## Office of Inspector General

Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

# Semiannual Report to Congress

April 1, 2020–September 30, 2020

OIG

# Semiannual Report to Congress

April 1, 2020–September 30, 2020


Office of Inspector General

Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

# Message From the Inspector General

Since our previous semiannual report to Congress, the COVID-19 pandemic has become part of our daily lives. Well over 200,000 Americans have died, and countless more face economic hardships and uncertainty while navigating work or unemployment, school, health concerns, caregiving responsibilities, and more—often while also struggling with isolation and the unpredictability of what lies ahead.

Safeguarding inspector general independence and impartiality is now, more so than ever, imperative to ensuring that the programs and operations of the establishments covered by the Inspector General Act of 1978, as amended, are operating efficiently and effectively and are free of fraud, waste, and abuse. The extraordinary response efforts undertaken by the government during the pandemic require effective and independent oversight for the American taxpayer. In support of this mission, I continue to serve on the Pandemic Response Accountability Committee, which is responsible for coordinating inspector general community–wide oversight of the government's COVID-19 pandemic response efforts.

Our independent oversight of the Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection is vital, and we remain committed to our mission during these challenging times. During the past 6 months, our office has been actively monitoring the measures taken by the Board through the authorization of a variety of lending facilities, such as those related to the Main Street Lending Program, established under unusual and exigent circumstances to support the nation's economy. Our monitoring effort has focused on topics such as the design, operation, governance, and oversight of the lending programs, as well as the effect of the programs on the Board's supervision and regulation activities. We recently announced our first audit of the Board's pandemic-related lending programs, which will examine the data aggregation, validation, and reporting processes for the Board's lending programs related to the Coronavirus Aid, Relief, and Economic Security Act, or CARES Act. We are also in the planning stages of an audit of the Board's oversight of the Federal Reserve Banks' vendor selection and management processes related to the Board's CARES Act lending programs, and we expect to announce additional pandemic-related reviews soon. Additionally, as part of the pandemic oversight law enforcement community, our investigations have already resulted in five indictments for a combined attempted fraud of $46 million, and we expect to see more such cases in the coming months. As part of our Bureau-related pandemic oversight, we are planning to conduct an audit of the Bureau's Office of Consumer Response, which collects, monitors, and responds to consumer complaints on financial services and products. This office is experiencing an organizational shift and has seen an increase in consumer

complaints as a result of the COVID-19 pandemic. We plan to assess the Bureau's effectiveness and timeliness in responding to these complaints.

In addition to pandemic-related oversight, we issued reports on the Bureau's budget and funding processes and periodic monitoring of supervised institutions. We reviewed the Bureau's budget and funding processes in response to a congressional request and in consideration of the fact that the Bureau receives its funding primarily through transfers from the Board, rather than through the federal appropriations process. We assessed the design and implementation of the controls over the Bureau's budget processes as well as its compliance with applicable laws and regulations. In our periodic monitoring evaluation, we assessed the Bureau's approach to monitoring supervised institutions for consistency with the Bureau's strategic plan and internal policies and procedures. The Bureau monitors supervised institutions to maintain reasonably current information on their activities and to assess whether changes in risks to consumers or markets warrant changes in the Bureau's planned supervisory activities. Other reports we issued during the reporting period covered the Bureau's travel and purchase card programs, contractor compliance, and personnel security program.

We also issued a Board evaluation report concerning the effectiveness of the Board's and the Reserve Banks' cybersecurity supervision approach for Large Institution Supervision Coordinating Committee firms. Continuing our efforts to ensure information security, we issued three memorandum reports discussing the results of the testing we conducted as part of our annual Federal Information Security Modernization Act of 2014 reviews of the effectiveness of the Board's and the Bureau's information security programs.

During this reporting period, we saw results in several high-profile investigations related to the programs and operations of the Board. The former president, the chief credit officer, and the executive vice president of First NBC Bank were indicted for an alleged fraud scheme totaling hundreds of millions of dollars and involving at least seven coconspirators; the former president of Whitaker Bank in Kentucky pleaded guilty to embezzling or misapplying more than $50,000 of the bank's funds; the former chief executive officer of Crown Bank in Minnesota pleaded guilty to wire fraud and filing a false income tax return; and the former vice president of loan operations for SmartBank in Tennessee was sentenced to prison and over $500,000 in restitution in a plea agreement after being charged with embezzlement and filing a false tax return. We also resolved 568 hotline complaints and closed 7 investigations, and our work resulted in 21 persons referred for criminal prosecution.

Finally, in addition to the uncertainty and financial hardships caused by the COVID-19 pandemic, we have seen widespread concern in our country over the past several months regarding systemic discrimination and racial injustice and have witnessed a surge of protests condemning this injustice. How we promote inclusion and equity has been an ongoing topic of conversation and action within the OIG. We know that

the wide-ranging experiences and perspectives that each staff member has brought to our organization are essential to our ability to produce thorough, insightful, and comprehensive products and services for our stakeholders. I look forward to continuing our efforts in this area as we endeavor to ensure that we have a workplace that is inclusive and a workforce that is diverse and engaged.

I am deeply thankful to and inspired by the OIG staff, who have shown incredible resourcefulness and resilience throughout the pandemic as we continue to pursue our important oversight mission.

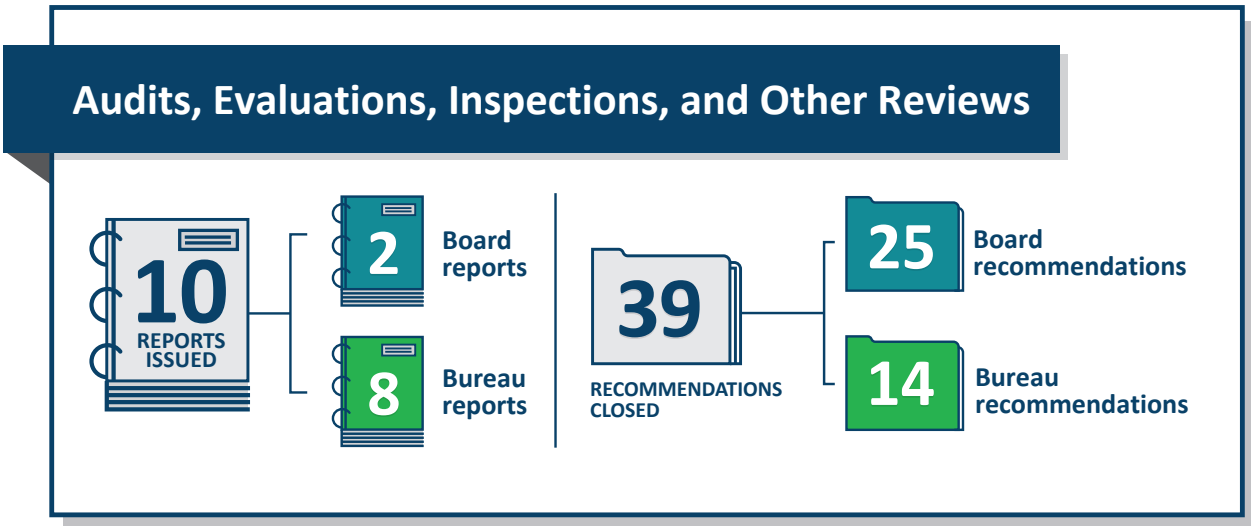
Sincerely,
Mark Bialek

Inspector General
October 30, 2020

# Contents

# Highlights

We continued to promote the integrity, economy, efficiency, and effectiveness of the programs and operations of the Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection. The following are highlights, in chronological order, of our work during this semiannual reporting period.




## The Bureau's Periodic Monitoring Program

The Bureau can improve its supervisory monitoring program by expanding the number of nondepository institutions it will monitor, better tailoring the resources dedicated to monitoring based on risk, and hiring additional examiners. In addition, the Division of Supervision, Enforcement and Fair Lending (SEFL) can improve its efforts to conduct and document periodic monitoring activities.

## The Board's Suitability and Personnel Screening Process

The results of our data analytics testing showed that the Board's suitability and personnel screening processes are operating effectively and in accordance with the agency's policies. We conducted this testing as part of our 2020 audit of the Board's information security program.

## The Bureau's Budget and Funding Processes

The Bureau designed and implemented controls over its budget and funding request processes and the Board designed and implemented controls over the funds transfer process. In addition, the Bureau generally complied with legal requirements to produce certain budget- and funding-related information and report it to certain stakeholders.

## The Bureau's Legal Enclave

A device that controls access to the environment housing the Bureau's Legal Enclave has a significant weakness, resulting in several security vulnerabilities. In addition, the Bureau had not appropriately tested contingency planning activities for the device. Further, technologies in the Legal Enclave have several security misconfigurations and security weaknesses, which increase the risk of unauthorized data access and system misuse.

## The Bureau's Personnel Security Program

The Bureau's Personnel Security Office (PSO) does not have measurable objectives to evaluate its performance related to reducing its adjudication backlog, nor does it have a plan with measurable objectives to manage the background investigation process going forward. In addition, the PSO does not have processes to reconcile its personnel security data. Because the Bureau needs time to address recent internal and external reviews of the program, we suspended our full evaluation after alerting the Bureau of our findings.

## The Board's Approach to the Cybersecurity Supervision of Large Institution Supervision Coordinating Committee Firms

The Board's approach to cybersecurity supervision of Large Institution Supervision Coordinating Committee (LISCC) firms continues to evolve and can be enhanced by clarifying roles and responsibilities, better defining how cybersecurity supervisory activities inform relevant ratings, enhancing its approach to cybersecurity training, and improving its guidance and training for reporting cybersecurity events.


## Three First NBC Executives and One Individual Indicted, Three Others Pleaded Guilty, in Fraud Against Failed $5 Billion Bank

The former president, chief credit officer, and executive vice president of First NBC Bank—the $5 billion bank that failed in April 2017—were indicted for an alleged fraud scheme totaling hundreds of millions of dollars and involving at least seven coconspirators. Three of those coconspirators pleaded guilty in recent months to fraud conspiracy charges and face up to 5–30 years in prison, another was indicted along with the executives, and the remaining three pleaded guilty to fraud conspiracy charges in 2018 and 2019.

## Five Individuals Charged in Paycheck Protection Program Fraud Cases Attempting $46 Million in Forgivable Loans

In four separate cases, five individuals were charged for allegedly filing fraudulent applications seeking a combined $46 million in forgivable loans guaranteed by the U.S. Small Business Administration (SBA)

through the Coronavirus Aid, Relief, and Economic Security (CARES) Act Paycheck Protection Program (PPP). The individuals sought loans for companies they owned or worked for by falsifying application information, such as payroll expenses and tax information. To date, the government has recovered about $4 million of the $7.5 million the defendants received.

## Former Whitaker Bank President Pleaded Guilty to Embezzlement

The former president of Whitaker Bank in Kentucky pleaded guilty to embezzling or misapplying more than $50,000 of the bank's funds. He was also charged by way of information, waiving his right to indictment by a federal grand jury.

## Former Crown Bank Executive Pleaded Guilty to Bank Fraud

The former chief executive officer (CEO) of Crown Bank in Minnesota pleaded guilty to one count of wire fraud and one count of filing a false income tax return. From 2012 to 2017, he made false entries to conduct transactions for his own benefit without notifying the bank's board of directors and without properly notifying the appropriate state and federal regulatory agencies. He also filed false tax returns failing to disclose his embezzled earnings, resulting in a tax loss of about $285,200.

