OFFICE OF INSPECTOR GENERAL

Evaluation Report 2017-SR-C-011

The CFPB Can Improve Its Practices to Safeguard the Office of Enforcement's Confidential Investigative Information

May 15, 2017

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

Report Contributors

Charlene Fadirepo, OIG Manager
Chie Hogenmiller, Project Lead
Rachael Young, Senior Auditor
Melissa Dorow, Auditor
Victor Calderon, Senior Forensic Auditor
Hau Clayton, Forensic Auditor
Michael VanHuysen, Senior OIG Manager for Supervision and Regulation
Melissa Heist, Associate Inspector General for Audits and Evaluations

Abbreviations

CFPB	Consumer Financial Protection Bureau
CII	confidential investigative information
CSI	confidential supervisory information
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
OIG	Office of Inspector General
PII	personally identifiable information
SEFL	Division of Supervision, Enforcement, and Fair Lending
T&I	Office of Technology and Innovation

Executive Summary:

The CFPB Can Improve Its Practices to Safeguard the Office of Enforcement's Confidential Investigative Information

2017-SR-C-011 May 15, 2017

Purpose

The Office of Inspector General conducted an evaluation of the Consumer Financial Protection Bureau (CFPB) Office of Enforcement's processes for protecting sensitive information. Our objective was to determine whether the Office of Enforcement has effective controls to manage and safeguard access to its confidential investigative information (CII). We did not seek to determine whether any unauthorized disclosures of sensitive information occurred.

Background

The Dodd-Frank Wall Street Reform and Consumer Protection Act authorizes the CFPB to take appropriate enforcement actions to address violations of federal consumer financial law. The CFPB's Office of Enforcement is responsible for this enforcement function and conducts investigations to ensure that financial institutions comply with applicable federal consumer financial laws. During the course of an investigation, the Office of Enforcement collects CII related to a potential violation of federal consumer financial law and maintains this CII in four electronic applications and two internal drives. CII may include personally identifiable information, depending on the nature of the investigation. As of February 7, 2017, the Office of Enforcement's work had resulted in approximately $11.5 billion in relief for over 27 million consumers.

Findings

We found that the Office of Enforcement's sensitive information has not always been restricted to Office of Enforcement employees who needed access to that information to perform their assigned duties. We determined that 113 unique users had access to at least one electronic application when it was no longer relevant to the performance of the users' assigned duties. These users continued to have access largely because of the Office of Enforcement's challenges with updating access rights. Further, according to Office of Enforcement management, complications resulting from an information technology system migration contributed to the office's generally allowing its employees broad access to the network drive that contains sensitive information. If access to sensitive information is not appropriately restricted, CII will be available to employees when they do not need it to perform their assigned duties, increasing the risk of inadvertent or unauthorized disclosure. During our fieldwork, the Office of Enforcement took several steps to improve its approach to restricting access.

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

Recommendations

Our report contains recommendations designed to improve the Office of Enforcement's practices for managing and safeguarding CII. These recommendations focus on enhancing practices for managing access rights to matter folders, improving the handling of printed sensitive information, and establishing a standard naming convention for electronically stored information. In its response to our draft report, the CFPB concurs with our recommendations. The agency describes actions and planned activities to improve the Office of Enforcement's practices for safeguarding CII. We will follow up to ensure that the recommendations are fully addressed.

Summary of Recommendations, OIG Report 2017-SR-C-011

Recommendation number	Page	Recommendation	Responsible office
1	17	Formalize in policy that employees should be granted access to the Office of Enforcement's review tools and network drive matter folders only when such access is relevant to their assigned duties.	Office of Enforcement
2	17	Update policies and procedures to specify the process for approving and updating matter folder access rights for the Office of Enforcement's review tools and network drive.	Office of Enforcement
3	17	Expand existing training for Office of Enforcement employees to reinforce the guidance on a. the office's interpretation that *demonstrated business need* means relevance to performing assigned duties. b. the access approval and updating process for the Office of Enforcement's review tools and network drive.	Office of Enforcement
4	17	Develop and implement a monitoring and testing approach to periodically confirm that the Office of Enforcement's matter folders are appropriately restricted.	Office of Enforcement
5	17	Coordinate with the Chief Information Officer to ensure that the new cloud environment, which is intended to replace the network drive, includes access approval and monitoring capabilities that meet the current and future needs of the Office of Enforcement.	Office of Enforcement
6	21	Develop and implement operational procedures specific to the Office of Enforcement for handling printed high-sensitivity information, including but not limited to information labeling requirements and the use of cover sheets.	Office of Enforcement
7	21	Establish a strategy to periodically reinforce handling and safeguarding requirements and establish a monitoring approach to test compliance with information handling and safeguarding policies and procedures.	Office of Enforcement
8	21	Monitor securable, access-controlled storage space, including but not limited to lockable cabinets and offices, to ensure that it meets the needs of all Office of Enforcement employees.	Office of Enforcement
9	23	Develop a policy to establish a standard naming convention for matter folders and other relevant Office of Enforcement folders to be used across all Office of Enforcement applications and internal drives.	Office of Enforcement

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

May 15, 2017

MEMORANDUM

TO: Anthony Alexis
Assistant Director, Office of Enforcement
Consumer Financial Protection Bureau

FROM: Melissa Heist
Associate Inspector General for Audits and Evaluations

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

The Office of Inspector General has completed its report on the subject evaluation. We conducted this evaluation to determine whether the Consumer Financial Protection Bureau's Office of Enforcement manages and safeguards confidential investigative information effectively.

