Implementation of the Digital Accountability and Transparency Act of 2014	Evaluation
Fiscal Year 2016 Risk Assessment of the CFPB's Purchase Card Program	Risk assessment
Fiscal Year 2016 Risk Assessment of the CFPB's Travel Card Program	Risk assessment
The CFPB Can Strengthen Its Controls for Identifying and Avoiding Conflicts of Interest Related to Vendor Activities	Evaluation
The CFPB's Civil Penalty Fund Is in Compliance With the Improper Payments Information Act of 2002, as Amended	Audit
The CFPB Can Strengthen Contract Award Controls and Administrative Processes	Audit

Total number of audit reports: 4
Total number of evaluation reports: 2
Total number of risk assessments: 2

Table A-4: OIG Reports to the CFPB With Recommendations That Were Open During the Reporting Period[a]

		Recommendations			Status of recommendations		
Report title	Issue date	Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
Evaluation of the Consumer Financial Protection Bureau's Consumer Response Unit	09/12	5	5	–	02/17	3	2
The CFPB Should Strengthen Internal Controls for Its Government Travel Card Program to Ensure Program Integrity	09/13	14	14	–	03/17	11	3
2013 Audit of the CFPB's Information Security Program	12/13	4	4	–	11/16	4	–
The CFPB Has Established Effective GPRA Processes, but Opportunities Exist for Further Enhancement	06/14	3	3	–	03/17	2	1
Security Control Review of the CFPB's Cloud Computing–Based General Support System (nonpublic report)	07/14	4	4	–	09/16	1	3

See notes at end of table.

Table A-4: OIG Reports to the CFPB With Recommendations That Were Open During the Reporting Period[a] (continued)

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
The CFPB Complies With Section 1100G of the Dodd-Frank Act, but Opportunities Exist for the CFPB to Enhance Its Process	09/14	3	3	–	03/17	3	–
Audit of the CFPB's Acquisition and Contract Management of Select Cloud Computing Services	09/14	4	4	–	09/16	3	1
2014 Audit of the CFPB's Information Security Program	11/14	3	3	–	11/16	2	1
The CFPB Can Enhance Its Diversity and Inclusion Efforts	03/15	17	17	–	03/17	14	3
Security Control Review of the CFPB's Tableau System (nonpublic report)	03/15	3	3	–	10/16	3	–
Security Control Review of the CFPB's Data Team Complaint Database (nonpublic report)	07/15	7	7	–	03/17	7	–
CFPB Headquarters Construction Costs Appear Reasonable and Controls Are Designed Appropriately	07/15	1	1	–	02/17	1	–
The CFPB Can Enhance Its Contract Management Processes and Related Controls	09/15	10	10	–	02/17	9	1
Opportunities Exist to Enhance Management Controls Over the CFPB's Consumer Complaint Database	09/15	8	8	–	03/17	7	1
2015 Audit of the CFPB's Information Security Program	11/15	2	2	–	11/16	2	–
Collecting Additional Information Can Help the CFPB Manage Its Future Space-Planning Activities	02/16	1	1	–	02/17	–	1
The CFPB Should Continue to Enhance Controls for Its Government Travel Card Program	06/16	9	9	–	03/17	1	8

See notes at end of table.

Table A-4: OIG Reports to the CFPB With Recommendations That Were Open During the Reporting Period[a] (continued)

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
2016 Audit of the CFPB's Information Security Program	11/16	3	3	–	–	–	3
The CFPB's Advisory Committees Help Inform Agency Activities, but Advisory Committees' Administration Should Be Enhanced	11/16	7	7	–	03/17	2	5
The CFPB Can Strengthen Its Controls for Identifying and Avoiding Conflicts of Interest Related to Vendor Activities	03/17	5	5	–	–	3	2
The CFPB Can Strengthen Contract Award Controls and Administrative Processes	03/17	6	6	–	–	–	6

a. A recommendation is closed if (1) the corrective action has been taken; (2) the recommendation is no longer applicable; or (3) the appropriate oversight committee or administrator has determined, after reviewing the position of the OIG and division management, that no further action by the agency is warranted. A recommendation is open if (1) division management agrees with the recommendation and is in the process of taking corrective action or (2) division management disagrees with the recommendation and we have referred or are referring it to the appropriate oversight committee or administrator for a final decision.

Table A-5: Audit, Inspection, and Evaluation Reports Issued to the Board and the CFPB With Questioned Costs, Unsupported Costs, or Recommendations That Funds Be Put to Better Use During the Reporting Period[a]

Reports	Number	Dollar value
With questioned costs, unsupported costs, or recommendations that funds be put to better use, regardless of whether a management decision had been made	0	$0

a. Because the Board and the CFPB are primarily regulatory and policymaking agencies, our recommendations typically focus on program effectiveness and efficiency, as well as strengthening internal controls. As such, the monetary benefit associated with their implementation typically is not readily quantifiable. In the event that an audit, inspection, or evaluation report contains quantifiable information regarding questioned costs, unsupported costs, or recommendations that funds be put to better use, this table will be expanded.

Table A-6: Summary Statistics on Investigations During the Reporting Period[a]

Investigative actions	Number or dollar value[b]
Investigative caseload	
Investigations open at end of previous reporting period	68
Investigations opened during the reporting period	17
Investigations closed during the reporting period	21
Investigations open at end of the period	64
Investigative results for the reporting period	
Persons referred to DOJ prosecutors	6
Persons referred to state/local prosecutors	0
Matters referred for prosecution	6
Joint investigations	37
Reports of investigations issued	3
Oral and/or written reprimands	0
Terminations of employment	0
Arrests	7
Suspensions	0
Debarments	0
Prohibitions from banking industry	1
Indictments	5
Criminal informations	9
Criminal complaints	0
Convictions	9
Civil actions	2
Administrative monetary recoveries and reimbursements	$0
Civil judgments	$638,000,000
Criminal fines, restitution, and special assessments	$8,009,552

a. Some of the investigative numbers may include data also captured by other OIGs.
b. Metrics: These statistics were compiled from the OIG's investigative case management and tracking system.

Table A-7: Summary Statistics on Hotline Activities During the Reporting Period

Hotline complaints	Number
Complaints pending from previous reporting period	16
Complaints received during reporting period	331
Total complaints for reporting period	347
Complaints resolved during reporting period	327
Complaints pending	20

Appendix B: Inspector General Empowerment Act of 2016 Requirements

The Inspector General Empowerment Act of 2016 amends section 5 of the Inspector General Act of 1978 by adding reporting requirements that must be included in OIG semiannual reports to Congress. These additional reporting requirements include summaries of certain audits, inspections, and evaluations; investigative statistics; summaries of investigations of senior government employees; whistleblower retaliation statistics; summaries of interference with OIG independence; and summaries of closed audits, evaluations, inspections, and investigations that were not publicly disclosed. Our response to these new requirements is below.

