Audit Report
2018-IT-C-003
February 14, 2018

Consumer Financial Protection Bureau

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

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

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

MEMORANDUM

DATE: February 14, 2018

TO: Claire Stapleton
Chief Privacy Officer
Consumer Financial Protection Bureau

FROM: Peter Sheridan
Assistant Inspector General for Information Technology

SUBJECT: 2017 Audit of the CFPB's Privacy Program

This memorandum transmits the independent auditors' report, prepared by Cotton & Company LLP, on the Consumer Financial Protection Bureau's (CFPB) privacy program. We contracted with Cotton & Company to conduct a performance audit of the CFPB's privacy program and its implementation.

The contract requires the audit to be performed in accordance with generally accepted government auditing standards. We reviewed and monitored the work of Cotton & Company to ensure compliance with the contract. Cotton & Company is responsible for the accompanying report, *Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program*, dated January 29, 2018.

The report includes recommendations designed to strengthen the CFPB's privacy and related security program. In its response to Cotton & Company's draft report, the CFPB concurs with the recommendations and outlines actions that are underway or will be taken to strengthen the CFPB's privacy and related security program. We will monitor the CFPB's progress in addressing these recommendations as part of future audits.

We appreciate the cooperation that Cotton & Company received from CFPB personnel during the audit. Please contact me if you would like to discuss this report or any related issues.

cc: Sartaj Alag, Chief Operating Officer and Associate Director, Operations Division
Jerry Horton, Chief Information Officer
Zachary Brown, Chief Information Security Officer
Linda Powell, Chief Data Officer
Elizabeth Reilly, Chief Financial Officer and Assistant Director, Office of the Chief Financial Officer
Dana James, Deputy Chief Financial Officer, Office of the Chief Financial Officer
Anya Williams, Finance and Policy Analyst, Office of the Chief Financial Officer
Carlos Villa, Finance and Policy Analyst, Office of the Chief Financial Officer

REPORT ON THE
INDEPENDENT AUDIT OF THE
CONSUMER FINANCIAL PROTECTION BUREAU'S PRIVACY PROGRAM

JANUARY 29, 2018

Cotton & Company LLP
635 Slaters Lane
Alexandria, Virginia 22314
703.836.6701 | 703.836.0941, fax
gbills@cottoncpa.com | www.cottoncpa.com

Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

January 29, 2018

To: Inspector General, Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau

Subject: Independent Performance Audit Report on the Consumer Financial Protection Bureau's Privacy Program

Cotton & Company LLP is pleased to submit this independent performance audit report on its audit of the Consumer Financial Protection Bureau's privacy program. Cotton & Company performed the work from October through December 2017.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, as amended, promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Overall, management did concur with our recommendations. We did not evaluate and are not expressing an opinion on management's comments. Management's written comments on our findings and recommendations can be found in Appendix I.

Sincerely,
Cotton & Company LLP

George E. Bills, CPA, CISSP, CISA, CIPP
Partner, Information Assurance

TABLE OF CONTENTS

PURPOSE

Cotton & Company LLP conducted an independent performance audit of the Consumer Financial Protection Bureau's (CFPB's) privacy program and practices. The objective of this audit was to assess the adequacy and effectiveness of the CFPB's privacy program and its implementation, including compliance with applicable statutory and regulatory requirements concerning the protection of personally identifiable information (PII) and with CFPB privacy policies and procedures.

This report is intended solely for the information and use of the Consumer Financial Protection Bureau and is not intended to be, and should not be, used by anyone other than these specified parties.

BACKGROUND

The CFPB aims to make consumer financial markets work for consumers, responsible providers, and the economy as a whole. The CFPB's goal is to protect consumers from unfair, deceptive, or abusive practices and take action against companies that break the law. To meet this goal, the CFPB collects a significant amount of sensitive personally identifiable information (PII) such as consumer financial data on credit card accounts, mortgage loans, arbitration case records, automotive sales, credit scores, private student loans, and storefront payday loans.

When collecting PII, the CFPB is responsible for ensuring that it only collects the minimum amount necessary, that it notifies the public of these collections, and that it develops and fully implements effective physical and logical security controls to protect the PII from unauthorized or inappropriate access.