We provided you with a draft of our report for review and comment. In your response, you concur with our recommendations and outline completed actions and planned activities to address our recommendations. We have included your response as appendix B to our report.

We appreciate the cooperation that we received from the Office of Enforcement and the Office of Technology and Innovation during our evaluation. Please contact me if you would like to discuss this report or any related issues.

cc: Chris D'Angelo
David Bleicken
Sartaj Alag
Jerry Horton
Joanna Pearl
Glenn Melcher
Elizabeth Reilly

Contents

Introduction

Objective

The Office of Inspector General (OIG) conducted an evaluation of the Consumer Financial Protection Bureau (CFPB) Office of Enforcement's processes for protecting sensitive information. Our objective was to determine whether the Office of Enforcement has effective controls to manage and safeguard access to its confidential investigative information (CII).[1] During the course of our evaluation, we reviewed documentation, interviewed Office of Enforcement employees, and conducted site visits. We did not evaluate whether any unauthorized disclosures of sensitive information occurred. Appendix A contains a description of our scope and methodology.

Background

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) established the CFPB to regulate the offering and provision of consumer financial products and services under federal consumer financial law. The CFPB is responsible for implementing, examining for compliance with, and enforcing federal consumer financial law in accordance with the requirements of the act.

The CFPB may use investigative tools and seek potential remedies for consumers through enforcement actions, such as administrative proceedings or civil actions. Relief available to the CFPB through these civil actions includes cease-and-desist-orders, equitable relief, rescission and reformation of contracts, monetary relief, and civil penalties. The CFPB's jurisdiction covers a wide range of areas, such as mortgage origination and servicing, credit cards, student loans, payday lending, real estate settlement services, and debt collection.

Office of Enforcement Organization and Structure

The Office of Enforcement is one of four offices in the Division of Supervision, Enforcement, and Fair Lending (SEFL).[2] The Office of Enforcement seeks to ensure compliance with federal consumer financial law by initiating investigative activities and enforcement actions when appropriate. The Office of Enforcement investigates parties to identify potential violations of law,

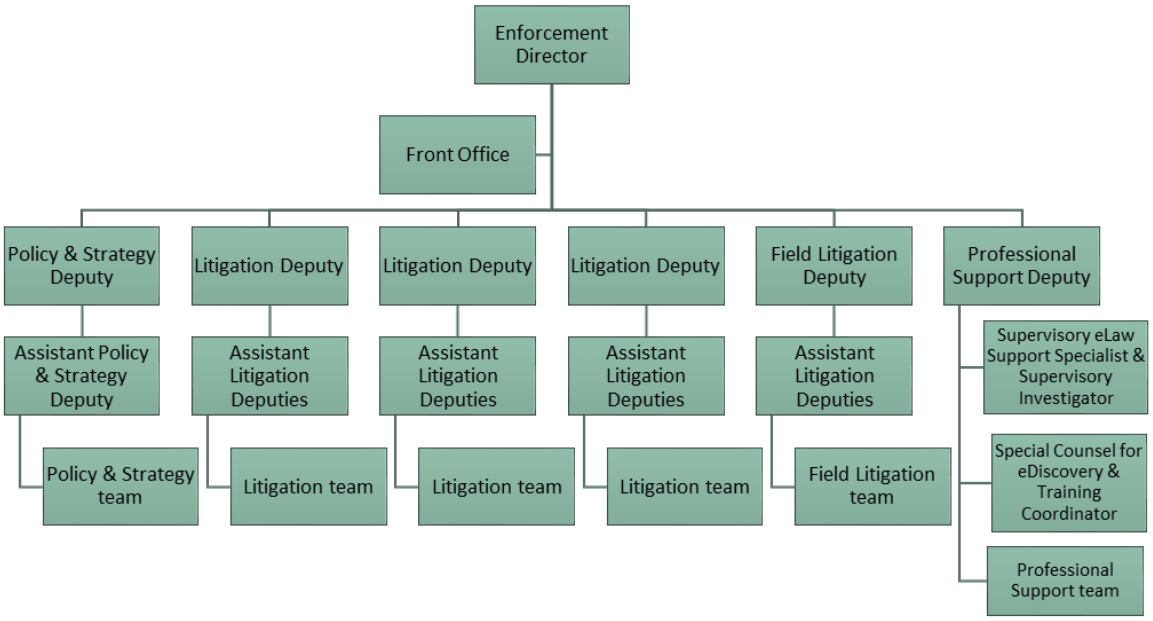
1. While this report focuses on the Office of Enforcement's practices for managing and safeguarding CII, the OIG's Office of Information Technology conducts a broader annual, independent evaluation of the CFPB's information security program, practices, and controls for select systems to meet the annual Federal Information Security Modernization Act of 2014 reporting responsibilities. For our most recent audit, see Office of Inspector General, *2016 Audit of the CFPB's Information Security Program*, OIG Report 2016-IT-C-012, November 10, 2016.