1. Summaries of each audit, inspection, and evaluation report issued to the Board or the CFPB for which no agency comment was returned within 60 days of receiving the report.

   There were no audit, inspection, or evaluation reports issued to the Board or the CFPB for which no agency comment was returned within 60 days of receiving the report.

2. Summaries of each audit, inspection, and evaluation report issued to the Board or the CFPB for which there are outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.

   See appendix C.

3. Statistical tables showing for the reporting period:

    a. the number of issued investigative reports

    b. the number of persons referred to DOJ for criminal prosecution

    c. the number of persons referred to state and local authorities for criminal prosecution

    d. the number of indictments and criminal informations that resulted from any prior referral to prosecuting authorities

    Describe the metrics used to develop the data for these new statistical tables.

    See table A-6.

4. A report on each investigation conducted by the OIG that involves a senior government employee in which allegations of misconduct were substantiated, which includes

    a. a detailed description of the facts and circumstances of the investigation as well as the status and disposition of the matter

    b. whether the matter was referred to DOJ and the date of the referral

    c. whether DOJ declined the referral and the date of such declination

    We initiated an investigation concerning allegations that a Board employee engaged in inappropriate conduct while on government time and during government travel. The investigation substantiated the allegations and determined that the employee also inappropriately used his Board-issued information technology equipment for personal benefit. This matter was presented to DOJ on January 27, 2017, and it declined prosecution. The employee subsequently resigned. This investigation was closed. (case I20160037)

We initiated an investigation concerning allegations that a CFPB employee viewed pornographic material on his CFPB-issued laptop computer. The investigation substantiated the allegations. We did not refer the matter to DOJ because no evidence relating to the serial exploitation of minors was found. A report of investigation was provided to the CFPB for action deemed appropriate. CFPB management initiated administrative action and proposed removal. (case I20160034)

5. A detailed description of any instance of whistleblower retaliation, including information about the official found to have engaged in retaliation and what, if any, consequences the agency imposed to hold that official accountable.

   We have no such instances to report.

6. A detailed description of any attempt by the Board or the CFPB to interfere with the independence of the OIG, including

   a. through budget constraints designed to limit OIG capabilities

   b. incidents when the agency has resisted or objected to OIG oversight activities or restricted or significantly delayed OIG access to information, including the justification of the establishment for such action

   We have no such attempts to report.

7. Detailed descriptions of

   a. inspections, evaluations, and audits conducted by the OIG that were closed and not disclosed to the public

   b. investigations conducted by the OIG involving a senior government employee that were closed and not disclosed to the public

   We had no inspections, evaluations, or audits that were closed and not disclosed to the public.

We initiated an investigation concerning allegations that a Board employee used his position to help another Board employee pursue a research project involving an untested operational risk capital model without proper review. The allegations were unsubstantiated. The investigation was closed. (case I20150048)

We initiated an investigation concerning allegations that a Board employee assigned internationally was not communicating with Board supervisors and was possibly absent without leave. The allegations were unsubstantiated. The investigation was closed. (case I20150059)

We initiated an investigation concerning allegations that a former Board employee improperly disclosed to an executive at a payment system advocacy group details of an impending regulatory change. The investigation found evidence that the former employee disclosed information concerning the change; however, it was determined that the disclosure did not constitute a disclosure of Board confidential information. The investigation was closed. (case I20160032)

Appendix C: Summaries of Reports With Outstanding Unimplemented Recommendations

The Inspector General Empowerment Act of 2016 requires that we provide summaries of each audit, inspection, and evaluation report issued to the Board or the CFPB for which there are outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.

Board of Governors of the Federal Reserve System

Table C-1: Reports to the Board With Unimplemented Recommendations, by Calendar Year[a]

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2011	2	3
2012	2	4
2013	2	3
2014	3	5
2015	4	12
2016	4	39
2017[b]	2	4

a. Because the Board is primarily a regulatory and policymaking agency, our recommendations typically focus on program effectiveness and efficiency, as well as strengthening internal controls. As such, the monetary benefit associated with their implementation typically is not readily quantifiable.
b. Through March 31, 2017.

Response to a Congressional Request Regarding the Economic Analysis Associated with Specified Rulemakings

June 13, 2011

Total number of recommendations: 2
Recommendations open: 2

In May 2011, we received a letter from the minority members of the Senate Committee on Banking, Housing, and Urban Affairs requesting that we review the economic analysis that the Board performed supporting five Dodd-Frank Act rulemakings. To respond to the members' request, we (1) interviewed more than 30 Board employees who worked on the respective rulemaking teams; (2) reviewed supporting documentation from each of the five rulemaking teams; and (3) developed and circulated a questionnaire to determine the qualifications of Board staff who performed economic analysis.

We determined that a number of key statutes provide the Board with rulemaking authority, but they generally do not require economic analysis as part of the Board's rulemaking activities. The Dodd-Frank Act did not mandate that an economic or cost-benefit analysis support the five rulemakings, but the Dodd-Frank Act required each of the respective rulemakings to address certain substantive considerations. In addition, the Paperwork Reduction Act and the Regulatory Flexibility Act required the Board to conduct narrowly tailored evaluations of each rulemaking's paperwork burden and effect on small entities, respectively.

We found that the Board routinely reviews economic data to monitor changing economic conditions and conducts the quantitative economic analysis necessary to satisfy statutory requirements and, on a discretionary basis, to support the rulemaking. Further, we determined that the Board generally sought public input for its rulemaking activities and typically reevaluates the effectiveness of its existing regulations every 5 years. We concluded that the Board generally followed a similar approach for the five rulemakings we reviewed and that the rulemakings we reviewed complied with the Paperwork Reduction Act, the Regulatory Flexibility Act, and the applicable Dodd-Frank Act requirements described in our report.

Our analysis yielded the following findings that resulted in recommendations. First, the Board's policy statement on rulemaking procedures had not been recently updated and, although rulemaking staff were cognizant of the Board's rulemaking practices, none of the staff members cited the policy statement. Second, our review of the *Federal Register* indicated that the notices associated with the respective rulemakings typically provided insight into the general approaches and data used in the economic analysis; however, in some cases, the Board's internal documentation did not clearly outline the work steps underlying the economic analysis.

We recommended that the Board (1) update the Rulemaking Procedures Policy Statement and broadly disseminate it to all employees involved in rulemaking activities and (2) consider establishing documentation standards for rulemaking economic analysis to help ensure reproducibility on an internal basis. In a response to our draft report, the Board stated that the two recommendations would be adopted.