## Former SmartBank Vice President Sentenced for Embezzlement Scheme

The former vice president of loan operations for SmartBank, a state member bank, was sentenced to 15 months in prison, 4 years' supervised release, and $516,630 in restitution in a plea agreement after being charged with one count of embezzlement and one count of filing a false tax return. From about 2013 to 2018, she manipulated SmartBank's general ledger to fund the issuance of 60 cashier's checks totaling nearly $360,000 for her own benefit and failed to report the embezzled funds as income on her tax returns.

# Introduction

Established by Congress, we are the independent oversight authority for the Board and the Bureau. In fulfilling this responsibility, we conduct audits, evaluations, investigations, and other reviews related to Board and Bureau programs and operations. By law, offices of inspector general are not authorized to perform agency program functions.

In accordance with the Inspector General Act of 1978, as amended (5 U.S.C. app. 3), our office has the following responsibilities:

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

Congress has also mandated additional responsibilities that influence our 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 (12 U.S.C. § 1831o(k)), outlines certain review and reporting obligations for our office when a state member bank failure occurs. The nature of those review and reporting requirements depends on the size of the loss to the Deposit Insurance Fund.
- 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. We perform 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 Bureau's information security programs and practices, including testing the effectiveness of security controls and practices for selected information systems.

- The Payment Integrity Information Act of 2019 (PIIA; 31 U.S.C. §§ 3351–58) requires agency heads to periodically review and identify programs and activities that may be susceptible to significant improper payments. The Bureau has determined that its Consumer Financial Civil Penalty Fund is subject to the PIIA. The PIIA requires us to determine each fiscal year whether the agency is in compliance with the act.
- Section 211(f) of the Dodd-Frank Act (12 U.S.C. § 5391(f)) requires that we review and report on the Board's supervision of any covered financial company that is placed into receivership. We are 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 must report annually about the IGs' concerns and recommendations, as well as issues that may apply to the broader financial sector. CIGFO can also 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 us to conduct periodic risk assessments and audits of the Board's and the Bureau'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 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 Bureau.

1. CIGFO comprises the IGs of the Board and the Bureau, 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 Bureau and (2) to make recommendations to promote uniformity in the supervision of financial institutions.

- The Digital Accountability and Transparency Act of 2014 (DATA Act; 31 U.S.C. § 6101 note) requires agencies to report financial and payment data in accordance with data standards established by the U.S. Department of the Treasury and the Office of Management and Budget. The Bureau 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 us to review a statistically valid sample of the data submitted by the agency and report on its completeness, timeliness, quality, and accuracy and on the agency's implementation and use of the data standards.

# Pandemic Response Oversight

Beginning in mid-March, the Board quickly took a series of actions to support aspects of the nation's economy that were affected by the COVID-19 pandemic. The Board has adjusted target interest rates and used its emergency lending authority under section 13(3) of the Federal Reserve Act to ensure liquidity in financial markets and provide lending support to various sectors of the economy. Signed into law on March 27, 2020, the CARES Act authorized, among other things, Treasury's investment in facilities established by the Board and mandated public reporting of information about the government's pandemic response. Significant coordination among the Board, Treasury, and numerous other federal agencies will be necessary as the Board continues its pandemic response.

As the OIG for the Board, we are initially focused on

- governance and controls to ensure consistent execution of the Board's programs by the Federal Reserve Banks designated to put them into action, as well as vendor activities to execute program objectives
- coordination activities among the Reserve Banks or the designated program manager to execute, monitor, and improve that execution over time
- data aggregation and validation, particularly before program-related information is shared with the public or congressional stakeholders
- the monitoring and tracking of unique features associated with specific programs, such as
    - the forgiveness of PPP loans and its effect on the security interests under the Paycheck Protection Program Liquidity Facility
    - the limits associated with the Primary and Secondary Market Corporate Credit Facilities
    - Treasury's equity investments in specific CARES Act programs

We have initiated our first pandemic response–related audit, which will assess the Board's processes for aggregating and reporting lending information related to its CARES Act programs, including the data validation processes it uses to ensure that the information is current, accurate, and complete. We will continue to actively collect and analyze information in these and other areas to identify emerging risks with a view to initiating additional targeted audits or evaluations.

In addition to oversight related to the Board's facilities and related activities directly supporting the economy, we are also actively monitoring

- measures taken to encourage financial institutions to lend consistent with the spirit and intent of specific lending programs, such as the PPP
- the Board's efforts to review community banking organizations' participation in pandemic response programs to confirm that participation is commensurate with an institution's governance, risk management, and internal control capabilities
- the extent to which pandemic response lending efforts reach intended recipients and serve intended communities
- specific measures to encourage and foster more lending during the pandemic response

Throughout these activities, the security of Board data, communications, networks, and systems that are essential to the Board's and the Federal Reserve System's pandemic response are of paramount importance. We have expanded our testing of critical information technology (IT) systems and broadened the scope of our security control reviews previously planned to meet FISMA requirements. We are also coordinating directly with various IT organizations throughout the System, including those Reserve Banks that provide services to the Board and across the System.

Further, we are dedicated to identifying and investigating potential fraud affecting the facilities and other Board programs central to the pandemic response. To do so, we leverage our relationships with various federal law enforcement organizations, U.S. attorney's offices, and components of the U.S. Department of Justice (DOJ). Already, we have helped bring charges in four cases against five individuals who attempted to defraud the government of more than $46 million in forgivable PPP loans.

Finally, we are focused on additional oversight activities as the OIG for the Bureau. Although the programs and operations of the Bureau are not directly provided funding by the CARES Act or tasked with CARES Act requirements, the agency plays a vital role in protecting consumers from pandemic-related consumer financial fraud and abuse. In this regard, we actively oversee Bureau supervisory activity and monitor the Bureau's consumer complaint and consumer education activities.

As we conduct these oversight activities, we will continue to work closely with other IGs, the U.S. Government Accountability Office, the Pandemic Response Accountability Committee (PRAC), and our congressional committees of jurisdiction in order to efficiently deploy oversight resources where they are most needed.

# Audits, Evaluations, Inspections, and Other Reviews

Audits assess aspects of the economy, efficiency, and effectiveness of Board and Bureau programs and operations. For example, we oversee audits of the Board's financial statements and conduct audits of (1) the efficiency and effectiveness of the Board's and the Bureau'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. Our audits are performed in accordance with *Government Auditing Standards*, which is issued by the comptroller general of the United States.

Evaluations and inspections also assess aspects of the economy, efficiency, and effectiveness of Board and Bureau programs and operations. Evaluations are generally focused on the effectiveness of specific programs or functions; we also conduct our legislatively mandated reviews of failed financial institutions supervised by the Board as evaluations. Inspections are often narrowly focused on particular issues or topics and provide time-critical analyses. Our evaluations and inspections are performed according to *Quality Standards for Inspection and Evaluation*, which is issued by the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

Other reviews may include risk assessments, data analytics or other testing, and program and operational reviews that are not performed in accordance with audit or evaluation standards.

The information below summarizes our audits, evaluations, and other reviews completed during the reporting period.

## Board of Governors of the Federal Reserve System

### Results of Data Analytics Testing of the Board's Suitability and Personnel Screening Processes

**2020-IT-B-016R** **July 13, 2020**

As part of our 2020 audit of the Board's information security program, which we performed to meet FISMA requirements, we conducted data analytics testing of the Board's suitability and personnel screening processes.

The results of our testing show that the Board's suitability and personnel screening processes are operating effectively and in accordance with the agency's policies. We will use the results of this testing to support our response to specific questions in the U.S. Department of Homeland Security's *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. We did not make any recommendations.

### The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced

**2020-SR-B-019** **September 30, 2020**

Cybersecurity threats to financial institutions are becoming more frequent and sophisticated. We assessed the effectiveness of the Board's cybersecurity supervision approach for LISCC firms—the largest, most systemically important domestic and foreign financial institutions supervised by the Board.

The Board's approach to cybersecurity supervision of LISCC firms continues to evolve and can be enhanced. The Board can strengthen its governance of LISCC firm cybersecurity supervision by clarifying the roles and responsibilities of the groups involved in supervision and planning activities and better defining how cybersecurity supervisory activities inform relevant ratings. The Board can also enhance its approach to cybersecurity training to ensure examiners keep their skills up to date. Additionally, the Board can improve its guidance and training for reporting cybersecurity events.

Our report contains recommendations designed to enhance the effectiveness of the Board's cybersecurity supervision of LISCC firms. The Board concurred with our recommendations.

## Bureau of Consumer Financial Protection

### Fiscal Year 2019 Risk Assessment of the Bureau's Government Travel Card Program

**April 1, 2020**

Bureau travel cards were used for 48,818 purchases totaling $11.1 million in fiscal year 2019. We conducted a risk assessment of the Bureau's travel card program to determine the necessary frequency and scope of travel card audits.

The results of the risk assessment show that the risk of illegal, improper, or erroneous use in the Bureau's travel card program is *medium*. Although a risk level of *medium* means that illegal, improper, or erroneous use is likely to occur, such an occurrence would be expected to have a limited effect on current operations and long-term objectives. Nevertheless, the Bureau's Office of Travel and Relocation should continue

to take appropriate actions to ensure proper oversight of its program. We completed an audit of the Bureau's travel card program in September 2018; as a result, we did not include an audit of the travel card program in our 2020 audit plan.

## Fiscal Year 2019 Risk Assessment of the Bureau's Purchase Card Program

**April 1, 2020**

Bureau purchase cards were used for some 3,900 transactions worth $2.7 million from June 30, 2018, through September 30, 2019. We conducted a risk assessment of the Bureau's purchase card program to determine the necessary frequency and scope of purchase card audits.

The results of the risk assessment show that the risk of illegal, improper, or erroneous use in the Bureau's purchase card program is *low*. The results of the risk assessment should not be interpreted to mean that a lower-risk program is free of illegal, improper, or erroneous use or internal control deficiencies. An audit of the program may identify issues not previously noted in the risk assessment. We completed an audit of the Bureau's purchase card program in December 2018; as a result, we did not include an audit of the program in our 2020 annual audit plan.

## Independent Accountants' Report on the Bureau Civil Penalty Fund's 2019 Compliance With the Improper Payments Information Act of 2002, as Amended

**2020-FMIC-C-013** **April 20, 2020**

The Improper Payments Information Act of 2002, as amended (IPIA), requires agency heads to periodically review and identify all programs and activities that may be susceptible to significant improper payments. In addition, each fiscal year the IG of each agency is required to determine and report on whether the agency is in compliance with the act. We contracted with an independent public accounting firm to audit the Bureau Civil Penalty Fund's compliance with IPIA for fiscal year 2019. The contract required the audit to be performed in accordance with the auditing standards applicable to performance audits contained in *Government Auditing Standards*, which is 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 the contract and *Government Auditing Standards*.

The independent public accounting firm determined that the Bureau complied with the two applicable requirements of IPIA for fiscal year 2019 as they relate to the Civil Penalty Fund. Specifically, the firm found that the Bureau published an annual financial statement for the most recent fiscal year, posted that report on the agency website, and conducted a program-specific risk assessment in conformance with section 2(a) of IPIA. The other four IPIA requirements are not applicable to the Civil Penalty Fund because

the Bureau has determined that the fund is not susceptible to significant improper payments. The firm made no recommendations in its report.

## Testing Results for the Bureau's Plan of Action and Milestones Process

**2020-IT-C-014** **April 29, 2020**

As part of our 2019 audit of the Bureau's information security program, which we performed to meet FISMA requirements, we tested the Bureau's plan of action and milestones (POA&M) process, which the agency uses to document and remediate information security weaknesses. We did not report this information in our 2019 FISMA audit report because it did not affect the Bureau's information security program maturity rating. However, we believe that this information can assist with the Bureau's ongoing efforts to strengthen its risk management program and the maturity of its POA&M process.