2. SEFL's other three offices are the Office of Supervision Policy, the Office of Supervision Examinations, and the Office of Fair Lending and Equal Opportunity.

including unfair, deceptive, or abusive acts or practices, and investigates practices by companies and individuals that offer or provide consumer financial products or services.[3] As of February 7, 2017, Office of Enforcement investigations and enforcement actions had resulted in approximately $11.5 billion in relief for over 27 million consumers.

The Office of Enforcement includes four litigation teams, each led by a Litigation Deputy and two Assistant Litigation Deputies (figure 1). The teams are staffed by 20–22 attorneys and 3–4 paralegals. The Policy and Strategy team and the Front Office staff, which includes the Office of Enforcement's administrative and resource management officers and legal assistants, provide strategic direction and support for the Office of Enforcement's investigations and litigation efforts. The Office of Enforcement's Professional Support team includes investigators, forensic accountants, statisticians, the Special Counsel for eDiscovery, eLaw Support Specialists and the Training Coordinator. All Office of Enforcement employees participate in the same onboarding process and training sessions for handling and safeguarding confidential information.

Figure 1: Office of Enforcement Organizational Chart



Source: Developed by the OIG based on a review of the CFPB's organizational charts.

Note: This organizational chart is not comprehensive and includes only details relevant to this evaluation.

3. Section 1031 of the Dodd-Frank Act, 12 U.S.C. § 5531, authorizes the CFPB to prevent a covered person or service provider from committing or engaging in an unfair, deceptive, or abusive act or practice under federal law in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service. Unfair, deceptive, or abusive acts or practices are generally defined as either (1) unfair—conduct likely to cause substantial consumer injury that is not reasonably avoidable, when the injury is not outweighed by benefits to consumers or to competition; (2) deceptive—a representation likely to mislead consumers who are acting reasonably under the circumstances, when that representation is material to the consumer's decision; or (3) abusive—conduct that materially interferes with a consumer's ability to understand a term or condition of a product or service or takes unreasonable advantage of the consumer.

The Office of Enforcement's headquarters and Southeast regional office are located in Washington, DC. The office also has regional offices in New York (Northeast), Chicago (Midwest), and San Francisco (West). Each regional office has between five and eight employees. The Field Litigation Deputy at headquarters and two Assistant Litigation Deputies manage the four regional offices.

The Office of Enforcement refers to its cases as *matters*. A team of one to three attorneys and a paralegal generally works on a matter. Depending on the nature and complexity of a matter, other team members may be added, including additional attorneys, forensic accountants, investigators, and data scientists.

The Office of Enforcement uses multiple contractors who specialize in e-discovery work.[4] The CFPB engaged these contractors through the U.S. Department of Justice's Mega 4 contract vehicle, which includes requirements that contractors undergo background checks and sign nondisclosure agreements.[5] An Office of Enforcement representative is responsible for monitoring the contractors' work and reimbursing the U.S. Department of Justice for work performed pursuant to the contract. Contractors work onsite at CFPB headquarters and play an important role in supporting the Office of Enforcement's eDiscovery team.

The Office of Enforcement's Use of Sensitive Information

The Office of Enforcement collects information from the entities subject to its investigations and litigation activities for the purposes of determining whether the law has been violated and conducting the office's mission. Office of Enforcement employees routinely handle CII[6] and may handle confidential supervisory information (CSI) and personally identifiable information (PII), depending on the nature of an investigation.[7]

- *CII* is civil investigative demand[8] material or any documentary material prepared by, on behalf of, received by, or for use by the CFPB or any other federal or state agency in the conduct of an investigation or enforcement action against a person, and any information derived from these documents.

- *CSI* includes any information related to the CFPB's supervisory activities, such as any documents, including reports of examination, prepared by, on behalf of, or for use by the

4. *E-discovery* is the process of identifying, preserving, collecting, reviewing, analyzing, and producing electronically stored information in response to a government investigation or during administrative, civil, or criminal legal actions.

5. The Mega 4 contract is a competitively awarded vehicle managed by the U.S. Department of Justice for the purposes of providing information technology and automated litigation support services to U.S. Department of Justice offices, boards, and divisions, as well as other federal government agencies. The contract is for 6 years (2013–2019).

6. For the purposes of this report, CII may include CSI if the investigation is a result of a supervisory examination and PII if such information is obtained from external entities.