Evaluation of Prompt Regulatory Action Implementation

FRB OIG 2011-05 **September 30, 2011**

Total number of recommendations: 1[1]
Recommendations open: 1

The OIGs of the Board, the FDIC, and Treasury conducted a review of the prompt regulatory action (PRA) provisions of the Federal Deposit Insurance Act. The PRA provisions of the act (section 38, Prompt Corrective Action [PCA], and section 39, Standards for Safety and Soundness) mandated that regulators establish a two-part regulatory framework for improving safeguards for the DIF. These provisions were intended to increase the likelihood that regulators would respond promptly and forcefully to minimize losses to the DIF when federally insured banks fail. Our work focused on the following objectives:

- determining the purpose of and circumstances that led to the PRA provisions (Federal Deposit Insurance Act sections 38 and 39) and lessons learned from the savings and loan crisis in the 1980s

1. This recommendation was directed jointly to the OCC, the FDIC, and the Board.

- evaluating to what extent PCA and the safety and soundness standards were a factor in bank failures and problem institutions during the current crisis
- assessing whether these provisions prompted federal regulators to act more quickly and more forcefully to limit losses to the DIF, in light of findings and lessons learned from the savings and loan crisis and regulators' use of PRA provisions in the current crisis
- determining whether there are other noncapital measures that provide a leading indication of risks to the DIF that should be considered as part of the PRA provisions

We found that PRA provisions were appropriately implemented and helped strengthen oversight to a degree. More specifically, we found the following:

- Regulators implemented PCA appropriately.
- Inherent limitations with PCA's capital-based framework and the sudden and severe economic decline affected PCA's effectiveness.
- Regulators identified deficiencies prior to undercapitalization.
- Regulators used other enforcement actions to address safety and soundness concerns before undercapitalization, but after financial decline occurred.
- Regulators made limited use of section 39 to address deficiencies identified.
- Critically undercapitalized institutions were closed promptly, but overall losses were significant.

To improve the effectiveness of the PRA framework and to meet the section 38 and 39 goals of identifying problems early and minimizing losses to the DIF, we recommended that the FDIC, Board, and OCC agency heads review the matters for consideration presented in this report and work through the Financial Stability Oversight Council to determine whether the PRA legislation or implementing regulations should be modified. The matters for consideration were (1) to develop specific criteria and corresponding enforcement actions for noncapital factors, (2) to increase the

minimum PCA capital levels, and (3) to continue to refine the deposit insurance system for banks with assets under $10 billion to assess greater premiums commensurate with risk taking.

Each of the agency responses to our draft report and the identified planned actions addressed the intent of the recommendation. The Board's written response concurs with the general findings in the report, defers the third subrecommendation to the FDIC, and notes that the Board has taken steps for partial closure on this recommendation.

Security Control Review of the National Remote Access Services System (nonpublic report)

March 30, 2012

Total number of recommendations: 8
Recommendations open: 1

We completed a security control review of the Federal Reserve System's National Remote Access Services (NRAS) system. The Board and the 12 Federal Reserve Banks use NRAS to remotely access Board and Federal Reserve Bank information systems. Our objectives were to evaluate the effectiveness of selected security controls and techniques to ensure that the Board maintains a remote access program that is generally compliant with FISMA requirements.

Overall, our review found that NRAS is technically and operationally sound and that the Board has developed an adequate process to administer the token keys for Board personnel. However, we identified opportunities to strengthen information security controls to help ensure that NRAS meets FISMA requirements.

In comments on a draft of our report, the Director of the Board's Division of Information Technology generally agreed with our recommendations and outlined corrective actions.

Security Control Review of the Board's Public Website (nonpublic report)

April 20, 2012

Total number of recommendations: 12
Recommendations open: 3

Consistent with the requirements of FISMA, we conducted a security control review of the Board's public website (PubWeb), which is listed as a major application on the Board's FISMA application inventory for the Office of Board Members. As part of the Board's Publications Program, PubWeb provides a large and diverse audience, including the public, with information about the mission and work of the Board and the functions of the Federal Reserve System.

Our audit objective was to evaluate the adequacy of selected security controls for protecting the PubWeb application from unauthorized access, modification, destruction, or disclosure. To accomplish this objective, we used a control assessment review program based on the security controls defined in National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*. This document provides a baseline for managerial, operational, and technical security controls for organizations to use in protecting their information systems.

Our review of the PubWeb application showed that, in general, controls are adequately designed and implemented. However, we identified opportunities to strengthen information security controls to help ensure that PubWeb meets FISMA requirements. The Director of the Board's Division of Information Technology and the Assistant to the Board, Office of Board Members, stated that they generally agree with the recommendations discussed in the report, and in many cases, corrective action has already been completed or is well underway. We will follow up on the implementation of these recommendations as part of our future FISMA-related audit activities.

Board Should Enhance Compliance with Small Entity Compliance Guide Requirements Contained in the Small Business Regulatory Enforcement Fairness Act of 1996

2013-AE-B-008 **July 1, 2013**

Total number of recommendations: 2
Recommendations open: 2

In this evaluation, we assessed the Board's compliance with certain requirements of the Small Business Regulatory Enforcement Fairness Act of 1996, as amended (SBREFA). We initiated this evaluation to determine the validity of a complaint received by the OIG Hotline concerning the Board's compliance with SBREFA.

SBREFA became law in 1996 and was later amended by the Small Business and Work Opportunity Act of 2007 to include specific requirements for small entity compliance guides. These guides are created by federal rulemaking agencies to explain the actions a small entity should take to comply with a rule. Section 605(b) of SBREFA generally allows the agency head to certify in the *Federal Register*, as part of the proposed or final rule, that the final rule will not have a significant economic impact on a substantial number of small entities. In such cases, a compliance guide does not have to be created. The 2007 amendments to SBREFA also included a congressional reporting requirement.

We found that the Board was not consistent in developing or updating small entity compliance guides in accordance with SBREFA requirements. In addition, the Board's compliance guides did not consistently provide clear guidance to small entities, explaining how to comply with certain rules or when the requirements of the specific rules would be satisfied. Instead, many of the guides merely restated and summarized each section of the rules.

We also reviewed the Board's compliance with the annual congressional reporting requirement to describe the status of the agency's compliance with the small entity compliance guide requirements created by the 2007 amendments to SBREFA. We requested documentation evidencing that the annual congressional reporting requirement had been satisfied, but we did not receive any.

We recommended that the Board establish centralized oversight and a standard method or approach for creating small entity compliance guides. We also recommended that the Board begin submitting the annual reports describing the agency's compliance with small entity compliance guide requirements to the relevant congressional committees as required by section 212(a)(6) of SBREFA. Management concurred with our recommendations and stated that it would take steps to implement them.