The CFPB's privacy team, which currently consists of five full-time privacy professionals, is responsible for all privacy activities throughout the CFPB. The head of the CFPB's privacy team is the Chief Privacy Officer (CPO), who is also designated as the Senior Agency Official for Privacy (SAOP). While the CPO does not report to the Head of the CFPB; instead, the CPO reports to the Chief Data Officer (CDO), who in turn reports to the Chief Information Officer (CIO), we did note that the CFPB has formally granted the CPO with direct access to the Head of the CFPB to communicate privacy issues when needed.

Further, the privacy team works closely with personnel throughout the CFPB, including the CIO, CDO, and Chief Information Security Officer (CISO), and is actively involved in key functions such as the Data Governance Board (DGB), Data Intake Group (DIG), and Data Release Group (DRG).The DGB is charged with assessing risks and benefits associated with managing the CFPB's data assets, as well as with reviewing and offering guidance on data policies. The privacy team serves on the DGB to ensure that the DGB accounts for privacy whenever it defines and interprets data policies for use across the CFPB.

The DIG is responsible for vetting and approving proposed data and datasets before the CFPB collects them. The privacy team reviews proposed data collections for compliance with applicable laws and policies and makes recommendations to the CIO regarding whether to approve the proposed collection. In addition, the DRG is charged with determining whether the CFPB must disclose public-use datasets and the extent of disclosure if so. The privacy team reviews requests to ensure that the CFPB protects the privacy of individuals in the released data. This includes validating whether releases employ effective de-identification techniques to reduce the risks associated with the public disclosure of datasets.

CONCLUSION

Overall, we found that the CFPB 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, we noted that the CFPB has documented privacy policies and procedures covering a wide range of topics, including privacy roles and responsibilities, privacy impact assessment (PIA) and system of records notice (SORN) management, training, breach notification and response, and monitoring and auditing.

Although the CFPB has substantially developed, documented, and implemented a privacy program with related policies and procedures, we identified two areas that require improvement: identification and maintenance of a comprehensive inventory of PII and physical controls over the CFPB's portable media.

RECOMMENDATIONS

Our report includes two recommendations designed to strengthen the CFPB's privacy and security program. In its response to our draft report, the CFPB concurred with our recommendations and outlined actions that are underway or that it intends to take to strengthen its privacy program.

AUDIT SCOPE AND METHODOLOGY

Cotton & Company conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that, based on the objectives of this audit, the evidence obtained through our review of the CFPB's privacy program provides a reasonable basis for our findings and conclusions.

We carried out our audit planning and testing procedures from October through December 2017. We based our audit scope and methodology on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J: Privacy Controls; NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*; and Office of Management and Budget (OMB) memoranda and circulars related to privacy. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets.[1]

In addition, Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act.[2] These documents outline federal privacy best practices for developing and implementing a privacy program and for identifying and reducing the collection and handling of sensitive PII, where appropriate. The CFPB is an independent federal agency and is therefore not required to follow all privacy and

[1] NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.
[2] OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003.

security guidance issued by OMB and NIST; however, the CFPB recognizes OMB and NIST guidance as best practices and has chosen to follow this guidance where appropriate.

Our audit reviewed all offices and privacy activities within the CFPB. We interviewed CFPB personnel associated with the CFPB's privacy program, as well as key personnel from various offices, including Technology & Innovation (T&I), CDO, Office of Human Capital, Enterprise Risk Management, Legal, and Physical Security.

We obtained and evaluated available documentation related to the CFPB's privacy program, including privacy policies and procedures, privacy training material and attendance records, and privacy information on the CFPB's external-facing webpages, including the CFPB's privacy policy, PIAs, and SORNs. We also obtained and reviewed relevant Government Accountability Office (GAO) and Office of Inspector General (OIG) privacy and security audit reports and CFPB internal control testing documentation related to the CFPB's privacy policies, procedures, and controls. This included documentation related to management's A-123 Continuous Monitoring (CM) and Security Assessment and Authorization (SA&A) testing.