7. CII and CSI are defined in 12 C.F.R. § 1070.2, and PII is defined in Office of Management and Budget Memorandum M-07-16. This evaluation focused on CII that the Office of Enforcement obtains for its litigation and investigative activities and CSI and PII to the extent that they are included in CII. Any reference to sensitive information, confidential information, CII, CSI, or PII does not denote a national security classification.

8. A *civil investigative demand* is a compulsory demand for documentary material, tangible items, reports, answers to written questions, or oral testimony.

CFPB or any other federal, state, or foreign government agency in the exercise of supervisory authority over a financial institution, and any information derived from such documents.

- *PII* is defined as any information that can be used to distinguish or trace an individual's identity, such as the individual's name, Social Security number, or biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name.

The Office of Enforcement's Main Applications and Drives

The Office of Enforcement maintains and stores sensitive electronic data in four electronic applications and two internal drives. Office of Enforcement management relies on one application to manage matter assignments and activities and three applications to review matter-related information. Office of Enforcement teams use two internal drives to store their work products and process electronic data received from entities.

1. **Electronic applications**—The matter management system tracks the status of matters and maintains staff assignments and other administrative tasks related to investigations and litigation activity. In addition, the Office of Enforcement uses three review tools to review matter-related information. These review tools enable users to process and categorize large datasets, search keywords, and identify and organize emails.

2. **Network drive**—The Office of Enforcement stores its work products, such as civil investigative demands and settlements, in folders on its network drive.

3. **Transfer shared drive**—In addition to the network drive, the Office of Enforcement uses a special shared drive that allows the eDiscovery team to load matter-related data received from entities before loading the data to the network drive or the review tools described below. The eDiscovery team uses this shared drive to prepare data for uploading, to fix corrupted data, and to troubleshoot.

The Investigative Information Request Process

The CFPB's rules relating to investigations govern the initiation and conduct of CFPB investigations.[9] Investigations conducted by the Office of Enforcement are formally opened by an authorization from the Assistant Director for the Office of Enforcement after internal review by the CFPB. The Office of Enforcement then typically obtains information through civil investigative demands or voluntary requests.[10] The Office of Enforcement's eDiscovery team reviews incoming submissions and advises litigation teams whether respondents complied with the Office of Enforcement's e-discovery requirements. For example, the eDiscovery team

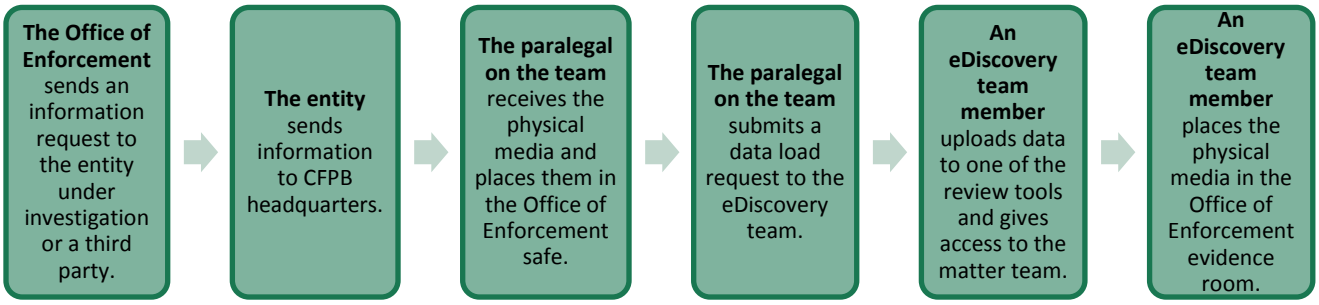
9. 12 C.F.R. § 1080 sets forth the rules that apply to CFPB investigations.

10. A *voluntary request* is a noncompulsory information request that may be used to seek information from an entity.

establishes document submission format requirements to enable proper loading of data to the review tools and encryption requirements for PII submissions.[11]

When requesting information, the Office of Enforcement instructs an entity to send the information to CFPB headquarters. The designated paralegal on the matter at headquarters initiates a data load request, and the eDiscovery team uploads the information to the review tool specified on the request and gives access to the matter team members (figure 2).

Figure 2: Process for Obtaining Information From External Entities



Source: Developed by the OIG based on a review of the Office of Enforcement investigative information intake process.

Policies and Standards for Handling Sensitive Information

The CFPB has developed policies and standards for handling sensitive information that all CFPB employees and contractors must follow. Specifically, in 2012 the CFPB developed the *Handbook for Sensitive Information at the CFPB*, which establishes minimum standards for protecting sensitive information. It explains how (1) to identify sensitive information, (2) to properly handle sensitive information, and (3) to report the loss or compromise of sensitive information. In 2014, the CFPB developed its *Information Sensitivity Leveling Standard* to guide the process of assigning sensitivity levels (*public*, *low*, *medium*, and *high*) to information held by the CFPB. According to these standards, CII is considered high-sensitivity information. The CFPB also published its *Policy on Information Governance at the CFPB* in 2014, which states that access to high-sensitivity information requires a demonstrated business need.