The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control

2013-AE-B-013 **September 5, 2013**

Total number of recommendations: 1
Recommendations open: 1

Our objective for this audit was to determine the processes for establishing, maintaining, and monitoring internal control within the Board. We focused on internal control over the effectiveness and efficiency of operations and compliance with laws and regulations, i.e., administrative internal control. Internal control is an integral part of managing an organization and is critical to improving organizational effectiveness and accountability. It comprises the plans, methods, and procedures used to meet the organization's mission, goals, and objectives. Internal control is the first line of defense in safeguarding assets and preventing and detecting errors and fraud; thus, it helps organizations achieve desired results through effective stewardship of government resources.

The Federal Managers' Financial Integrity Act (FMFIA) requires that each executive agency establish internal accounting and administrative controls in compliance with standards established by the U.S. Government Accountability Office and prepare an annual statement on internal control based on an evaluation performed using Office of Management and Budget guidelines. Although the Board is not subject to FMFIA, the Board decided to voluntarily comply with the spirit and intent of FMFIA shortly after its enactment.

We found that the Board's divisions have processes for establishing administrative internal control that are tailored to their specific

responsibilities. These controls generally use best practices and are designed to increase efficiency and react to changing environments; however, the Board's processes for maintaining and monitoring these controls can be enhanced. Specifically, we found that the Board does not have an agencywide process for maintaining and monitoring its administrative internal control. The Board's approach to addressing the provisions of FMFIA does not require management to assess and monitor administrative internal control. We believe that an agencywide process that maintains, monitors, and reports on administrative internal control can assist the Board in effectively and efficiently achieving its mission, goals, and objectives, as well as address the organizational challenges outlined in the Board's 2012–2015 strategic framework.

We recommended that the Chief Operating Officer designate responsible officials or an office to develop and implement an agencywide policy and process to more closely follow the spirit and intent of FMFIA and develop a training program to increase staff awareness about maintaining and monitoring administrative internal control. Management concurred with the recommendation's intent, stating that the Board has already implemented, or is in the process of implementing, several enhanced administrative processes. Management added that it would evaluate whether and in what form an agencywide framework makes sense, given the priorities and budgetary constraints underlying the Board's new strategic framework, and that it would coordinate with the Executive Committee of the Board to implement any additional requirements.

Enforcement Actions and Professional Liability Claims Against Institution-Affiliated Parties and Individuals Associated with Failed Institutions

2014-SR-B-011 **July 25, 2014**

Total number of recommendations: 3[2]
Recommendations open: 2

Our office, the FDIC OIG, and the Treasury OIG participated in this evaluation concerning actions that the FDIC, the Board, and the OCC took against individuals and entities in response to actions

2. Two of these recommendations were directed jointly to the Board, the OCC, and the FDIC. One recommendation was directed jointly to the Board and the OCC.

that harmed financial institutions. The objectives of the evaluation were (1) to describe the FDIC's, the Board's, and the OCC's processes for investigating and pursuing enforcement actions against institution-affiliated parties associated with failed institutions, as well as the results of those efforts; (2) to describe the FDIC's process for investigating and pursuing professional liability claims against individuals and entities associated with failed institutions and its coordination with the Board and the OCC; (3) to determine the results of the FDIC's, the Board's, and the OCC's efforts in investigating and pursuing enforcement actions against institution-affiliated parties and the FDIC's efforts in pursuing professional liability claims; and (4) to assess key factors that may impact the pursuit of enforcement actions and professional liability claims.

The joint evaluation team found that several factors appeared to affect the three regulators' ability to pursue enforcement actions against institution-affiliated parties. Those factors included the rigorous statutory criteria for sustaining removal/prohibition orders; the extent to which each regulator was willing to use certain enforcement action tools, such as personal cease and desist orders; the risk appetite of the FDIC, the Board, and the OCC for bringing enforcement actions; enforcement action statutes of limitation; and staff resources. The report also notes that these regulators should address differences in how they notify each other when initiating enforcement actions against institution-affiliated parties and depository institutions.

The three report recommendations that apply to the Board seek to strengthen the Board's program for pursuing enforcement actions. In its response to the report, the Board acknowledged the recommendations and described its planned activities.

Opportunities Exist to Enhance the Board's Oversight of Future Complex Enforcement Actions

2014-SR-B-015 **September 30, 2014**

Total number of recommendations: 5
Recommendations open: 2

In February 2013, the Board and the OCC issued amended consent orders that require mortgage servicers to provide about $3.67 billion in payments to nearly 4.2 million borrowers based on possible

harm and to provide other foreclosure prevention assistance. Our objectives for this evaluation were (1) to evaluate the Board's overall approach to oversight of the amended consent orders, (2) to determine the effectiveness of the Board's oversight of the borrower slotting process, and (3) to determine the effectiveness of the Board's oversight of the servicers' paying agent, Rust Consulting, Inc.

We found that the Board's advance preparation and planning efforts for the payment agreement with the 13 servicers that joined the agreement in January 2013 were not commensurate with the complexity associated with this unprecedented interagency effort. In addition, project management resources were not available to the Board's oversight team for this initiative. Further, we found that data integrity issues at two servicers affected the reliability and consistency of the slotting results. The payment agreement required servicers to slot borrowers into categories of possible harm—with payment amounts set for each category—that were defined by Board and OCC staff. The approach to resolving these data integrity issues may have resulted in borrowers who experienced similar harm receiving different payment amounts. We also determined that an approach had not been selected to end the payment agreement. Despite these challenges and limitations, as of August 15, 2014, borrowers had cashed or deposited checks representing about $3.15 billion, or approximately 86 percent, of the total $3.67 billion.

We made five recommendations to improve the Board's oversight of future complex enforcement strategies. The Board generally agreed with our recommendations and noted the corrective actions that it had implemented or intended to implement.

Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle

2014-IT-B-021 **December 18, 2014**

Total number of recommendations: 3
Recommendations open: 1

We completed a review of the operational efficiency and effectiveness of the Board's information security life cycle. We performed this audit pursuant to requirements set forth in FISMA.

Overall, we found that the Chief Information Officer maintains a FISMA-compliant information security program that is consistent with requirements for certification and accreditation established by the National Institute of Standards and Technology and the Office of Management and Budget; however, we identified opportunities to improve the operational efficiency and effectiveness of the Board's management of its information security life cycle.

Our report contains recommendations designed to improve the operational efficiency and effectiveness of the Board's information security life cycle process. The Director of the Division of Information Technology agreed with the recommendations and stated that the division would take action to address the recommendations.

Review of the Failure of Waccamaw Bank

2015-SR-B-005 **March 26, 2015**

Total number of recommendations: 5
Recommendations open: 2

Waccamaw Bank was supervised both by the Federal Reserve Bank of Richmond under delegated authority from the Board and by the North Carolina Office of the Commissioner of Banks. On June 8, 2012, the North Carolina Office of the Commissioner of Banks closed Waccamaw Bank and appointed the FDIC as receiver. The FDIC estimated that the failure of Waccamaw Bank would result in a $51.1 million loss to the DIF, which was beneath the material loss threshold. Consistent with Dodd-Frank Act requirements, we concluded that Waccamaw Bank's failure presented unusual circumstances that warranted an in-depth review.