We found that costs associated with remediating cybersecurity weaknesses listed in POA&Ms were not accurately accounted for. We also identified instances in which the status of cybersecurity weaknesses included in the Bureau's automated solution for POA&M management was inaccurate.

We made recommendations designed to strengthen the Bureau's process for managing cybersecurity weaknesses. The Bureau concurred with our recommendations.

## The Bureau Can Improve Its Periodic Monitoring Program to Better Target Risk and Enhance Training for Examiners

**2020-SR-C-015** **June 24, 2020**

SEFL monitors supervised institutions to maintain reasonably current information on their activities and to assess whether changes in risks to consumers or markets warrant changes in SEFL's planned supervisory activities. We evaluated SEFL's approach to monitoring supervised institutions for consistency with the Bureau's strategic plan and internal policies and procedures.

In July 2019, SEFL completed an internal initiative that included an assessment of its periodic monitoring program. Both SEFL's internal initiative and our independent assessment found that the agency can improve its supervisory monitoring program. Specifically, SEFL can expand the number of nondepository institutions it monitors, better tailor the resources dedicated to monitoring based on risk, and hire additional examiners to augment monitoring and the supervision program more broadly. Additionally, we determined that examiners did not consistently conduct or document periodic monitoring activities in accordance with SEFL's guidance. We also found that examiners may lack clarity on how periodic monitoring activities factor into SEFL's prioritization process and its broader supervision program. In January 2020, during the drafting of our report, SEFL finalized updates to its periodic monitoring policy,

which include expanding its monitoring program to cover additional nondepository institutions. We understand that SEFL is currently in the process of hiring additional examiners, in part to support its monitoring efforts.

Our report contains recommendations designed to further enhance the Bureau's periodic monitoring program. The Bureau concurred with our recommendations, and we closed one of those recommendations upon report issuance based on documentation provided by the Bureau.

## The Bureau's Budget and Funding Processes

**July 22, 2020**

The Bureau is funded primarily through transfers from the Board, averaging $487.1 million a year from fiscal year 2012 to fiscal year 2019. We assessed the design and implementation of the controls over the Bureau's budget processes as well as its compliance with applicable laws and regulations. The scope of our review focused on (1) the Bureau's budget formulation and execution processes, (2) the Bureau's process for requesting funds from the Board, and (3) the Board's process for transferring funds to the Bureau.

We determined that, to fulfill their respective Dodd-Frank Act responsibilities, the Bureau designed and implemented controls over its budget and funding request processes and the Board designed and implemented controls over the funds transfer process. In addition, the Bureau generally complied with legal requirements to produce certain budget- and funding-related information and report it to certain stakeholders.

## Technical Testing Results for the Bureau's Legal Enclave

**2020-IT-C-017R** **July 22, 2020**

As part of our 2019 audit of the Bureau's information security program, which we performed to meet FISMA requirements, we tested technical controls for the agency's Legal Enclave. The Legal Enclave includes systems and processes that are used to collect, store, process, and transmit critical information related to investigations and litigation.

We found a significant weakness on a device that controls access to the environment housing the Legal Enclave, resulting in several security vulnerabilities. Further, the Bureau had not appropriately tested contingency planning activities for the device. In addition, we identified several security misconfigurations and security weaknesses for technologies in the Legal Enclave, which increase the risk of unauthorized data access and system misuse. Although the Bureau was aware of several of these issues, it had not taken timely action to mitigate the risks; the Bureau had accepted specific risks related to certain vulnerabilities in the Legal Enclave but had not formally documented its rationale for these decisions.

We made recommendations designed to further assist the agency in its ongoing efforts to strengthen technical security controls. The Bureau concurred with our recommendations.

## Results of Scoping and Suspension of the Evaluation of the Bureau's Personnel Security Program

**2020-MO-C-018** **August 17, 2020**

The Bureau's PSO manages the background investigation process for its federal employees and contractors in coordination with the U.S. Office of Personnel Management. We initiated an evaluation to assess the efficiency and effectiveness of the Bureau's personnel security program. However, the Bureau recently completed an internal review of the program, which identified other areas for improvement, and the U.S. Office of Personnel Management launched a separate review in March 2020. Because the Bureau needs time to fully address the results from these additional reviews, we suspended our evaluation.

As part of our scoping efforts before we suspended our evaluation, we found that the PSO does not have measurable objectives to evaluate its performance related to reducing its adjudication backlog, nor does it have a plan with measurable objectives to manage the background investigation process going forward. In addition, we found that the PSO does not have processes to reconcile its personnel security data.

We made recommendations designed to strengthen the Bureau's performance monitoring capabilities for the personnel security program and improve processes related to data accuracy. The Bureau generally concurred with our recommendations.

# Failed State Member Bank Reviews

Section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Act, requires that we review and report within 6 months on Board-supervised financial institutions whose failure results in a material loss to the Deposit Insurance Fund. Section 38(k) also requires that we (1) semiannually report certain information on financial institutions that incur nonmaterial losses to the Deposit Insurance Fund and (2) conduct an in-depth review of any nonmaterial losses to the Deposit Insurance Fund that exhibit unusual circumstances. No state member bank failures occurred during this reporting period.

Please refer to table A-2, which outlines the progress to address recommendations associated with prior failed bank reviews.

# Investigations

Our Office of Investigations investigates criminal, civil, and administrative wrongdoing by Board and Bureau employees as well as alleged misconduct or criminal activity that affects the Board's or the Bureau's ability to effectively supervise and regulate the financial community. We operate 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. Our investigations are conducted in compliance with *Quality Standards for Investigations*, issued by CIGIE, and *Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority*.

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

## 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 (state member banks). 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 senior officials 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.

### Three First NBC Executives Indicted, Three Other Individuals Pleaded Guilty, in Fraud Against Failed $5 Billion Bank

Fraud cases involving First NBC Bank—the $5 billion bank that failed in April 2017—saw several new developments this reporting period, adding to cases reported in our prior semiannual reports to Congress.

Based in New Orleans, the bank was a subsidiary of First NBC Bank Holding Company, a Board-supervised bank holding company.

## Three First NBC Executives and One Borrower Indicted for Fraud

Three First NBC Bank executives—President Ashton Ryan, Chief Credit Officer William Burnell, and Executive Vice President Robert Calloway—were indicted for defrauding First NBC Bank. Frank Adolph, a borrower, was also indicted for defrauding the bank. If convicted, the four defendants face, for each of the charged counts, up to 30 years in prison, a fine of $1 million or the greater of twice the gain to a defendant or twice the loss to any victim, up to 5 years' supervised release, and a $100 mandatory special assessment. An indictment is merely an accusation, and the guilt of the defendants must be proven beyond a reasonable doubt.

From 2006 through April 2017, Ryan, Burnell, Calloway, and Adolph allegedly conspired to defraud First NBC Bank through a variety of schemes. Specifically, the four and others conspired to defraud the bank by disguising the financial status of certain borrowers and their troubled loans, concealing the true financial condition of the bank from the board, auditors, and examiners. In addition to Adolph, the other alleged conspiring borrowers were

- developer Gary Gibbs, developer Warren Treme, and hotel owner Arvind "Mike" Vira, who each recently pleaded guilty to conspiracy to commit bank fraud (see below)
- bank general counsel Gregory St. Angelo and business owner Kenneth Charity, who each pleaded guilty to conspiracy to commit bank fraud in July 2019
- contractor Jeffrey Dunlap, who pleaded guilty to conspiracy to commit bank fraud in October 2018

Calloway was Gibbs's loan officer, and Ryan served as the loan officer or oversaw the loan officers for all these borrowers. Burnell approved the risk rating for the borrowers' loans and was the gatekeeper tasked with protecting the safety and soundness of the bank's loan portfolio.

During the course of the conspiracy, Ryan, Burnell, and Calloway repeatedly extended new loans to the borrowers to cover their previous loans and overdraft fees, which they could not have otherwise paid. To hide this practice, Ryan, Burnell, and Calloway made false statements in loan documents and elsewhere about the purposes of the loans, the borrowers' abilities to repay the loans, and the sources of funds used to pay the loans. The new loans also prevented the borrowers from appearing on lists that Ryan and Burnell gave the bank's board each month, which would have highlighted that the borrowers were unable to make loan payments or had cash flow problems. When members of the board or the bank's outside auditors or examiners asked about loans to these borrowers, Ryan, Burnell, and Calloway made further false statements to conceal their activities.

As a result, the balance on these borrowers' loans continued to grow. By the time regulators closed First NBC Bank in April 2017, Gibbs owed the bank $123 million; St. Angelo, $46 million; Vira, $39 million; Dunlap, $22 million; Charity, $18 million; Adolph, $6 million; and Treme, $6 million. The bank's failure cost the Federal Deposit Insurance Corporation's (FDIC) Deposit Insurance Fund just under $1 billion.

All the while, Ryan, Burnell, and Calloway each received millions of dollars in compensation from First NBC Bank. Ryan also received personal benefits from three of the borrower relationships. Vira loaned millions to Ryan at the same time Vira was a borrower at the bank, and Ryan and Vira conspired to hide their business dealings from the board, auditors, and examiners. Treme was Ryan's partner in several businesses and real estate development projects, and Ryan used Treme's borrowing from the bank as a way to spend loan proceeds on Ryan's own projects. Even when parts of Ryan's business dealings with Vira and Treme were revealed to regulators, Ryan continued to conceal from regulators that he exercised authority over loans to Vira and Treme. Dunlap was a contractor for a business that Ryan and Treme ran, and Ryan used loan proceeds from Dunlap's business to benefit his own development project, Wadsworth Estates. Ryan never disclosed his business relationship with Dunlap to the board, auditors, or examiners. Burnell was aware of this business relationship and also never disclosed it to the board, auditors, or examiners.

This case was investigated by our office, the Federal Bureau of Investigation (FBI), and the FDIC OIG. It is being prosecuted by the U.S. Attorney's Office for the Eastern District of Louisiana.

## Developer Pleaded Guilty to Working With First NBC Executives in $123 Million Fraud

Gary Gibbs, a developer in Florida, pleaded guilty to conspiracy to defraud First NBC Bank. Gibbs faces up to 30 years in prison, a fine of the greater of twice the gain to the defendant or twice the loss to any victim, and up to 5 years' supervised release.

From about 2010 through April 2017, Gibbs had personal and business relationships with First NBC Bank. During that time, Gibbs and his business entities were regularly unable to pay existing loans or overdrafts on First NBC Bank accounts. Bank President Ashton Ryan, Chief Credit Officer William Burnell, and Executive Vice President Robert Calloway disguised Gibbs's and his entities' true financial condition by making new loans to pay his existing loans and cover his overdrafts and by falsely increasing the income of Gibbs's entities to hide the amount of money the entities were losing. Ryan, Burnell, and Calloway also falsified month-end reports to hide their activities from the bank's board, auditors, and examiners. Neither Ryan nor Calloway disclosed that Gibbs was considering defaulting on his loans or filing for bankruptcy, which would have revealed that Gibbs did not generate enough cash to pay his loans. By the time First NBC Bank failed in April 2017, the defendant and his entities owed the bank over $123 million.

This case was investigated by our office, the FBI, and the FDIC OIG. It is being prosecuted by the U.S. Attorney's Office for the Eastern District of Louisiana.

## Developer Pleaded Guilty to Conspiracy to Defraud First NBC Bank of $6 Million

Warren Treme, a developer in Louisiana, pleaded guilty to conspiracy to defraud First NBC Bank. Treme faces up to 30 years in prison, a fine of $1 million or the greater of twice the gain to the defendant or twice the loss to any victim, up to 5 years' supervised release, and a $100 mandatory special assessment.