According to a CFPB official, the agency affords each division the discretion to interpret agency-level policies and procedures in a manner consistent with the division's operational needs. The CFPB regulation covering confidential information prohibits current or former employees from disclosing confidential information to any employee unless it is relevant to that employee's assigned duties.[12] CFPB officials indicated that the Office of Enforcement has interpreted the relevance standard contained in the regulation to be consistent with the CFPB's demonstrated

11. The *Federal Rules of Civil Procedure* govern the procedure in all civil actions and proceedings in the United States district courts. In particular, *Federal Rules of Civil Procedure* 26 through 37 guide the discovery process.

12. 12 C.F.R. § 1070.41 prohibits current or former employees or contractors or consultants of the CFPB, or any other person in possession of confidential information, from disclosing such confidential information by any means to (1) any person who is not an employee, contractor, or consultant of the CFPB or (2) any CFPB employee, contractor, or consultant when the disclosure of such confidential information to that employee, contractor, or consultant is not relevant to the performance of the employee's, contractor's, or consultant's assigned duties.

business need standard outlined in the policy, meaning that access to the office's sensitive information should be based on the relevance of the information to the employee's assigned duties.

In addition, SEFL and the Office of Enforcement have issued a memorandum and procedures specific to the handling of and access to Office of Enforcement confidential information. The *SEFL Staff Memorandum 2014-01*, issued in January 2014, requires that Office of Enforcement employees store investigation material in a folder on the Office of Enforcement's network drive to which access is limited to the employees and supervisors working on the investigation. In addition, the Office of Enforcement's Policies and Procedures Manual, as updated in September 2015, required its employees to restrict access to matter folders on the network drive to those employees working on the matter.[13]

Office of Enforcement employees participate in training programs on the proper handling and safeguarding of sensitive information. In 2015, the Office of Enforcement developed its Enforcement Orientation: Sensitive and Confidential Information Training for new employees, which includes guidelines for protecting confidential information, including advising employees to share confidential information only with colleagues with a need to know. All SEFL employees, including those in the Office of Enforcement, are also required to take the annual CSI training, The Treatment of CSI, which includes instruction on safeguarding information shared by other agencies, limiting access to nonpublic information, and handling CSI. In addition, Office of Enforcement employees participate in annual PII training that is organized by the CFPB's Privacy Office. The training is role based and intended to reflect PII scenarios that employees may encounter in their routine job duties.

13. According to Office of Enforcement officials, an additional update to the manual was made after the conclusion of our fieldwork that revised this requirement to reflect the Office of Enforcement's current process.

Finding 1: The Office of Enforcement's Approach to Matter Folder Access Limits Its Ability to Safeguard Sensitive Information

We found that despite recent improvements in the Office of Enforcement's practices for managing access rights to its matter folders, access to sensitive information contained in its review tools and its network drive was not restricted to employees who needed access to that information to perform their assigned duties, in accordance with CFPB and division-specific policies and expectations. Specifically, access to certain matter folders containing high-sensitivity, raw investigative information on the Office of Enforcement's three review tools and network drive was not limited to the employees assigned to the matter.[14] We found that all users have the appropriate level of access to the Office of Enforcement's transfer shared drive. The CFPB's *Information Sensitivity Leveling Standard* requires that access to high-sensitivity information be restricted to users with a demonstrated business need, which the Office of Enforcement interprets as relevance to assigned duties, and recommends that high-sensitivity information be stored in a central, access-controlled location. Further, the CFPB's *Handbook for Sensitive Information* states that sensitive information should be stored electronically using restricted folders. In addition, SEFL and the Office of Enforcement have issued a memorandum and procedures specific to the network drive to reinforce these requirements. Users had access to matter folders containing information not relevant to their assigned duties primarily because of challenges in keeping access rights current. For example, the Office of Enforcement did not always terminate access rights for employees who left the agency or who moved to another division. If access to matter folders is not appropriately restricted based on relevance to assigned duties, CII will be available to employees who do not need access to that information to perform their assigned duties, increasing the risk of inadvertent or unauthorized disclosure.

Access to Review Tools Was Not Always Limited to Employees Who Needed Access to Perform Their Assigned Duties

We found that access to the Office of Enforcement's three review tools[15] was not limited based on relevance to Office of Enforcement employees' assigned duties. Specifically, we found that 99 of 127 matter folders in review tool A (78 percent), 25 of 135 matter folders in review tool B (19 percent), and 4 of 32 matter folders in review tool C (13 percent) were able to be accessed by at least one user who did not need access to perform the user's assigned duties.

14. Raw data acquired through Office of Enforcement authorities, or otherwise constituting CII, is considered high-sensitivity information according to the CFPB's standards. Information with a sensitivity rating of *high* carries a significant legal, reputational, or financial risk to the CFPB, individuals, or business entities should it be improperly accessed, used, or disclosed.