Based on the in-depth review, we determined that Waccamaw Bank failed because its board of directors and senior management did not control the risks associated with its rapid growth strategy. As a result, the bank sustained significant losses during a downturn in its local real estate market. In addition, we learned that (1) supervisory activity records were not retained in accordance with Board policy, (2) Waccamaw Bank's written agreement did not contain a provision that required regulatory approval of material transactions, and (3) Board and Federal Reserve Bank of Richmond appeals policies were silent on procedural aspects for second-level and third-level appeals.

We made recommendations related to the Board's records retention and appeals policies and procedures. The Director of the Division of Banking Supervision and Regulation agreed with our recommendations and outlined planned corrective actions to address them.

Security Control Review of the Board's Consolidated Supervision Comparative Analysis, Planning and Execution System

2015-IT-B-015 **September 2, 2015**

Total number of recommendations: 3
Recommendations open: 3

We completed a security control review of the Board's Consolidated Supervision Comparative Analysis, Planning and Execution System (C-SCAPE), which is intended to provide supervisory teams throughout the Federal Reserve System with tools and methods to plan and execute supervisory events, manage issues, and enhance decisionmaking around the examination planning process. Our audit objective was to evaluate the adequacy of selected security controls implemented by the Board to protect C-SCAPE from unauthorized access, modification, destruction, or disclosure. We also evaluated C-SCAPE's compliance with FISMA and the information security policies, procedures, standards, and guidelines of the Board.

Overall, we found that the Board has taken steps to secure the C-SCAPE application in accordance with FISMA and the Board's information security program. However, during

vulnerability scanning of the databases supporting C-SCAPE, we found vulnerabilities that require the attention of the C-SCAPE application owner and the Board's Division of Information Technology. Additionally, we noted that the C-SCAPE application audit logs do not record certain database activity on financial institution information.

Our report includes recommendations to address C-SCAPE database vulnerabilities. We also identified items for management's consideration that were already being addressed by management. The Chief Information Officer and the Director of the Division of Banking Supervision and Regulation agreed with our recommendations.

2015 Audit of the Board's Information Security Program

2015-IT-B-019 **November 13, 2015**

Total number of recommendations: 4
Recommendations open: 1

FISMA requires IGs to conduct an annual, independent evaluation of their respective agencies' information security programs and practices. In support of FISMA's independent evaluation requirements, DHS issued guidance to IGs on FISMA reporting for 2015. The guidance directs IGs to evaluate agencies' information security programs in 10 areas. The guidance also references a new five-level maturity model for IGs to use in assessing agencies' information security continuous monitoring programs. In accordance with these requirements, we reviewed the Board's information security program. Specifically, we evaluated (1) the Board's compliance with FISMA and related information security policies, procedures, standards, and guidance and (2) the effectiveness of security controls and techniques for a subset of the Board's information systems.

Overall, we found that the Board's Chief Information Officer has developed, documented, and implemented an information security program that is generally consistent with the requirements established by FISMA and the 10 areas outlined in DHS's FISMA reporting guidance for IGs.

Our report includes recommendations to strengthen the Board's information security program in the areas of information

security continuous monitoring, configuration management, and identity and access management. The Board agreed with our recommendations and noted that it was addressing them. Further, based on corrective actions taken by the Board's Information Security Officer, we closed the open recommendations from our prior years' FISMA reports related to contractor systems, information security continuous monitoring, and plans of action and milestones.

Security Control Review of the Board's Statistics and Reserves System

2015-IT-B-021 **December 17, 2015**

Total number of recommendations: 6
Recommendations open: 6

The Board's Statistics and Reserves System (STAR) is a web-based application that collects and edits over 75 periodic statistical reports that are received from financial institutions. In addition, the system manages financial institutions' reserve requirements and term deposits. We performed this audit in accordance with FISMA requirements. Specifically, we evaluated the adequacy of selected information security controls for protecting Board data in STAR from unauthorized access, modification, destruction, or disclosure, as well as the system's compliance with FISMA and the Board's information security policies, procedures, standards, and guidelines.

Overall, we found that the Board's Division of Monetary Affairs and its Division of Information Technology have taken several steps to implement information security controls for STAR, in accordance with FISMA and the *Board Information Security Program*. However, we found that improvements are needed in the Board's security governance of STAR to ensure that information security controls are adequately implemented, assessed, authorized, and monitored.

Our report includes recommendations that focus on strengthening information security controls related to planning, security assessment and authorization, contingency planning, auditing, access control, risk assessment, and system and information integrity. The Board agreed with our recommendations and outlined actions that had been or would be taken to address them.

The Board Should Strengthen Controls to Safeguard Embargoed Sensitive Economic Information Provided to News Organizations

2016-MO-B-006 **April 15, 2016**

Total number of recommendations: 9
Recommendations open: 9

Our audit objective was to assess the Board's controls to protect sensitive economic information from unauthorized disclosure when it is provided under embargo to news organizations either through a press lockup room located at the Board or through the Board's embargo application, which enables news participants to remotely access information made available by the Board.

During the course of this audit, we discovered issues that warranted the Board's immediate attention. We issued a restricted early alert memorandum to the Board on July 16, 2015, that outlined these concerns and included recommendations. On August 19, 2015, a news organization broke the embargo of the Federal Open Market Committee meeting minutes that had been provided through the embargo application. On August 21, 2015, the Board ceased using the embargo application to provide news organizations embargoed access to Federal Open Market Committee–related information and other market-moving economic publications within the scope of our audit. Separately, the Board relocated its press lockup room in September 2015, a move that had been planned before our audit began.

We identified opportunities for the Board (1) to more strictly adhere to controls already established in policies, procedures, and agreements with participating news organizations and (2) to establish new controls to more effectively safeguard embargoed economic information. We also identified risks to providing information under embargo through the embargo application.

Our report contains recommendations designed to strengthen the Board's controls to safeguard sensitive economic information provided to news organizations under embargo and includes actions taken by the Board in response to the early alert memorandum. The Board generally concurred with our recommendations and noted both that substantial improvements were planned before we began our review and that many were implemented during our review.

Security Control Review of the Board's Active Directory Implementation

2016-IT-B-008 **May 11, 2016**

Total number of recommendations: 10
Recommendations open: 10

Our audit objective, as required by FISMA, was to evaluate the administration and security design effectiveness of the Active Directory operating environment implemented at the Board. To accomplish this objective, we (1) evaluated whether the Board has conducted a proper risk assessment of the Board's Active Directory domain; (2) determined whether tools and processes have been implemented to continuously monitor the Board's Active Directory domain; (3) determined whether the tools and processes implemented allow for users (active employees, contractors, super users, administrators, and others) to be properly identified; (4) determined whether the Board's Active Directory domain is properly configured and scanned for vulnerabilities; and (5) determined whether contingency planning processes have been established for the Board's Active Directory domain.