Finally, we judgmentally selected CFPB employees and contractors from all offices within the CFPB and issued them a survey covering a number of privacy topics. We used the responses from this survey to support our testing of NIST SP 800-53, Revision 4, Appendix J controls and identify areas in which further testing may be necessary based on risk.

We performed these activities to evaluate the overall effectiveness of the CFPB's privacy program and its compliance with applicable CFPB and federal privacy requirements. We conducted testing at the CFPB's main building in Washington, D.C. and at our headquarters in Old Town Alexandria, Virginia, from October to December 2017.

AUDIT FINDINGS AND RECOMMENDATIONS

A. The CFPB Must Develop and Maintain a Comprehensive Inventory of All PII

The CFPB does not have a comprehensive inventory that identifies all PII or privacy data collected, processed, handled, and stored throughout the organization. We requested and obtained an inventory of the CFPB's privacy data from the CPO, who extracted it from the CDO's data repository. The inventory included detailed information on data collected as part of the CFPB's core business activities. Although this inventory did clearly identify where the CFPB considered business data to be privacy-related and whether the data required a PIA or SORN, we noted that the inventory did not include data used by the Office of Human Capital, Administrative Operations, or Office of Chief Financial Officer.

In addition, we noted that the CFPB's internal review under OMB Circular A-123, *Management's Responsibility for Internal Control,* identified issues with the CFPB's PII inventory, including determining that the inventory did not include PII datasets obtained by those CFPB offices that have been delegated privacy management authority. We noted that T&I disagreed with the internal review's recommendations related to this weakness.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Control SE-1, *Inventory of Personally Identifiable Information,* states:

> *The organization:*

a. Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

Further, NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Control DM-1, *Minimization of Personally Identifiable Information,* states:

The organization…

c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

The CFPB's Privacy Office is responsible for all privacy activities throughout the CFPB; however, we noted that its current PII inventory only includes data related to the CFPB's primary business activities. The Office of Human Capital and Administrative Operations have been delegated information governance oversight authority by the CIO and are therefore allowed to manage their own data. In addition, because the Office of the Chief Financial Officer operates separately from the rest of the CFPB, it is also allowed to separately manage the data that it processes and stores.

An agency's inventory of PII should serve as a central piece around which the agency designs, implements, and periodically monitors other privacy and security activities. Without a comprehensive and centralized inventory, the likelihood that the CFPB will not identify, track, and appropriately secure sensitive PII increases.

Recommendation: We recommend that the CFPB:

1. Develop, document, and fully implement a formal process to identify, track, and periodically update all PII collected, processed and stored throughout the CFPB. At a minimum this inventory should clearly identify what PII the CFPB is collecting or handling, who within the CFPB is responsible for the security of the PII, where the PII is stored (both physical and logical), and whether a privacy impact assessment or SORN is required.

Management Response:
The Bureau concurs with this recommendation. The Bureau maintains a data catalog, list of systems containing sensitive data, as well as SORNs describing the data contained within those systems. We will explore ways to centralize information related to operational datasets containing sensitive information that have not yet been incorporated into the data catalog.

B. The CFPB Must Strengthen Physical Security Controls over Portable Media and Passwords

The CFPB must strengthen physical security controls over its portable media and passwords. Specifically, we performed an after-hours walkthrough of the CFPB's work space and noted that:

- CFPB personnel routinely did not physically secure CFPB-issued laptops when leaving the laptops unattended.
- One individual left their CFPB-issued phone and thumb drive unattended.
- One CFPB employee appeared to have written down their password on a sheet of paper that they then left on their desk.

CFPB employees and contractors are not following CFPB guidance. CFPB-COO-CS02, *Acceptable Use of CFPB Information Technology Resources,* states:

> *Users must physically protect CFPB information resources when left unattended. Recommended precautions include, but are not limited to, placing sensitive information or devices that contain such information in a locked case, desk drawer, office, or a locked automobile trunk, or securing laptops to a fixed object with a locked cable.*

In addition, NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* Control 3.10, *Physical and Environmental Security, Mobile and portable systems,* states, "Organizations should secure storage of laptop computers when they are not in use."