15. The Office of Enforcement stores CII obtained from third parties in its three review tools.

Overall, we found that 113 unique users had access to at least one of the review tools when they no longer needed it.[16] The Office of Enforcement explained that each identified instance of a user with access to information not relevant to the performance of the user's assigned duties fell into one of the following five categories:

1. The user was no longer in the Office of Enforcement.
2. The user was previously on detail from another CFPB office but had since returned to his or her original office and no longer required access.
3. The user did not have current approval from an Assistant Litigation Deputy.[17]
4. The user's role changed.
5. The user was no longer employed by the CFPB.[18]

Among these five categories, 72 of the 113 users with access to information not relevant to the performance of their assigned duties (64 percent) are still employed by the agency and bound by certain civil and criminal restrictions on releasing confidential information; nonetheless, the employees' access to such confidential information presents a potential risk. We also determined that Office of Enforcement contractors need access to matter folders to upload information and grant access to the matter teams; therefore, the contractors' access rights were relevant to their assigned duties.

The OIG's Methodology for Comparing Access Rights

We used the Office of Enforcement's matter management system as of April 2016 as a baseline to determine the assigned team members associated with each matter. We compared user access data from the Office of Enforcement's three review tools and the transfer shared drive to the team members identified in the matter management system to verify that access to matter information is restricted to matter team members. We obtained feedback from the Office of Enforcement for all discrepancies and adjusted the results accordingly.

16. For each review tool, we analyzed the Office of Enforcement's explanations for users with access not relevant to their assigned duties. To avoid the potential for double counting, we analyzed these explanations by unique user. For example, one user may have had access to five different matter folders in a review tool not relevant to the user's assigned duties; because all explanations for a particular user were identical, we only counted each unique user one time in our analysis. Explanations for unique users with access not relevant to their assigned duties are depicted in the pie charts in figures 3, 4, and 5.

17. This category describes users who previously needed access to the information in the related matter folder to perform their assigned duties but no longer require access to that information.

18. These situations present limited risk to the agency because individuals who have left the CFPB should not have access to CFPB systems.

Review Tool A

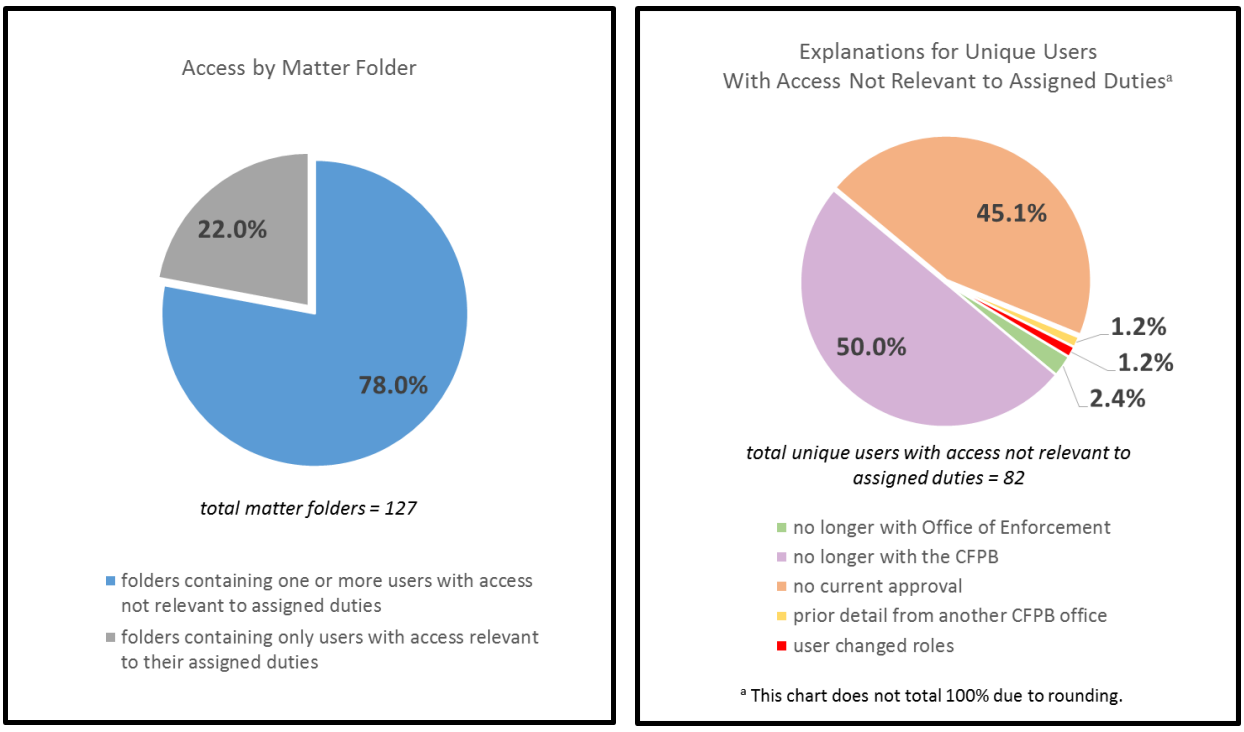
We found that 82 of the 113 unique users had access to matter folders in review tool A when the information was no longer relevant to the performance of their assigned duties. Half the instances (41 of 82) of users having access to information not relevant to their assigned duties in review tool A were employees no longer employed by the CFPB. These situations present limited risk to the agency.[19]

As shown in figure 3, 2.4 percent of review tool A's users who had access to information not relevant to the performance of their assigned duties were employees no longer with the Office of Enforcement but still employed by the CFPB. Figure 3 also shows that 1.2 percent of the users were employees who had been, but no longer were, on detail to the Office of Enforcement from another CFPB office. These instances pose a risk to the CFPB because as current CFPB employees, they have access to the matter folders in review tool A.