Overall, we found that the Board is effectively administering and protecting the Active Directory infrastructure. We found, however, that the Board can strengthen Active Directory controls in the areas of risk management, continuous monitoring, user group management, contractor account management, and system documentation. In addition, we identified a risk for management's continued attention related to transport layer security. Our report includes recommendations to address these findings, and the Board generally concurred with those recommendations.

2016 Audit of the Board's Information Security Program

2016-IT-B-013 **November 10, 2016**

Total number of recommendations: 9
Recommendations open: 9

See the summary in the body of this report.

Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities

2016-SR-B-014 **November 14, 2016**

Total number of recommendations: 11
Recommendations open: 11

See the summary in the body of this report.

The Board Can Improve Documentation of Office of Foreign Assets Control Examinations

2017-SR-B-003 **March 15, 2017**

Total number of recommendations: 2
Recommendations open: 2

See the summary in the body of this report.

The Board Can Improve the Effectiveness of Continuous Monitoring as a Supervisory Tool

2017-SR-B-005 **March 29, 2017**

Total number of recommendations: 2
Recommendations open: 2

See the summary in the body of this report.

Consumer Financial Protection Bureau

Table C-2: Reports to the CFPB With Unimplemented Recommendations, by Calendar Year[a]

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2012	1	2
2013	1	3
2014	4	6
2015	3	5
2016	4	17
2017[b]	2	8

a. Because the CFPB is primarily a regulatory and policymaking agency, our recommendations typically focus on program effectiveness and efficiency, as well as strengthening internal controls. As such, the monetary benefit associated with their implementation typically is not readily quantifiable.
b. Through March 31, 2017.

Evaluation of the Consumer Financial Protection Bureau's Consumer Response Unit

September 28, 2012

Total number of recommendations: 5
Recommendations open: 2

We completed a review of the CFPB's Consumer Response unit. The Dodd-Frank Act mandated that the CFPB "establish a unit whose functions shall include establishing a single, toll-free telephone number, a website, and a database to facilitate the centralized collection of, monitoring of, and response to consumer complaints regarding consumer financial products or services" offered by the companies under its jurisdiction.[3] The Dodd-Frank Act also requires that the CFPB coordinate with other federal

3. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 1013(b)(3)(A), 124 Stat. 1376, 1969 (2010) (codified at 12 U.S.C. § 5493(b)(3)(A) (2010)).

agencies to appropriately process complaints.[4] To satisfy the Dodd-Frank Act's requirements for processing consumer complaints, the CFPB created the Consumer Response unit. Our objectives were (1) to evaluate the process the CFPB has established to receive, respond to, and track consumer complaints; (2) to assess the CFPB's coordination with federal and state agencies regarding the processing and referral of complaints; and (3) to determine the extent to which the CFPB is assessing its effectiveness and timeliness in responding to consumer complaints.

Our analysis determined that the CFPB has a reasonable process to receive, respond to, and track consumer complaints. In addition, the CFPB's consumer response process generally complies with Dodd-Frank Act requirements, the Privacy Act, and industry best practices. The CFPB has a comprehensive manual of standard operating procedures for processing complaints. The manual includes internal controls to mitigate risk in processing consumer complaints. Further, no issues came to our attention to indicate noncompliance with or internal control weaknesses related to the size and nature of the Consumer Response unit's organizational structure, oversight of its contracted contact centers, communication within the Consumer Response unit and throughout the CFPB, coordination with other regulatory agencies for complaint referrals, and the CFPB's schedule for the incremental acceptance of complaints by financial product.

However, our review did note areas in which the CFPB can improve processes and strengthen controls in the Consumer Response unit. Our report contains recommendations to address (1) the inaccurate manual data entry of consumer complaints, (2) the inconsistency of complaint management system data, (3) the lack of a finalized

4. The Dodd-Frank Act requires the CFPB to enter into a memorandum of understanding with "any affected Federal regulatory agency regarding procedures by which any covered person, and the prudential regulators, and any other agency having jurisdiction over a covered person, including the Secretary of the Department of Housing and Urban Development and the Secretary of Education, shall comply with this section." Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 1034(d), 124 Stat. 1376, 2009 (2010) (codified at 12 U.S.C. § 5534(d) (2010)). The term *covered person* is defined as "any person that engages in offering or providing a consumer financial product or service," as well as any affiliate thereof if the affiliate acts as a service provider to such person. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 1002(6), 124 Stat. 1376, 1956 (2010) (codified at 12 U.S.C. § 5481(6) (2010)).

agencywide privacy policy, (4) the lack of a comprehensive quality assurance program, and (5) the lack of a centralized tracking system for quality assurance reviews. The Assistant Director of the Consumer Response unit agreed with our recommendations and specified actions that had been taken, were underway, or were planned to implement them.

The CFPB Should Strengthen Internal Controls for Its Government Travel Card Program to Ensure Program Integrity

2013-AE-C-017 **September 30, 2013**

Total number of recommendations: 14
Recommendations open: 3

Our objective for this audit was to determine the effectiveness of the CFPB's internal controls for its government travel card (GTC) program. Specifically, we assessed compliance with policies and procedures and whether internal controls were designed and operating effectively to prevent and detect fraudulent or unauthorized use of travel cards and to provide reasonable assurance that cards are properly issued, monitored, and closed out.

Through its GTC program, the CFPB provides its employees with the necessary resources to arrange and pay for official business travel and other travel-related expenses and to receive reimbursements for authorized expenses. The CFPB's Travel and Relocation Office within the Office of the Chief Financial Officer oversees the GTC program. In fiscal year 2012, the CFPB spent more than $10 million, or about 3 percent of its incurred expenses, on travel. As of April 30, 2013, the CFPB had 743 active cardholder accounts.

We found that internal controls for the CFPB GTC program should be strengthened to ensure program integrity. Although controls over the GTC issuance process were designed and operating effectively, controls were not designed or operating effectively (1) to prevent and detect fraudulent or unauthorized use of GTCs and (2) to provide reasonable assurance that cards are properly monitored and closed out.

We made 14 recommendations designed to assist the CFPB in strengthening its internal controls over the GTC program. Management concurred with our recommendations, has taken

corrective actions to close 11 recommendations, and has begun taking steps to implement the remaining 3 open recommendations.