From about 2008 through April 2017, Treme had personal and business relationships with First NBC Bank. He also co-owned several entities with Ashton Ryan, the bank's president. Because of this conflict of interest, Ryan should not have been involved with the Treme's loans. However, Ryan exercised authority over Treme's loans with William Burnell, the chief credit officer. Throughout his borrowing relationship at First NBC Bank, Treme lacked sufficient income and cash flow from his businesses to pay his loans and personal expenses. Ryan and Burnell disguised Treme's true financial condition by making new loans to pay his existing loans.

Further, Ryan and Burnell schemed to take $400,000 from Treme's business partners as part of a settlement. Rather than using the $400,000 to pay down an outstanding loan debt owed by Treme and his business partners, Ryan and Burnell gave $300,000 to Treme. Treme spent the money on gambling, a trip to the Caribbean, and expenses related to a real estate development company he co-owned with Ryan. During a subsequent bank board meeting, Ryan and Burnell falsely stated that the $300,000 was used to pay down the outstanding loan debt owed by Treme and his business partners.

This case was investigated by our office, the FBI, and the FDIC OIG. It is being prosecuted by the U.S. Attorney's Office for the Eastern District of Louisiana.

## New Orleans Hotel Owner Pleaded Guilty in Conspiracy to Defraud First NBC Bank

Arvind "Mike" Vira, a hotel owner and Louisiana resident, pleaded guilty to conspiracy to defraud First NBC Bank. Vira faces up to 5 years in prison, a fine of $250,000 or the greater of twice the gain to Vira or twice the loss to any victim, up to 3 years' supervised release, and a mandatory $100 special assessment.

From about April 2010 through April 2017, Vira had personal and business relationships with First NBC Bank. During that time, Ashton Ryan, the bank's president, allegedly acted as Vira's de facto loan officer and ensured that Vira received beneficial interest rates on savings accounts, checking accounts, and loans. In return, Vira allegedly agreed to make loans to Ryan and to keep the loans hidden from bank employees at Ryan's direction. Ryan likewise concealed this relationship from others at the bank and from FDIC examiners. Further, at Ryan's behest, Vira inflated his own assets on financial statements that

he submitted to First NBC Bank in support of his loans. As a result, Vira and Ryan allegedly were able to defraud the bank by using nominee loans to funnel money to Ryan without bank or regulatory scrutiny.

This case was investigated by our office, the FBI, and the FDIC OIG. It is being prosecuted by the U.S. Attorney's Office for the Eastern District of Louisiana.

## Five Individuals Charged in Pandemic-Related Fraud Attempting $46 Million in Forgivable PPP Loans

In four separate cases, five individuals were charged for allegedly filing fraudulent loan applications seeking a combined $46 million in forgivable loans guaranteed by the SBA through the CARES Act PPP.

### California Man Charged in $22 Million PPP Fraud

A California man was charged with bank fraud for allegedly participating in a scheme to file fraudulent PPP loan applications seeking over $22 million on behalf of several businesses.

According to the allegations, the defendant submitted nine fraudulent loan applications. In support of the applications, he made numerous false and misleading statements about the companies' respective business operations and payroll expenses. The applications were also supported by fake documents, including falsified federal tax filings, and failed to disclose his prior criminal record. He received more than $1 million from one of the approved PPP loan applications.

This case was investigated by our office, the FBI, and the SBA OIG. It is being prosecuted by the U.S. Attorney's Office for the Northern District of California.

### Owner of IT Services Company Indicted in $13 Million PPP Fraud

The owner, president, and CEO of an IT services company in Massachusetts was indicted for allegedly filing fraudulent PPP loan applications seeking more than $13 million. Specifically, he was charged with four counts of wire fraud and one count of making a false statement to a financial institution.

According to the allegations, in the loan applications, filed during April–June 2020, the defendant misrepresented payroll expenses, exaggerated employee counts, and falsely certified that his employees' primary residence was in the United States. He also submitted falsified documentation in support of his PPP applications. According to the indictment, he received over $2 million of the $13 million in PPP funds he applied for.

This case was investigated by our office, the FDIC OIG, the FBI, the Internal Revenue Service (IRS) Criminal Investigation (CI), and the SBA OIG. It is being prosecuted by the DOJ and the U.S. Attorney's Office for the District of Massachusetts.

### Business Owners Charged in $7 Million PPP Fraud

Two brothers, owners of multiple businesses, were charged with wire fraud conspiracy for their alleged participation in a scheme to file fraudulent PPP loan applications seeking nearly $7 million.

According to the allegations, the brothers conspired to submit and submitted at least eight fraudulent PPP loan applications. In support of their applications, they made numerous false and misleading statements about their companies' respective business operations and payroll expenses. Further, the fraudulent loan applications were supported by fake documents, including falsified federal tax filings. Finally, the defendants used fraudulently obtained loan proceeds on personal expenses, including securities, home improvements, and a vehicle. To date, the government has seized over $400,000 of the more than $600,000 that the defendants obtained.

This case was investigated by our office, the FDIC OIG, the FBI, the SBA OIG, and the Federal Housing Finance Agency (FHFA) OIG. It is being prosecuted by the DOJ and the U.S. Attorney's Office for the Western District of New York.

### Florida Man Charged in $3.9 Million PPP Fraud

A Florida man was charged in a scheme to fraudulently obtain $3.9 million in PPP loans and use those funds, in part, to purchase a Lamborghini for himself. He was charged with one count of bank fraud, one count of making false statements to a financial institution, and one count of engaging in transactions in unlawful proceeds. Authorities seized $3.4 million from his bank accounts and the $318,000 sports car at the time of his arrest.

According to the allegations, the defendant sought some $13.5 million in PPP loans through applications to an insured financial institution on behalf of different companies. The applications made numerous false and misleading statements about the companies' respective payroll expenses. The financial institution approved and funded about $3.9 million in loans. Within days of receiving the PPP funds, he purchased a 2020 Lamborghini Huracán, which he registered jointly in his name and in the name of one of his companies. Soon after, he failed to make the payroll payments he claimed on his loan applications. He did, however, make purchases at luxury retailers and resorts in Miami Beach.

This case was investigated by our office, the FDIC OIG, the IRS CI, the SBA OIG, and the U.S. Postal Inspection Service. It is being prosecuted by the DOJ and the U.S. Attorney's Office for the Southern District of Florida.

## Former Whitaker Bank President Pleaded Guilty to Embezzlement

A former president of Whitaker Bank, a state member bank in Kentucky, pleaded guilty to embezzling or misapplying more than $50,000 of the bank's funds. He was also charged by way of information, waiving

his right to indictment by a federal grand jury. He faces up to 30 years in prison, a $1 million fine, 5 years' supervised release, a $100 special assessment, and forfeiture and restitution.

The former president admitted that, from January 12, 2016, to August 13, 2018, he willfully misapplied assets of the bank. He admitted to stealing golf carts and other property from a foreclosed country club owned by Whitaker Bank. He also admitted to being reimbursed for personal expenses, including vehicle repairs, technology purchases for his family, and landscaping at his home, which he intentionally misreported as legitimate work expenses.

This case was investigated by our office, the FDIC OIG, and the FBI. It is being prosecuted by the U.S. Attorney's Office for the Eastern District of Kentucky.

## Former Crown Bank CEO Pleaded Guilty to Bank Fraud

A former CEO of Crown Bank in Minnesota pleaded guilty to one count of wire fraud and one count of filing a false income tax return. The bank is a subsidiary of Crown Bankshares, Inc., a bank holding company supervised by the Board. The former CEO was also the president and member of the board of directors of Crown Bankshares, Inc.

The former CEO fraudulently used the bank's funds to pay substantial personal debts and expenses and altered records to hide his activity. From 2012 to 2017, he made false entries to conduct transactions for his own benefit without notifying the bank's board of directors and without properly notifying the appropriate state and federal regulatory agencies. He also allegedly deceived investors about a pending deal for another bank to acquire Crown Bank at a premium when there was no agreement with the bank in question. Further, he allegedly filed a false income tax return for 2016 by not disclosing $720,000 in income from transactions designed to look like loans or stock purchases from third parties but that were instead going directly to himself. The false tax return resulted in a tax loss of about $285,200.

This case was investigated by our office, the FBI, the FDIC OIG, and the IRS CI. It is being prosecuted by the U.S. Attorney's Office for the District of Minnesota in Minneapolis.

## Former First Midwest Bank Vice President Sentenced for Embezzlement

A former vice president and market sales manager at First Midwest Bank, a state member bank in Illinois, was sentenced to 6 months in federal prison after pleading guilty to an information charging him with one count of embezzlement from a financial institution. He was also sentenced to 2 years' supervised release and ordered to pay $125,457 in restitution and a $100 special assessment. As a result of his conviction, he is prohibited from employment by any federally insured depository institution.

From around November 2016 to February 2019, the former vice president used his position of private trust on 131 occasions to cause First Midwest Bank to debit a total of $125,457 from its general ledger accounts based on his false and fraudulent representations that, among other things, the requested funds were being credited to bank customers or were used to fund promotional and charitable events in the community. He attempted to conceal his embezzlement by causing First Midwest Bank to deposit the general ledger funds into about 15 different bank accounts under his control, including accounts in his name, in the names of his family members, and in the names of two individuals without their knowledge or authorization. He obtained the two individuals' personal information by using the bank's computers to access their accounts.

This investigation was conducted by our office. It was prosecuted by the U.S. Attorney's Office for the Northern District of Illinois.

## Former SmartBank Vice President of Loan Operations Sentenced for Embezzlement

A former vice president of loan operations for SmartBank, a state member bank based in Tennessee, was sentenced to 15 months in prison, 4 years' supervised release, and $516,630 in restitution in a plea agreement after being charged with one count of embezzlement and one count of filing a false tax return.

The former vice president of loan operations' responsibilities included overseeing the entry of financial transactions in SmartBank's general ledger system. From about 2013 to 2018, she manipulated SmartBank's general ledger to fund the issuance of 60 cashier's checks totaling nearly $360,000. About $150,000 was deposited into her bank account and used to pay credit card bills, auto loan payments, and other living expenses. The rest, including about $27,000 used to purchase a travel trailer, supported her lifestyle. Further, she manipulated SmartBank's general ledger system to fraudulently reduce her home mortgage loan by more than $200,000 and her parents' home mortgage loan by $46,000. In addition, she failed to report the embezzled funds as income on her tax returns.

This investigation was conducted by our office, the FBI, the FHFA OIG, and the IRS CI. It was prosecuted by the U.S. Attorney's Office for the Eastern District of Tennessee.

## Former Arvest Bank Employee Pleaded Guilty for Embezzlement Scheme

A former mortgage sales assistant at Arvest Bank, a state member bank in Oklahoma, pleaded guilty to one count of fraud and related activity in connection with access devices.

In 2019, she used her position to embezzle almost $25,000 from an elderly customer of the bank. She created a series of debit card transactions and false entries to cover up the scheme. As part of the plea

deal, she will be required to repay the funds to the victim and prohibited from working in the banking industry. She also faces up to 10 years in prison and a $250,000 fine.

This investigation was conducted by our office. It was prosecuted by the U.S. Attorney's Office for the Northern District of Oklahoma.

### Former Arvest Bank Branch Manager Sentenced for Embezzlement Scheme

A former branch manager at Arvest Bank, a state member bank in Arkansas, was sentenced to one weekend in jail, 2 years' supervised release, and a $100 special assessment after pleading guilty to making false entries in bank records. As a result of her conviction, she is prohibited from employment by any federally insured depository institution.