About 45 percent of review tool A's unique users who had access to information not relevant to the performance of their assigned duties were employees who did not have current approval from the Litigation Deputy or an Assistant Litigation Deputy. These employees were working in the Office of Enforcement, but access to the sensitive information in those matter folders did not appear to be relevant to their current assignments. Additionally, one employee changed roles in the Office of Enforcement but still had access to previously assigned matter folders.

19. Individuals who have left the CFPB should not have access to the CFPB's network and, by extension, the matter folders.

Figure 3: Access Results for Review Tool A

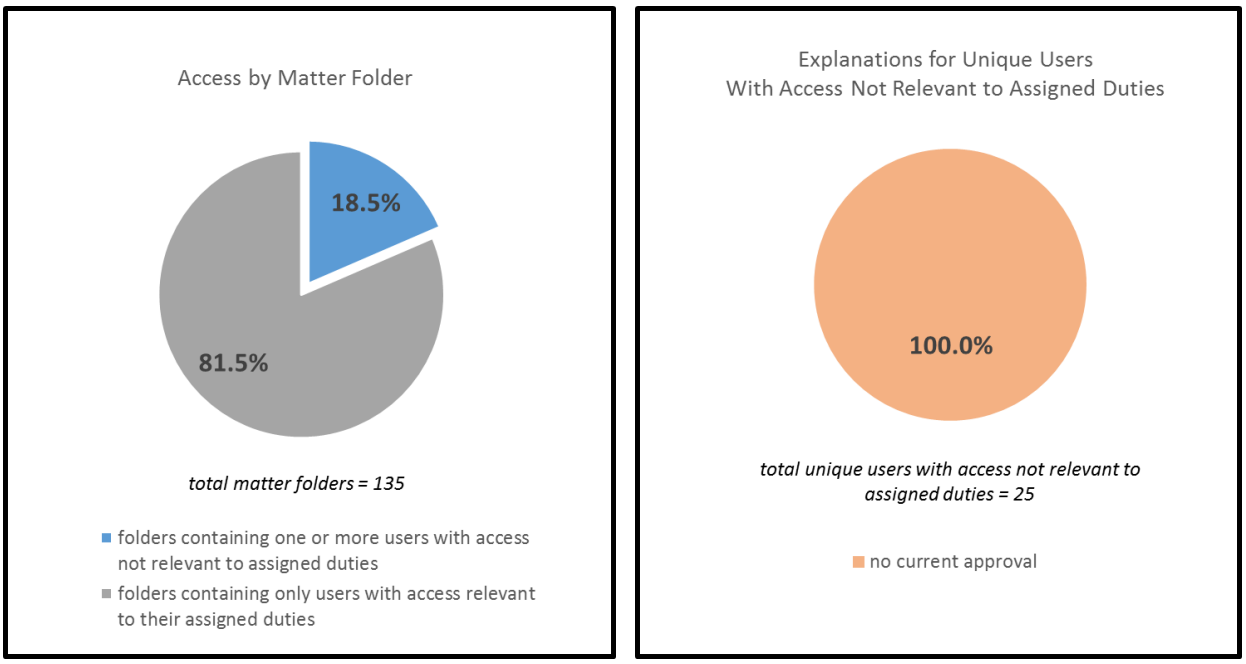


Source: Developed by the OIG based on the results of our access rights comparisons and explanations provided by the Office of Enforcement.

Review Tool B

We found that 25 of the 113 unique users had access to matter folders in review tool B when the information was no longer relevant to the performance of their assigned duties. As shown in figure 4, all 25 were employees who did not have current approval for access from the Litigation Deputy or an Assistant Litigation Deputy.