The CFPB Has Established Effective GPRA Processes, but Opportunities Exist for Further Enhancement

2014-MO-C-008 **June 30, 2014**

Total number of recommendations: 3
Recommendations open: 1

We conducted this audit to assess (1) the effectiveness of the CFPB's processes that address the Government Performance and Results Act of 1993, as amended by the GPRA Modernization Act of 2010 (GPRA) and (2) the CFPB's compliance with applicable sections of GPRA. GPRA requires that most executive agencies produce strategic plans every 4 years and publish annual agency performance plans. The CFPB determined that it is generally subject to the requirements of GPRA, except for those provisions of GPRA that require agencies to follow guidance issued by the Office of Management and Budget or to submit to the Office of Management and Budget's jurisdiction or oversight.

We found that the CFPB developed effective strategic and performance planning processes. The CFPB expanded these processes beyond GPRA requirements by developing division-level strategic plans with division-level performance goals and performance measures and implementing a quarterly performance review process. We found that the CFPB fully satisfied 22 of 28 applicable GPRA requirements and that opportunities existed for the CFPB to further enhance its GPRA processes.

Our report contains three recommendations designed to ensure full GPRA compliance and to assist the CFPB in building on its success in establishing GPRA processes. Management identified actions that had been or would be taken to address our recommendations.

Security Control Review of the CFPB's Cloud Computing–Based General Support System

2014-IT-C-010 **July 17, 2014**

Total number of recommendations: 4
Recommendations open: 3

FISMA requires the OIG to evaluate the effectiveness of the information security controls and techniques for a subset of the agency's information systems, including those provided or managed by another agency, a contractor, or another organization. To meet FISMA requirements, we reviewed the information system security controls for the CFPB's cloud computing–based general support system.

The CFPB has invested in a cloud computing–based general support system that provides the information technology infrastructure to support the agency's applications and common enterprise services, such as email, instant messaging, and file storage. The general support system is jointly managed and operated by the CFPB and a third party, and it is classified as a moderate-risk system.

Overall, we found that the CFPB has taken a number of steps to secure its cloud computing–based general support system in accordance with FISMA requirements. However, we found that improvements are needed to ensure that FISMA processes and controls are effective and consistently implemented across all information security areas for the general support system.

Our report includes recommendations to strengthen security controls for the general support system in four information security areas: system and information integrity, configuration management, contingency planning, and incident response. The CFPB's Chief Information Officer concurred with our recommendations and outlined actions that had been or would be taken to address them.

Audit of the CFPB's Acquisition and Contract Management of Select Cloud Computing Services

2014-IT-C-016 **September 30, 2014**

Total number of recommendations: 4
Recommendations open: 1

In January 2014, CIGIE spearheaded a governmentwide review of select agencies' efforts to adopt cloud computing technologies. In support of this initiative, our objective was to review the CFPB's acquisition and contract management for two of the CFPB's seven cloud service providers to determine whether requirements for security, service levels, and access to records were planned for, defined in contracts, and being monitored.

Overall, we found that (1) the CFPB's contracts for cloud computing services included roles and responsibilities, information security requirements, and service-level expectations; (2) the CFPB has established a process to monitor both contractual and service-level requirements for its cloud service providers; and (3) the agency collects and maintains nondisclosure agreements from contractor personnel to protect sensitive information. However, we identified opportunities for improvement in the procurement and use of cloud services, such as performing alternatives analysis and cost analysis and including clauses that provide the access needed for electronic discovery and performance of criminal and noncriminal investigations. We also found that one of the contracts we reviewed did not (1) include a clause granting the OIG the right to examine agency records or (2) detail specific penalties or remedies for noncompliance with contract terms and service levels.

Our report contains four recommendations to assist the CFPB's Chief Information Officer in strengthening processes for the acquisition and contract management of cloud services. The Chief Information Officer concurred with our recommendations and outlined actions that had been taken or would be implemented to address them.

2014 Audit of the CFPB's Information Security Program

2014-IT-C-020 **November 14, 2014**

Total number of recommendations: 3
Recommendations open: 1

We completed our annual review of the CFPB's information security program. FISMA requires the OIG to conduct an annual, independent evaluation of the agency's information security program and practices. We found that the CFPB continued to take steps to mature its information security program and to ensure that it is consistent with the requirements of FISMA. Overall, we found that the CFPB's information security program was consistent with 9 of 11 information security areas. Although corrective actions were underway, further improvements were needed in security training and contingency planning. Although we found that the CFPB's information security program was generally consistent with the requirements for continuous monitoring, configuration management, and incident response, we identified opportunities to strengthen these areas through automation and centralization.

Our report includes three new recommendations designed to strengthen the CFPB's information security continuous monitoring and configuration management practices. The Chief Information Officer concurred with our recommendations and outlined actions that had been taken, were underway, and were planned to strengthen the CFPB's information security program. In addition, our 2013 FISMA audit report included recommendations to develop and implement (1) an organizationwide configuration management plan and consistent process for patch management, (2) a capability to centrally track and analyze audit logs and security incident information, and (3) a role-based training program.

The CFPB Can Enhance Its Diversity and Inclusion Efforts

2015-MO-C-002 **March 4, 2015**

Total number of recommendations: 17
Recommendations open: 3

Our review of the CFPB's diversity and inclusion efforts was conducted in response to a congressional request. Overall, our audit determined that the CFPB had taken steps to foster a diverse

and inclusive workforce since it began operations in July 2011. These steps included elevating the Office of Minority and Women Inclusion and the Office of Equal Employment Opportunity to the Office of the Director; conducting listening sessions with employees to identify and respond to perceptions of fairness, equality, and inclusion; and creating an internal advisory council and working groups to focus on diversity and inclusion issues.

We identified four areas of the CFPB's diversity and inclusion efforts that could be enhanced. First, diversity and inclusion training was not mandatory for CFPB employees, supervisors, and senior managers. Second, data quality issues existed in the CFPB's tracking spreadsheets for equal employment opportunity complaints and negotiated grievances, and certain data related to performance management were not analyzed for trends that could indicate potential diversity and inclusion issues. Third, the CFPB's diversity and inclusion strategic plan had not been finalized, and opportunities existed for the CFPB to strengthen supervisors' and senior managers' accountability for implementing diversity and inclusion initiatives and human resources–related policies. Finally, the CFPB could benefit from a formal succession planning process to help ensure that it will have a sufficient and diverse pool of candidates for its senior management positions. We acknowledged that initiatives and activities that were beyond the scope of our review also contributed to enhancing diversity and inclusion.

Our report contains recommendations designed to improve the monitoring and the promotion of diversity and inclusion at the CFPB, as well as to strengthen related controls. The CFPB concurred with our recommendations and outlined planned, ongoing, and completed activities related to analyzing performance management data, performance management training, and tracking of equal employment opportunity and non–equal employment opportunity complaints. The CFPB has since taken action to address and close several recommendations.