The former branch manager misused her authority to conduct nearly $22,000 in fraudulent transactions in bank customers' accounts. She attempted to conceal her activity by creating bogus transaction documents showing funds moving between the customers' accounts when in reality she was embezzling the funds.

This investigation was conducted by our office. It was prosecuted by the U.S. Attorney's Office for the Eastern District of Arkansas.

## Bureau of Consumer Financial Protection

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

Our investigations concerning the Bureau's responsibilities typically involve allegations that company directors or officers provided falsified business data and financial records to the Bureau, lied to or misled examiners, or obstructed examinations in a manner that may have affected the Bureau's ability to carry

out its supervisory responsibilities. Such activity may result in criminal violations, such as false statements or obstruction of examinations.

Other than the material found in appendix B, no publicly reportable developments occurred during this reporting period in our Bureau-related investigations.

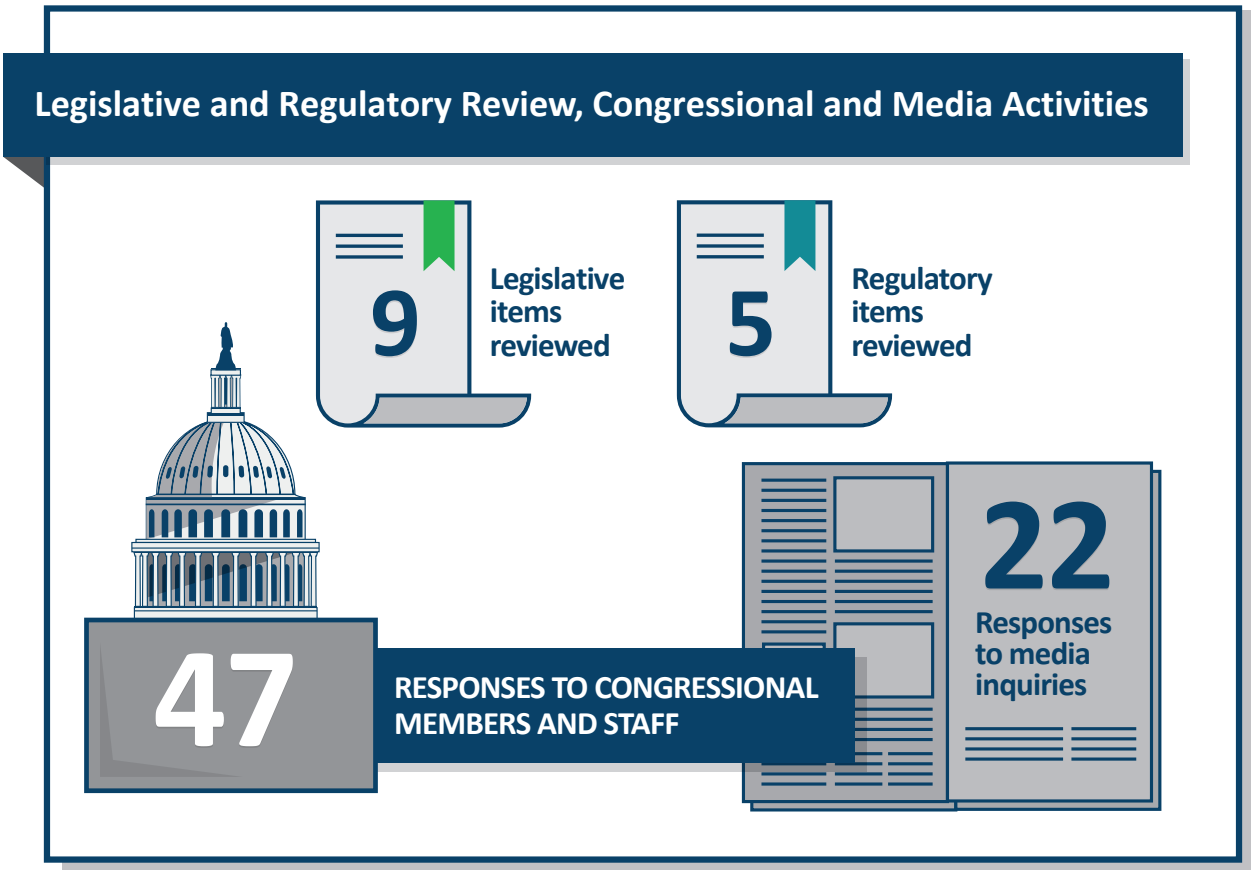
# Hotline

The OIG Hotline helps people report fraud, waste, abuse, and mismanagement related to the programs or operations of the Board and the Bureau. Hotline staff can be reached by phone, web form, fax, or mail. We review all incoming hotline communications, research and analyze the issues raised, and determine how best to address the complaints.

During this reporting period, the OIG Hotline received 571 complaints. Complaints within our purview are evaluated and, when appropriate, referred to the relevant component within the OIG for audit, evaluation, investigation, or other review. Some complaints convey concerns about matters within the responsibility of other federal agencies or matters that should be addressed by a program or operation of the Board or the Bureau. We refer such complaints to the appropriate federal agency for evaluation and resolution.

We continue to receive many noncriminal consumer complaints regarding consumer financial products and services. For these matters, we typically refer complainants to the consumer group of the appropriate federal regulator for the institution involved, such as the Bureau's Office of Consumer Response, Federal Reserve Consumer Help, or other law enforcement agencies as appropriate. In addition, we receive misdirected complaints regarding COVID-19 pandemic–related programs and operations. In such cases, we refer either the individual or the original complaint to the appropriate agency for further evaluation.

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




## Legislative and Regulatory Review

Our Office of Legal Services is the independent legal counsel to the IG and OIG staff. Legal Services provides comprehensive legal advice, research, counseling, analysis, and representation in support of our 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 us, the Board, or the Bureau.

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 Bureau's programs and operations. During this reporting period, Legal Services reviewed 9 legislative items and 5 regulatory items.

## Congressional and Media Activities

We communicate and coordinate with various congressional committees on issues of mutual interest. During this reporting period, we provided 47 responses to congressional members and staff concerning the Board and the Bureau. Additionally, we responded to 22 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.

As part of the OIG community, we are proud to be part of the Oversight.gov effort. Oversight.gov is a searchable website containing the latest public reports from federal OIGs. It provides access to over 17,000 reports, detailing for fiscal year 2020 alone over $26 billion in potential savings and over 8,000 recommendations to improve programs across the federal government.

The IG serves as a member of CIGIE's Legislation Committee and Technology Committee and is the vice chair of the Investigations Committee. The Legislation Committee is the central point of information for legislative initiatives and congressional activities that may affect the OIG community, such as proposed cybersecurity legislation that was reviewed during the reporting period. The Technology Committee facilitates effective IT audits, evaluations, and investigations and provides a forum for the expression of the OIG community's perspective on governmentwide IT operations. The Investigations Committee advises the OIG community on issues involving criminal investigations, criminal investigations personnel, and criminal investigative guidelines. The IG is also a member of CIGIE's Diversity, Equity, and Inclusion Working Group.

In addition, the IG serves on CIGIE's PRAC, which coordinates oversight of federal funds authorized by the CARES Act and the COVID-19 pandemic response. The IG is the vice chair of the PRAC Investigations Subcommittee and is a member of the PRAC Financial Institutions Oversight Subcommittee.

Our associate inspector general for information technology, as the chair of the Information Technology Committee of the Federal Audit Executive Council, works with IT audit staff throughout the OIG community and reports to the CIGIE Technology Committee on common IT audit issues.

Our associate inspector general for legal services and our Legal Services staff attorneys are members of the Council of Counsels to the Inspector General, and our quality assurance staff founded and are current members of the Federal Audit Executive Council's Quality Assurance Work Group.

# Peer Reviews

Government auditing and investigative standards require that our audit and investigative units be reviewed by a peer OIG organization every 3 years. In addition, CIGIE has launched a pilot program in which inspection and evaluation units are peer reviewed by an external team every 3 years.

The Inspector General Act of 1978, as amended, requires that OIGs provide in their semiannual reports to Congress information about (1) the most recent peer reviews of their respective organizations and (2) their peer reviews of other OIGs conducted within the semiannual reporting period. The following information addresses these requirements.

- In September 2017, the National Science Foundation OIG completed a 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.[3]
- In August 2019, the OIG for the Tennessee Valley Authority 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.
- In November 2019, a team comprising the OIGs for the FHFA, the Tennessee Valley Authority, and the U.S. Department of Labor completed a peer review of our evaluations policies and procedures as well as a subset of evaluations completed. No rating was assigned because the review was conducted as part of a pilot program. The review found that we sufficiently met CIGIE's *Quality Standards for Inspection and Evaluation*. There were no report recommendations, but the review team did identify suggestions to improve our compliance with internal policies and procedures.

See our website for peer review reports of our organization.

3. The National Archives and Records Administration completed a peer review of our audit organization after the close of the semiannual reporting period, in October 2020. We received a peer review rating of *pass*.

# Appendix A: Statistical Tables

## Table A-1. Audit, Inspection, and Evaluation Reports and Other Reviews Issued to the Board During the Reporting Period

| Report title | Type of report |
|---|---|
| Results of Data Analytics Testing of the Board's Suitability and Personnel Screening Processes | Data analytics testing |
| The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced | Evaluation |
| Total number of audit reports: 0<br>Total number of evaluation reports: 1<br>Total number of other reviews: 1 | |

## Table A-2. OIG Reports to the Board With Recommendations That Were Open During the Reporting Period

| Report title | Issue date | Recommendations | | | Status of recommendations | | |
|---|---|---|---|---|---|---|---|
| | | Number | Management agrees | Management disagrees | Last follow-up date | Closed | Open |
| The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control | 09/13 | 1 | 1 | 0 | 03/20 | 0 | 1 |
| Review of the Failure of Waccamaw Bank | 03/15 | 5 | 5 | 0 | 07/20 | 5 | 0 |
| 2016 Audit of the Board's Information Security Program | 11/16 | 9 | 9 | 0 | 10/19 | 8 | 1 |
| Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities | 11/16 | 11 | 11 | 0 | 09/20 | 11 | 0 |
| The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing | 04/17 | 8 | 8 | 0 | 09/20 | 4 | 4 |
| 2017 Audit of the Board's Information Security Program | 10/17 | 9 | 9 | 0 | 10/19 | 3 | 6 |

See notes at end of table.

| Report title | Issue date | Recommendations | | | Status of recommendations | | |
|---|---|---|---|---|---|---|---|
| | | Number | Management agrees | Management disagrees | Last follow-up date | Closed | Open |
| The Board's Organizational Governance System Can Be Strengthened | 12/17 | 14 | 14 | 0 | 09/20 | 10 | 4 |
| Security Control Review of the Board's Public Website (nonpublic) | 03/18 | 7 | 7 | 0 | 06/20 | 4 | 3 |
| Security Control Review of the Board Division of Research and Statistics' General Support System (nonpublic) | 09/18 | 9 | 9 | 0 | 03/20 | 7 | 2 |
| 2018 Audit of the Board's Information Security Program | 10/18 | 6 | 6 | 0 | 10/19 | 1 | 5 |
| The Board Can Strengthen Information Technology Governance | 11/18 | 6 | 6 | 0 | 06/20 | 3 | 3 |
| The Board's Currency Shipment Process Is Generally Effective but Can Be Enhanced to Gain Efficiencies and to Improve Contract Administration | 12/18 | 8 | 8 | 0 | 09/20 | 3 | 5 |
| The Board Can Strengthen Controls Over Its Academic Assistance Program | 12/18 | 9 | 9 | 0 | 09/20 | 9 | 0 |
| The Board Can Take Additional Steps to Advance Workforce Planning | 03/19 | 2 | 2 | 0 | 09/20 | 2 | 0 |