Management stated that the CFPB provides its employees and contractors with cable locks; however, we noted that the employees and contractors are not consistently using these locks. We further noted that the CFPB does not appear to have a process in place for periodically assessing whether employees and contractors are complying with CFPB and NIST requirements and adequately securing mobile devices and passwords when leaving them unattended.

NIST SP 800-124, Revision 1, *Guidelines on Cell Phone and PDA Security*, notes that even mobile devices only used within an organization's facilities are often transported from place to place within the facilities. The mobile nature of the devices makes them much more likely to be lost or stolen than are other devices, leaving their data at increased risk of compromise. The likelihood that unattended CFPB laptops may be stolen when left unsecured is therefore significantly higher. Further, although the CFPB encrypts its laptops and other portable media, we noted that it does not enforce or require two-factor authentication on these devices, including laptops. This increases the risk that sensitive PII stored on stolen laptops could be inappropriately accessed.

Recommendation: We recommend that the CFPB CIO:

2. Develop, document, and implement a formal process for monitoring compliance with physical security requirements around portable media such as laptops, thumb drives, and smart phones, as well as around passwords and hard copies of sensitive PII.

Management Response:
The Bureau concurs with this recommendation. The Technology & Innovation Office, in coordination with Administrative Operations, will develop a process to monitor compliance with physical security requirements.

APPENDIX I - MANAGEMENT RESPONSES

1700 G Street NW, Washington, DC 20552

January 19, 2018

Mr. Peter Sheridan
Associate Inspector General for Information Technology
Board of Governors of the Federal Reserve System &
Consumer Financial Protection Bureau
20th and C Streets, NW
Washington, DC 20551

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on *Cotton and Company LLP's Independent Performance Audit on the CFPB's Privacy Program.* We are pleased that you found that the Bureau has substantially developed, documented, and implemented a privacy program that addresses applicable federal privacy requirements and security risks related to the collection, processing, handling, storing and dissemination of sensitive privacy data. In fiscal year (FY) 2018, we will continue to enhance our processes and technologies to address each recommendation cited in the report.

We value your objective, independent viewpoints and consider our OIG to be a trusted source of informed, accurate, and insightful information.

Thank you for the professionalism and courtesy that you and all of the OIG personnel demonstrated throughout this review. We have provided comments for each recommendation.

Sincerely,

Jerry W. Horton

Jerry Horton
Chief Information Officer

consumerfinance.gov

Response to recommendations presented in the Draft IG Report,
"Cotton and Company LLP's Independent Performance Audit on the CFPB's Privacy Program"

Recommendation 1: Develop, document, and fully implement a formal process to identify, track, and periodically update all PII collected, processed, and stored throughout the CFPB. At a minimum this inventory should clearly identify what PII CFPB is collecting or handling, who within CFPB is responsible for the security of the PII, where the PII is stored (both physical and logical), and whether a privacy impact assessment or SORN is required.

Management Response: The Bureau concurs with this recommendation. The Bureau maintains a data catalog, list of systems containing sensitive data, as well as SORNs describing the data contained within those systems. We will explore ways to centralize information related to operational datasets containing sensitive information that have not yet been incorporated into the data catalog.

Recommendation 2: Develop, document and implement a formal process to monitor for compliance with physical security requirements around portable media such as laptops, thumb drives and smart phones, as well as passwords and hard copies of sensitive PII.

Management Response: The Bureau concurs with this recommendation. The Technology & Innovation Office, in coordination with Administrative Operations, will develop a process to monitor compliance with physical security requirements.

ABBREVIATIONS

CFPB	Consumer Financial Protection Bureau
CDO	Chief Data Officer
CPO	Chief Privacy Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Continuous Monitoring
DIG	Data Intake Group
DGB	Data Governance Board
DRG	Data Release Group
GAO	Government Accountability Office
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SA&A	Security Assessment & Authorization
SAOP	Senior Agency Official for Privacy
SORN	System of Records Notice
SP	Special Publication
T&I	Technology & Innovation