The CFPB Can Enhance Its Contract Management Processes and Related Controls

2015-FMIC-C-014 **September 2, 2015**

Total number of recommendations: 10
Recommendations open: 1

We completed an audit of the CFPB's contract management processes and related controls. Our audit objective was to assess the CFPB's compliance with applicable laws, regulations, and CFPB policies and procedures related to contract management, as well as the effectiveness of the CFPB's internal controls related to contract management.

In general, we found the CFPB to be in compliance with applicable laws, regulations, and CFPB policies and procedures, although we noted that certain contract management controls could have been improved in 3 contracts among the 29 contracts in our sample. We also found that 32 of the 79 contractor performance evaluations required by the *Federal Acquisition Regulation* were overdue. Further, the Bureau of the Fiscal Service's Division of Procurement omitted a contract clause designed to clarify the OIG's access to contractor records from one of the 10 contracts we sampled for this purpose. The CFPB's Office of Minority and Women Inclusion is required to develop standards and procedures to ensure that minority-owned and women-owned businesses are considered for CFPB procurements, including procedures that will enable the CFPB to know whether contractors have failed to make a good faith effort to include minorities and women in their workforce. Although there is no statutory deadline, these standards and procedures had not yet been developed.

Our report includes recommendations designed to improve the CFPB's contract management processes and related controls. The CFPB concurred with our recommendations.

Opportunities Exist to Enhance Management Controls Over the CFPB's Consumer Complaint Database

2015-FMIC-C-016 **September 10, 2015**

Total number of recommendations: 8
Recommendations open: 1

Our audit objective was to assess the effectiveness of the CFPB's controls over the accuracy and completeness of its public-facing Consumer Complaint Database.

We determined that the CFPB's Office of Consumer Response had implemented controls to monitor the accuracy of complaint data in the internal case management system, but it had not established separate management controls to ensure the accuracy of the Consumer Complaint Database. We also found that the Office of Consumer Response was not (1) reviewing all company closing responses, including verifying whether the company-selected response is consistent with the definition, and (2) consistently publishing untimely company closing responses in the Consumer Complaint Database. In addition, consumers were not consistently offered the opportunity to dispute untimely company responses. Finally, although the Consumer Complaint Database website asserts that complaint data are refreshed daily, we found that the Office of Consumer Response did not consistently notify the public when the database was not updated.

Because the Data Team Complaint Database plays a role in the daily update process, our findings should be considered in conjunction with the security control deficiencies associated with the Data Team Complaint Database that were identified in OIG Report 2015-IT-C-011, *Security Control Review of the CFPB's Data Team Complaint Database*.

Our report includes recommendations designed to improve the CFPB's controls over the accuracy and completeness of the Consumer Complaint Database. The CFPB concurred with our recommendations.

Collecting Additional Information Can Help the CFPB Manage Its Future Space-Planning Activities

2016-FMIC-C-002 **February 3, 2016**

Total number of recommendations: 1
Recommendations open: 1

The CFPB's Office of Administrative Operations is responsible for managing space for approximately 1,500 CFPB employees in its headquarters and regional offices. In fiscal year 2015, the CFPB budgeted $29.6 million for its occupancy agreements for these offices, which includes $10.0 million for temporary office space that is needed because the CFPB is renovating its headquarters building. We assessed the CFPB's short-term and long-term space planning to determine whether controls are in place to effectively manage the agency's space needs and associated costs. We focused on the CFPB's processes for planning, obtaining, and managing space for both its headquarters and regional offices.

We identified controls that the Office of Administrative Operations is using to plan for CFPB headquarters office space; however, we found that the CFPB could benefit from implementing a process to manage information about its regional space needs and associated costs. The Office of Administrative Operations plans to continue using the U.S. General Services Administration for its future regional space procurement needs, and the U.S. General Services Administration gathers relevant information from the CFPB to gain an understanding of its space requirements. Therefore, our report includes a recommendation designed to ensure that the CFPB consistently collects, maintains, and uses information about its evolving space needs to manage the agency's future space planning and associated costs. The CFPB agreed with our recommendation and outlined planned corrective actions.

The CFPB Should Continue to Enhance Controls for Its Government Travel Card Program

2016-FMIC-C-009 **June 27, 2016**

Total number of recommendations: 9
Recommendations open: 8

Our audit objective was to determine whether the CFPB had established and maintained internal controls for its GTC program in accordance with the Government Charge Card Abuse Prevention Act of 2012.

We found that although the CFPB had implemented several controls over its GTC program, some controls were not designed or operating effectively (1) to prevent or identify unauthorized use of the GTCs and (2) to provide reasonable assurance that cards were closed in a timely manner upon employees' separation. Therefore, our report contains recommendations designed to help ensure GTC program integrity. The CFPB concurred with our recommendations.

2016 Audit of the CFPB's Information Security Program

2016-IT-C-012 **November 10, 2016**

Total number of recommendations: 3
Recommendations open: 3

See the summary in the body of this report.

The CFPB's Advisory Committees Help Inform Agency Activities, but Advisory Committees' Administration Should Be Enhanced

2016-MO-C-016 **November 30, 2016**

Total number of recommendations: 7
Recommendations open: 5

See the summary in the body of this report.

The CFPB Can Strengthen Its Controls for Identifying and Avoiding Conflicts of Interest Related to Vendor Activities

2017-SR-C-004 **March 15, 2017**

Total number of recommendations: 5
Recommendations open: 2

See the summary in the body of this report.

The CFPB Can Strengthen Contract Award Controls and Administrative Processes

2017-FMIC-C-007 **March 30, 2017**

Total number of recommendations: 6
Recommendations open: 6

See the summary in the body of this report.

Abbreviations

Board	Board of Governors of the Federal Reserve System
CFPB	Consumer Financial Protection Bureau
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
C-SCAPE	Consolidated Supervision Comparative Analysis, Planning and Execution System
DATA Act	Digital Accountability and Transparency Act of 2014
DHS	U.S. Department of Homeland Security
DIF	Deposit Insurance Fund
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOJ	U.S. Department of Justice
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FHFA	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
FMFIA	Federal Managers' Financial Integrity Act
GPRA	Government Performance and Results Act of 1993, as amended by the GPRA Modernization Act of 2010
GTC	government travel card
HUD	U.S. Department of Housing and Urban Development
IG	Inspector General
IPIA	Improper Payments Information Act of 2002, as amended
IRS	Internal Revenue Service
LBO	large banking organization
LISCC	Large Institution Supervision Coordinating Committee
NRAS	National Remote Access Services
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control
OIG	Office of Inspector General
PCA	prompt corrective action
PRA	prompt regulatory action
PubWeb	Board's public website
SBREFA	Small Business Regulatory Enforcement Fairness Act of 1996, as amended
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
STAR	Statistics and Reserves System
Treasury	U.S. Department of the Treasury

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551
Phone: 202-973-5000 | Fax: 202-973-5044

OIG Hotline 1-800-827-3340 | OIGHotline@frb.gov