See notes at end of table.

| Report title | Issue date | Recommendations | | | Status of recommendations | | |
|---|---|---|---|---|---|---|---|
| | | Number | Management agrees | Management disagrees | Last follow-up date | Closed | Open |
| Leveraging Certain Strategies May Help the Board Timely Implement and Sustain Enterprisewide Workforce Planning | 09/19 | 2 | 2 | 0 | 06/20 | 2 | 0 |
| The Board Can Enhance Its Internal Enforcement Action Issuance and Termination Processes by Clarifying the Processes, Addressing Inefficiencies, and Improving Transparency | 09/19 | 6 | 6 | 0 | 09/20 | 3 | 3 |
| The Board's Law Enforcement Operations Bureau Can Improve Internal Processes | 09/19 | 6 | 6 | 0 | 09/20 | 4 | 2 |
| 2019 Audit of the Board's Information Security Program | 10/19 | 6 | 6 | 0 | n.a. | 0 | 6 |
| The Board Should Finalize Guidance to Clearly Define Those Considered Senior Examiners and Subject to the Associated Postemployment Restriction | 03/20 | 1 | 1 | 0 | 9/20 | 0 | 1 |
| The Board's Oversight of Its Designated Financial Market Utility Supervision Program Is Generally Effective, but Certain Program Aspects Can Be Improved | 03/20 | 6 | 6 | 0 | n.a. | 0 | 6 |

See notes at end of table.

| Report title | Issue date | Recommendations | | | Status of recommendations | | |
|---|---|---|---|---|---|---|---|
| | | Number | Management agrees | Management disagrees | Last follow-up date | Closed | Open |
| The Board Can Enhance Certain Aspects of Its Enforcement Action Monitoring Practices | 03/20 | 1 | 1 | 0 | 09/20 | 0 | 1 |
| The Board Can Further Enhance the Design and Implementation of Its Operating Budget Process | 03/20 | 2 | 2 | 0 | n.a. | 0 | 2 |
| The Board Can Strengthen Its Oversight of the Protective Services Unit and Improve Controls for Certain Protective Services Unit Processes | 03/20 | 6 | 6 | 0 | n.a. | 0 | 6 |
| The Board Can Improve Its Contract Administration Processes | 03/20 | 13 | 13 | 0 | 9/20 | 0 | 13 |
| The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced | 09/20 | 10 | 10 | 0 | n.a. | 0 | 10 |

Note: 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.

n.a. not applicable.

## Table A-3. Audit, Inspection, and Evaluation Reports and Other Reviews Issued to the Bureau During the Reporting Period

| Report title | Type of report |
|---|---|
| Fiscal Year 2019 Risk Assessment of the Bureau's Government Travel Card Program | Risk assessment |
| Fiscal Year 2019 Risk Assessment of the Bureau's Purchase Card Program | Risk assessment |
| Independent Accountants' Report on the Bureau Civil Penalty Fund's 2019 Compliance With the Improper Payments Information Act of 2002, as Amended | Audit |
| Testing Results for the Bureau's Plan of Action and Milestones Process | Testing |
| The Bureau Can Improve Its Periodic Monitoring Program to Better Target Risk and Enhance Training for Examiners | Evaluation |
| The Bureau's Budget and Funding Processes | Review |
| Technical Testing Results for the Bureau's Legal Enclave | Technical testing |
| Results of Scoping and Suspension of the Evaluation of the Bureau's Personnel Security Program | Suspended evaluation |
| Total number of audit reports: 1<br>Total number of evaluation reports: 1<br>Total number of other reviews: 6 | |

## Table A-4. OIG Reports to the Bureau With Recommendations That Were Open During the Reporting Period

| Report title | Issue date | Recommendations | | | Status of recommendations | | |
|---|---|---|---|---|---|---|---|
| | | Number | Management agrees | Management disagrees | Last follow-up date | Closed | Open |
| The CFPB Should Strengthen Internal Controls for Its Government Travel Card Program to Ensure Program Integrity | 09/13 | 14 | 14 | 0 | 09/20 | 14 | 0 |
| 2014 Audit of the CFPB's Information Security Program | 11/14 | 3 | 3 | 0 | 06/19 | 2 | 1 |
| The CFPB Should Continue to Enhance Controls for Its Government Travel Card Program | 06/16 | 9 | 9 | 0 | 09/20 | 9 | 0 |
| 2016 Audit of the CFPB's Information Security Program | 11/16 | 3 | 3 | 0 | 07/19 | 2 | 1 |
| 2017 Audit of the CFPB's Information Security Program | 10/17 | 7 | 7 | 0 | 07/19 | 5 | 2 |
| The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data | 01/18 | 11 | 11 | 0 | 03/20 | 9 | 2 |
| Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program | 02/18 | 2 | 2 | 0 | 01/20 | 1 | 1 |
| The Bureau's Travel Card Program Controls Are Generally Effective but Could Be Further Strengthened | 09/18 | 4 | 4 | 0 | 09/20 | 4 | 0 |

See notes at end of table.

| Report title | Issue date | Recommendations | | | Status of recommendations | | |
|---|---|---|---|---|---|---|---|
| | | Number | Management agrees | Management disagrees | Last follow-up date | Closed | Open |
| 2018 Audit of the Bureau's Information Security Program | 10/18 | 4 | 4 | 0 | 10/19 | 1 | 3 |
| The Bureau Can Improve Its Follow-Up Process for Matters Requiring Attention at Supervised Institutions | 01/19 | 6 | 6 | 0 | 09/20 | 6 | 0 |
| Technical Testing Results for the Bureau's SQL Server Environment (nonpublic) | 05/19 | 5 | 5 | 0 | n.a. | 0 | 5 |
| Bureau Efforts to Share Consumer Complaint Data Internally Are Generally Effective; Improvements Can Be Made to Enhance Training and Strengthen Access Approval | 06/19 | 6 | 6 | 0 | 06/20 | 6 | 0 |
| The Bureau Can Improve The Effectiveness of Its Life Cycle Processes for FedRAMP | 07/19 | 3 | 3 | 0 | 06/20 | 0 | 3 |
| 2019 Audit of the Bureau's Information Security Program | 10/19 | 7 | 7 | 0 | n.a. | 0 | 7 |
| The Bureau's Office of Enforcement Has Centralized and Improved Its Final Order Follow-Up Activities, but Additional Resources and Guidance Are Needed | 03/20 | 3 | 3 | 0 | 06/20 | 1 | 2 |
| Testing Results for the Bureau's Plan of Action and Milestones Process | 04/20 | 2 | 2 | 0 | n.a. | 0 | 2 |

See notes at end of table.

| Report title | Issue date | Recommendations | | | Status of recommendations | | |
|---|---|---|---|---|---|---|---|
| | | Number | Management agrees | Management disagrees | Last follow-up date | Closed | Open |
| The Bureau Can Improve Its Periodic Monitoring Program to Better Target Risk and Enhance Training for Examiners | 06/20 | 4 | 4 | 0 | 09/20 | 3 | 1 |
| Technical Testing Results for the Bureau's Legal Enclave (nonpublic) | 07/20 | 4 | 4 | 0 | n.a. | 0 | 4 |
| Results of Scoping and Suspension of the Evaluation of the Bureau's Personnel Security Program | 08/20 | 3 | 3 | 0 | 08/20 | 0 | 3 |

Note: 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.

n.a. not applicable.

## Table A-5. Audit, Inspection, and Evaluation Reports Issued to the Board and the Bureau With Questioned Costs, Unsupported Costs, or Recommendations That Funds Be Put to Better Use During the Reporting Period

| 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 |

Note: Because the Board and the Bureau 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

| Investigative actions | Number or dollar value[a] |
|---|---|
| **Investigative caseload** | |
| Investigations open at end of previous reporting period | 68 |
| Investigations opened during the reporting period | 46 |
| Investigations closed during the reporting period | 7 |
| Investigations open at end of the reporting period | 107 |
| **Investigative results for the reporting period** | |
| Persons referred to U.S. Department of Justice prosecutors | 21 |
| Persons referred to state/local prosecutors | 0 |
| Declinations received | 8 |
| Joint investigations | 69 |
| Reports of investigation issued | 1 |
| Oral and/or written reprimands | 0 |
| Terminations of employment | 0 |
| Arrests | 14 |
| Suspensions | 0 |
| Debarments | 0 |
| Prohibitions from banking industry | 3 |
| Indictments | 10 |
| Criminal informations | 9 |
| Criminal complaints | 7 |
| Convictions | 6 |
| Civil actions | $0 |

See notes at end of table.

| Investigative actions | Number or dollar value[a] |
|---|---|
| Administrative monetary recoveries and reimbursements | $0 |
| Civil judgments | $0 |
| Criminal fines, restitution, and special assessments | $672,487 |
| Forfeiture | $0 |

Note: Some of the investigative numbers may include data also captured by other OIGs.

a. 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 | 18 |
| Complaints received during reporting period | 571 |
| Total complaints for reporting period | 589 |
| Complaints resolved during reporting period | 568 |
| Complaints pending | 21 |

# Appendix B: Inspector General Empowerment Act of 2016 Requirements

The Inspector General Empowerment Act of 2016 amended 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 and the name of the senior government official, if already made public by the OIG; 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 requirements is below.

**Summaries of each audit, inspection, and evaluation report issued to the Board or the Bureau for which no agency comment was returned within 60 days of receiving the report or for which no management decision has been made by the end of the reporting period.**

- We have no such instances to report.

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

- See appendix C.

**Statistical tables showing for the reporting period (1) the number of issued investigative reports, (2) the number of persons referred to the U.S. Department of Justice for criminal prosecution, (3) the number of persons referred to state and local authorities for criminal prosecution, and (4) 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.

**A report on each investigation conducted by the OIG that involves a senior government employee in which allegations of misconduct were substantiated, which includes (1) the name of the senior government official, if already made public by the OIG; (2) a detailed description of the facts and circumstances of the investigation as well as the status and disposition of the matter; (3) whether the**

**matter was referred to the U.S. Department of Justice and the date of the referral; and (4) whether the U.S. Department of Justice declined the referral and the date of such declination.**

- We have no such instances to report.

**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.

**A detailed description of any attempt by the Board or the Bureau to interfere with the independence of the OIG, including (1) through budget constraints designed to limit OIG capabilities and (2) 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.

**Detailed descriptions of (1) inspections, evaluations, and audits conducted by the OIG that were closed and not disclosed to the public and (2) investigations conducted by the OIG involving a senior government employee that were closed and not disclosed to the public.**

- We initiated an investigation concerning allegations that a senior Board employee was involved in an advance fee loan scheme. The allegations were unsubstantiated, and the investigation was closed. The victim was located outside the United States; therefore, the matter was referred to a law enforcement agency in the victim's country.
- We initiated an investigation concerning allegations that a senior Bureau employee abused their authority and considered an applicant's political affiliation during the hiring process. These allegations were unsubstantiated, and the investigation was closed.
- We initiated an investigation concerning allegations of abuse of authority; gross mismanagement; and other waste, fraud, and abuse by a senior Board employee. These allegations were unsubstantiated, and the investigation was closed.
- We initiated an investigation concerning allegations that two senior Bureau employees violated the Bureau's *Acceptable Use of CFPB Information Technology Resources* policy. These allegations were unsubstantiated, and the investigation was closed.

# 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 Bureau 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

| Year | Number of reports with unimplemented recommendations | Number of unimplemented recommendations |
|---|---|---|
| 2013 | 1 | 1 |
| 2014 | 0 | 0 |
| 2015 | 0 | 0 |
| 2016 | 1 | 1 |
| 2017 | 3 | 14 |
| 2018 | 5 | 18 |
| 2019 | 3 | 11 |
| 2020[a] | 7 | 39 |

Note: 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.

a. Through September 30, 2020.

## 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 found that the Board's divisions had processes for establishing administrative internal control that were tailored to their specific responsibilities. These controls generally used best practices and were designed to increase efficiency and react to changing environments; however, the Board's processes for maintaining and monitoring these controls could have been enhanced. Specifically, we found that the Board did not have an agencywide process for maintaining and monitoring its administrative internal control. 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.

## 2016 Audit of the Board's Information Security Program

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

**Total number of recommendations: 9**
**Recommendations open: 1**

In accordance with FISMA 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 had taken several steps to mature its information security program to ensure that the program was consistent with FISMA requirements. 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 could have strengthened its risk management program by ensuring that Board divisions were consistently implementing the organization's risk management processes related to security controls assessment, security planning, and authorization. In addition, we found 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 could have strengthened its incident response capabilities.

## The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing

**2017-IT-B-009** **April 17, 2017**

**Total number of recommendations: 8**
**Recommendations open: 4**

We assessed (1) the Board's current cybersecurity oversight approach and governance structure, (2) the current examination practices for financial market utilities and multiregional data processing servicer (MDPS) firms for which the Board has oversight responsibilities, and (3) the Board's ongoing initiative for the future state of cybersecurity oversight. We found that the Division of Supervision and Regulation could improve the oversight of MDPS firms by (1) enforcing a reporting requirement in the Bank Service Company Act, (2) considering the implementation of an enhanced governance structure for these firms, (3) providing additional guidance on the supervisory expectations for these firms, and (4) ensuring that the division's intelligence and incident management function is aware of the technologies used by MDPS firms. We also identified opportunities to improve the recruiting, retention, tracking, and succession planning of cybersecurity resources, as well as opportunities to enhance the internal communications about cybersecurity-related risks.

## 2017 Audit of the Board's Information Security Program

**2017-IT-B-018** **October 31, 2017**

**Total number of recommendations: 9**
**Recommendations open: 6**

We evaluated the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. We followed U.S. Department of Homeland Security guidelines and evaluated the information security program's maturity level (from a low of 1 to a high of 5) across several areas.

The Board's information security program is operating at a level-3 maturity (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. Further, it has implemented an effective security training program that includes phishing exercises and associated performance metrics. However, the Board can mature its information security program to ensure that it is effective, or operating at level-4 maturity (*managed and measurable*). The lack of an agencywide risk-management governance structure and strategy as well as decentralized IT services result in an incomplete view of the risks affecting the security posture of the Board and impede its ability to implement an effective information security program. In addition, several security processes, such

as configuration management and information security continuous monitoring, were not effectively implemented agencywide.

## The Board's Organizational Governance System Can Be Strengthened

**2017-FMIC-B-020** **December 11, 2017**

**Total number of recommendations: 14**
**Recommendations open: 4**

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

The Board's core organizational governance structure aligns with benchmark institutions and selected governance principles, as does its public disclosure of governance documents. Nonetheless, the Board can strengthen its governance system by clarifying and regularly reviewing purposes, roles and responsibilities, authorities, and working procedures of its standing committees; enhancing the orientation program for new governors and reviewing and formalizing the process for selecting dedicated advisors; setting clearer communication expectations and exploring additional opportunities for information sharing among governors; reviewing, communicating, and reinforcing the Board of Governors' expectations of the chief operating officer and the heads of the administrative functions; and establishing and documenting the Executive Committee's mission, protocols, and authorities.

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

**2018-IT-B-008R** **March 21, 2018**

**Total number of recommendations: 7**
**Recommendations open: 3**

We evaluated the adequacy of select information security controls for protecting the Board's public website from compromise. Overall, the information security controls that we tested were adequately designed and implemented. However, we identified opportunities for improvement in the areas of configuration management and risk management.

## Security Control Review of the Board Division of Research and Statistics' General Support System (nonpublic)

**2018-IT-B-015R** **September 26, 2018**

**Total number of recommendations: 9**
**Recommendations open: 2**

We evaluated the effectiveness of select security controls and techniques for the Division of Research and Statistics' general support system, as well as the system's compliance with FISMA and Board information security policies, procedures, standards, and guidelines.

Overall, we found that the division has taken steps to implement information security controls for its general support system in accordance with FISMA and Board information security policies, procedures, standards, and guidelines. We identified opportunities for improvement in the implementation of the Board's information system security life cycle for the division's general support system to ensure that information security controls are effectively implemented, assessed, authorized, and monitored.

## 2018 Audit of the Board's Information Security Program

**2018-IT-B-017** **October 31, 2018**

**Total number of recommendations: 6**
**Recommendations open: 5**

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Board. We evaluated the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Board's information security program is operating at a level-4 (*managed and measurable*) maturity, which indicates an overall effective level of security. The Board has opportunities to mature its information security program in FISMA domains across all five security functions outlined in the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

## The Board Can Strengthen Information Technology Governance

**2018-IT-B-020** **November 5, 2018**

**Total number of recommendations: 6**
**Recommendations open: 3**

The efficiency and effectiveness of the Board's agencywide information security program is contingent on enterprisewide visibility into IT operations. As part of our requirements under FISMA, we assessed

whether the Board's current organizational structure and authorities support its IT needs—specifically, the organizational structure and authorities associated with security, privacy, capital planning, budgeting, and acquisition.

Overall, we found that certain aspects of the Board's organizational structure and authorities could inhibit the Board's achievement of its strategic objectives regarding technology as well as its achievement of an effective FISMA maturity rating. Although the Board has IT governance mechanisms in place, we found opportunities for improvement in the areas of security, budgeting, procurement, and capital planning.

## The Board's Currency Shipment Process Is Generally Effective but Can Be Enhanced to Gain Efficiencies and to Improve Contract Administration

**2018-FMIC-B-021** **December 3, 2018**

**Total number of recommendations: 8**
**Recommendations open: 5**

We assessed the efficiency and effectiveness of the Board's management of the currency shipment process and the effectiveness of related contracting activities.

The Board's currency shipment process is generally effective; however, the process can be enhanced to gain time and cost efficiencies. The currency forecasting process can be streamlined, and selecting different transportation modes for certain currency shipment routes and evaluating alternatives to transporting shipping equipment could yield transportation cost savings. Additionally, the Board can improve the administration of its armored carrier contracts.

## The Board Can Enhance Its Internal Enforcement Action Issuance and Termination Processes by Clarifying the Processes, Addressing Inefficiencies, and Improving Transparency

**2019-SR-B-013** **September 25, 2019**

**Total number of recommendations: 6**
**Recommendations open: 3**

We assessed the efficiency and effectiveness of the Board's and the Reserve Banks' enforcement action issuance and termination processes and practices.

We found that the Board and the Reserve Banks have implemented some effective practices to support the enforcement action issuance and termination processes; however, we identified opportunities for the Board to enhance these processes. Specifically, we found that the Board can clarify certain aspects of these internal processes, such as the steps in these processes, the Board stakeholders' roles

and responsibilities, and the Board members' involvement. In addition, we found that the Board can (1) improve the timeliness and efficiency of its enforcement action issuance and termination processes and (2) increase transparency with respect to the status of ongoing enforcement actions.

## The Board's Law Enforcement Operations Bureau Can Improve Internal Processes

**2019-MO-B-014** **September 30, 2019**

**Total number of recommendations: 6**
**Recommendations open: 2**

We assessed whether the control environment in the Law Enforcement Unit's (LEU) Operations Bureau is operating effectively to support the LEU's mission as well as components of the Management Division's strategic goals.

We found that the LEU's Operations Bureau can improve standards and processes associated with its control environment to better support the LEU's mission. Specifically, we found that the LEU did not document the roles, responsibilities, training qualifications, and reporting requirements after modifying its process for internal reviews. We also found that the LEU can better communicate its decisions and the rationale for changes affecting the Operations Bureau and can take further action to improve communication generally. Additionally, the LEU can better capitalize on professional development opportunities for officers and new supervisors. Lastly, the LEU should also strengthen its processes for determining shift and post assignments.

## 2019 Audit of the Board's Information Security Program

**2019-IT-B-016** **October 31, 2019**

**Total number of recommendations: 6**
**Recommendations open: 6**

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Board. We evaluated the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Board's information security program is operating effectively at a level-4 (*managed and measurable*) maturity. The Board has opportunities to mature its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

## The Board Should Finalize Guidance to Clearly Define Those Considered Senior Examiners and Subject to the Associated Postemployment Restriction

**2020-SR-B-003** **March 9, 2020**

**Total number of recommendations: 1**
**Recommendations open: 1**

We assessed the effectiveness of controls designed to ensure compliance with the requirements outlined in Supervision and Regulation Letter 16-16.

We found that the four Reserve Banks in our sample have issued policies and procedures to identify senior examiners, require that they be notified of their postemployment restriction, and require workpaper reviews as appropriate. These Reserve Banks took different approaches, however, to determining whom to designate as a *senior examiner*.

Although the Board found through a 2017 horizontal review that the Reserve Banks implemented the Board's postemployment restriction guidance, the review also found that the Reserve Banks did not always apply the *senior examiner* definition in accordance with the guidance. Thus, the 2017 review team recommended that the Board issue additional guidance to clarify the definition of a *senior examiner*. As of November 2019, the Board had not finalized this guidance.

## The Board's Oversight of Its Designated Financial Market Utility Supervision Program Is Generally Effective, but Certain Program Aspects Can Be Improved

**2020-FMIC-B-005** **March 18, 2020**

**Total number of recommendations: 6**
**Recommendations open: 6**

We assessed the effectiveness of the Board's oversight of its designated financial market utility (DFMU) supervision program.

The Board has implemented practices and processes (1) to ensure governance over the DFMU supervision program, (2) to collaborate with other supervisory agencies in accordance with authorities provided in the Dodd-Frank Act, and (3) to conduct reviews of material changes filed by DFMUs that meet the Board's responsibilities under title VIII of the Dodd-Frank Act. However, we identified opportunities for the Board to enhance these practices and processes. Specifically, the Board should publish certain internal delegations of authority and define certain roles and responsibilities within the DFMU supervision program. The Board also can enhance its processes for collaborating with other supervisory agencies.

Lastly, the Board can better prepare for emergency changes filed by the DFMUs for which it is the supervisory agency.

## The Board Can Enhance Certain Aspects of Its Enforcement Action Monitoring Practices

**2020-SR-B-006** **March 18, 2020**

**Total number of recommendations: 1**
**Recommendations open: 1**

We assessed the effectiveness of the Board's and the Reserve Banks' enforcement action monitoring practices, with a focus on supervised financial institutions within the community banking organization and the large and foreign banking organization portfolios.

We found that the Reserve Banks in our sample have implemented some effective practices for monitoring enforcement actions; however, we identified opportunities for the Board to enhance certain aspects of these practices. Specifically, we found that the Reserve Banks in our sample use different information systems for monitoring enforcement actions against institutions in the community banking organization portfolio. We learned that the Board currently has an initiative underway to develop a common technology platform for supervisory activities across the System for institutions with less than $100 billion in total assets, including community banking organizations. We also identified certain instances of Reserve Bank staff not posting supervised institutions' progress reports describing their enforcement action remediation efforts to the required system of record.

## The Board Can Further Enhance the Design and Implementation of Its Operating Budget Process

**2020-FMIC-B-010** **March 25, 2020**

**Total number of recommendations: 2**
**Recommendations open: 2**

We assessed the design and implementation of the Board's processes for formulating and executing its annual operating budget.

The Board has made changes over the past several years to improve its budget process; the Board has acknowledged perennial underspending and is addressing it by focusing on slowing growth and spending more consistently with budget estimates. The Board can further enhance the design and implementation of its operating budget process by communicating its budget process in an overarching document, strengthening the connection between budget and strategy, and implementing an agencywide approach to executing the approved budget.

## The Board Can Strengthen Its Oversight of the Protective Services Unit and Improve Controls for Certain Protective Services Unit Processes

**2020-MO-B-011** **March 25, 2020**

**Total number of recommendations: 6**
**Recommendations open: 6**

We assessed the Internal Oversight Committee's 2018 evaluation of the Protective Services Unit (PSU), as well as the PSU's operations to support its mission.

The 2018 Internal Oversight Committee evaluation of PSU operations generally complied with the committee's guidance, although we found opportunities for improvement that could strengthen future evaluations of the PSU's operations. In our assessment of PSU operations, we found that the PSU complied with its policies and procedures for certain aspects of protection measures and protective intelligence. However, the PSU (1) does not have procedures related to vehicle maintenance, (2) does not require driving refresher training for special agents, and (3) did not consistently maintain records of destroyed credentials for separated agents.

## The Board Can Improve Its Contract Administration Processes

**2020-FMIC-B-012** **March 30, 2020**

**Total number of recommendations: 13**
**Recommendations open: 13**

We assessed the Board's compliance with laws, regulations, and Board policies and procedures applicable to contract administration, as well as the effectiveness of the Board's internal controls related to contract administration. We focused on the Board's contract administration processes from postaward to contract closeout.

We found that the Division of Financial Management can improve its contract administration processes as well as related internal controls. In addition, contracting officer's representatives do not appear to be adequately trained to fulfill their responsibilities.

## The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced

**2020-SR-B-019** **September 30, 2020**

**Total number of recommendations: 10**
**Recommendations open: 10**

See the summary in the body of this report.

# Bureau of Consumer Financial Protection

## Table C-2. Reports to the Bureau With Unimplemented Recommendations, by Calendar Year

| Year | Number of reports with unimplemented recommendations | Number of unimplemented recommendations |
|---|---|---|
| 2014 | 1 | 1 |
| 2015 | 0 | 0 |
| 2016 | 1 | 1 |
| 2017 | 1 | 2 |
| 2018 | 3 | 6 |
| 2019 | 3 | 15 |
| 2020[a] | 5 | 12 |

Note: Because the Bureau 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.

a. Through September 30, 2020.

## 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 found that the Bureau continued to take steps to mature its information security program and to ensure that it was consistent with the requirements of FISMA. Overall, we found that the Bureau'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. We found that the Bureau's information security program was generally consistent with the requirements for continuous monitoring, configuration management, and incident response; however, we identified opportunities to strengthen these areas through automation and centralization.

## 2016 Audit of the CFPB's Information Security Program

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

**Total number of recommendations: 3**
**Recommendations open: 1**

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

We found that the Bureau had taken several steps to mature its information security program to ensure that it was consistent with FISMA requirements. For instance, we found that both the information security continuous monitoring and incident response programs were operating at an overall maturity of level 3 (*consistently implemented*). However, we identified several improvements needed in the Bureau's information security program in the areas of risk management, identity and access management, and contingency planning. Specifically, we noted that the Bureau could have strengthened 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. We also noted that the Bureau had not completed an agencywide business impact analysis to guide its contingency planning activities, nor had it fully updated its continuity of operations plan to reflect the transition of its IT infrastructure from the U.S. Department of the Treasury.

## 2017 Audit of the CFPB's Information Security Program

**2017-IT-C-019** **October 31, 2017**

**Total number of recommendations: 7**
**Recommendations open: 2**

We evaluated the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. We followed U.S. Department of Homeland Security guidelines and evaluated the information security program's maturity level (from a low of 1 to a high of 5) across several areas.

The Bureau's overall information security program is operating at a level-3 maturity (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. However, the Bureau can mature its information security program to ensure that it is effective, or operating at level-4 maturity (*managed and measurable*). Specifically, the agency can strengthen its ongoing efforts to establish an enterprise risk-management program by defining a risk appetite statement and associated

risk tolerance levels and developing and maintaining an agencywide risk profile. It can also improve configuration monitoring processes for agency databases and applications, multifactor authentication for the internal network and systems, assessments of the effectiveness of security awareness and training activities, and incident response and contingency planning capabilities.

## The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data

**2018-MO-C-001** **January 22, 2018**

**Total number of recommendations: 11**
**Recommendations open: 2**

The Bureau's offboarding process for employees and contractors covers, among other things, the return of property, records management, and ethics counseling on conflicts of interest. We determined whether the agency's controls over these aspects of offboarding effectively mitigate reputational and security risks.

Although the Bureau has offboarding controls related to conflicts of interest for executive employees' postemployment restrictions, the Bureau has opportunities to strengthen controls in other areas. Specifically, the agency did not always deactivate badges timely or record the status of badges for separating employees and contractors, did not consistently maintain IT asset documentation, did not always conduct records briefings, did not always maintain nondisclosure agreements for contractors, and did not accurately maintain certain separation and contractor data.

## Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program

**2018-IT-C-003** **February 14, 2018**

**Total number of recommendations: 2**
**Recommendations open: 1**

We contracted with a third party to conduct a performance audit of the Bureau's privacy program and its implementation.

Overall, the contractor found that the Bureau has substantially developed, documented, and implemented a privacy program that addresses applicable federal privacy requirements and security risks related to collecting, processing, handling, storing, and disseminating sensitive privacy data. Further, the contractor noted that the Bureau has documented privacy policies and procedures covering a wide range of topics, including privacy roles and responsibilities, privacy impact assessment and system of records notice management, training, breach notification and response, and monitoring and auditing.

## 2018 Audit of the Bureau's Information Security Program

**2018-IT-C-018** **October 31, 2018**

**Total number of recommendations: 4**
**Recommendations open: 3**

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Bureau. We evaluated the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Bureau's information security program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level. The Bureau also has opportunities to mature its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program is effective.

## Technical Testing Results for the Bureau's SQL Server Environment (nonpublic)

**2019-IT-C-007R** **May 22, 2019**

**Total number of recommendations: 5**
**Recommendations open: 5**

We identified that the security configurations for select SQL Server instances and databases were not aligned with established baselines and that significant weaknesses exist in controls for account management and configuration management. We believe that these continuing weaknesses heighten the risk of a breach of sensitive data maintained in the Bureau's SQL Server environment.

## The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP

**2019-IT-C-009** **July 17, 2019**

**Total number of recommendations: 3**
**Recommendations open: 3**

To meet our FISMA requirements, we determined whether the Bureau has implemented an effective life cycle process for deploying and managing Federal Risk and Authorization Management Program (FedRAMP) cloud systems, including ensuring that effective security controls are implemented.

We found that the Bureau has developed a life cycle process for deploying and managing security risks for Bureau systems, which include the FedRAMP cloud systems it uses. However, we found that the

process is not yet effective in ensuring that (1) risks are comprehensively assessed prior to deploying new cloud systems, (2) continuous monitoring is performed to identify security control weaknesses after deployment, and (3) electronic media sanitization renders sensitive Bureau data unrecoverable when cloud systems are decommissioned.

## 2019 Audit of the Bureau's Information Security Program

**2019-IT-C-015** **October 31, 2019**

**Total number of recommendations: 7**
**Recommendations open: 7**

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Bureau. We evaluated the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Bureau's information security program is operating effectively at a level-4 (*managed and measurable*) maturity. We identified opportunities for the Bureau to strengthen its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

## The Bureau's Office of Enforcement Has Centralized and Improved Its Final Order Follow-Up Activities, but Additional Resources and Guidance Are Needed

**2020-SR-C-002** **March 2, 2020**

**Total number of recommendations: 3**
**Recommendations open: 2**

We assessed the effectiveness of Enforcement's processes for monitoring and conducting follow-up activities related to final orders.

Enforcement has implemented some effective practices to improve its follow-up on final orders; however, we identified additional opportunities for Enforcement to improve its final order follow-up activities and reporting. First, we determined that Enforcement encountered challenges completing follow-up activities within the time frames established by its compliance team for 5 of 12 orders we reviewed. In addition, the enforcement actions page on the Bureau's public website provided information on the status of public enforcement actions that was prone to misinterpretation, because the website did not define the status categories or describe the purpose of the status information. After we completed our fieldwork and shared preliminary observations with the Bureau, the agency revised the status categories and indicated that it intends to provide additional clarifying information on its website. Finally, Enforcement can

establish comprehensive guidance addressing expectations for conducting and documenting follow-up activities to help promote consistency.

## Testing Results for the Bureau's Plan of Action and Milestones Process

**2020-IT-C-014** **April 29, 2020**

**Total number of recommendations: 2**
**Recommendations open: 2**

See the summary in the body of this report.

## The Bureau Can Improve Its Periodic Monitoring Program to Better Target Risk and Enhance Training for Examiners

**2020-SR-C-015** **June 24, 2020**

**Total number of recommendations: 4**
**Recommendations open: 1**

See the summary in the body of this report.

## Technical Testing Results for the Bureau's Legal Enclave (nonpublic)

**2020-IT-C-017R** **July 22, 2020**

**Total number of recommendations: 4**
**Recommendations open: 4**

See the summary in the body of this report.

## Results of Scoping and Suspension of the Evaluation of the Bureau's Personnel Security Program

**2020-MO-C-018** **August 17, 2020**

**Total number of recommendations: 3**
**Recommendations open: 3**

See the summary in the body of this report.

# Abbreviations

| | |
|---|---|
| **CARES Act** | Coronavirus Aid, Relief, and Economic Security Act |
| **CEO** | chief executive officer |
| **CFPB** | Consumer Financial Protection Bureau |
| **CI** | Criminal Investigation |
| **CIGFO** | Council of Inspectors General on Financial Oversight |
| **CIGIE** | Council of the Inspectors General on Integrity and Efficiency |
| **DATA Act** | Digital Accountability and Transparency Act of 2014 |
| **DFMU** | designated financial market utility |
| **DOJ** | U.S. Department of Justice |
| **FBI** | Federal Bureau of Investigation |
| **FDIC** | Federal Deposit Insurance Corporation |
| **FedRAMP** | Federal Risk and Authorization Management Program |
| **FFIEC** | Federal Financial Institutions Examination Council |
| **FHFA** | Federal Housing Finance Agency |
| **FISMA** | Federal Information Security Modernization Act of 2014 |
| **IG** | inspector general |
| **IPIA** | Improper Payments Information Act of 2002, as amended |
| **IRS** | Internal Revenue Service |
| **IT** | information technology |
| **LEU** | Law Enforcement Unit |
| **LISCC** | Large Institution Supervision Coordinating Committee |
| **MDPS** | multiregional data processing servicer |
| **PIIA** | Payment Integrity Information Act of 2019 |
| **POA&M** | plan of action and milestones |
| **PPP** | Paycheck Protection Program |
| **PRAC** | Pandemic Response Accountability Committee |
| **PSO** | Personnel Security Office |
| **PSU** | Protective Services Unit |
| **SBA** | U.S. Small Business Administration |
| **SEFL** | Division of Supervision, Enforcement and Fair Lending |

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

20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551
Phone: 202-973-5000 | Fax: 202-973-5044

---

**OIG Hotline**

oig.federalreserve.gov/hotline
oig.consumerfinance.gov/hotline

800-827-3340