Figure 4: Access Results for Review Tool B

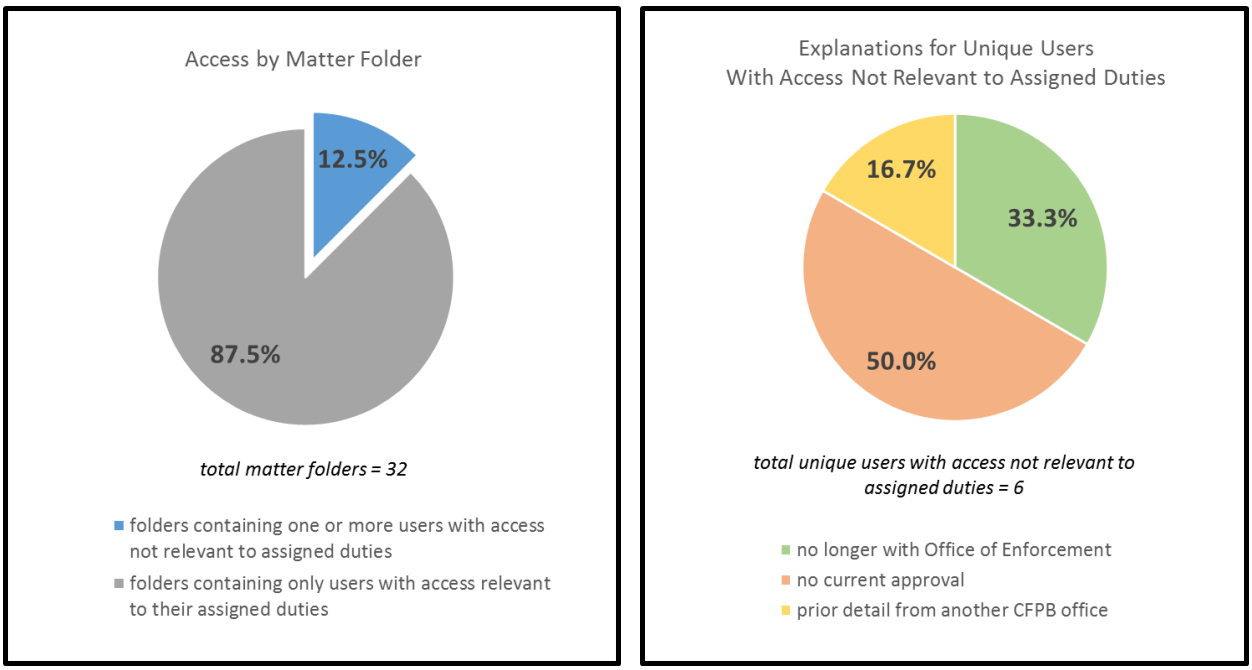


Source: Developed by the OIG based on the results of our access rights comparisons and explanations provided by the Office of Enforcement.

Review Tool C

We found that 6 of the 113 unique users had access to matter folders in review tool C when the information was no longer relevant to the performance of their assigned duties. As shown in figure 5, two employees were no longer with the Office of Enforcement but were still employed by the CFPB, and one employee was detailed from another CFPB office and has since returned to that office. These instances may pose a risk to the agency because these individuals are still CFPB employees with network access and have access to review tool C. We found that employees who did not have current approval from the Litigation Deputy or an Assistant Litigation Deputy accounted for the remaining instances of access to the information not relevant to their assigned duties.

Figure 5: Access Results for Review Tool C



Source: Developed by the OIG based on the results of our access rights comparisons and explanations provided by the Office of Enforcement.

Transfer Shared Drive

We found that all users have appropriate access to matter folders in the Office of Enforcement's transfer shared drive. Access to the transfer shared drive is limited to the Office of Enforcement's contractors, members of the CFPB's Office of Technology and Innovation (T&I), and members of the eDiscovery team.

The CFPB Requires Restricted Access to High-Sensitivity Information

The Office of Enforcement stores CII obtained from third parties in its three review tools, and according to CFPB standards, these data have a sensitivity rating of *high*. The CFPB's *Information Sensitivity Leveling Standard* requires that access to high-sensitivity information be restricted to users with a demonstrated business need. The standard also states that high-sensitivity information should be stored in a central, access-controlled location. Further, the CFPB *Handbook for Sensitive Information* states that sensitive information should be stored electronically using restricted folders.

Internal Controls Should Be Monitored to Ensure They Remain Effective

The U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government* states the importance of controls, including ongoing monitoring of internal controls. Managers should continually assess and evaluate whether the appropriate employees have access to confidential information. Once-effective procedures can become less effective over time, or the application of controls may change. Such changes can result from the arrival of new personnel, the variability of training and supervision, time and resource constraints, or other factors. Monitoring ensures that internal control continues to operate effectively and is accomplished by (1) appropriate personnel assessing the design and operation of controls on a suitably timely basis and (2) management taking necessary actions to address any issues.

Access Rights Were Not Regularly Reviewed and Kept Current

Challenges with monitoring, terminating, and maintaining access rights resulted in access to the review tools for employees who did not need it to perform their currently assigned duties. T&I grants access to review tools A and C, which are housed on the CFPB network. A third-party vendor owns and manages review tool B, which is stored on the vendor's server. One Office of Enforcement eDiscovery team lead explained that the review tools are capable of producing reports to monitor user access, and the eDiscovery team is expected to initiate removal of a user's access to the review tools when the team is informed that an employee has left the CFPB. The eDiscovery team lead stated that the Office of Enforcement requests quarterly access reports from the contractor. It does not appear that the Office of Enforcement used these reports to confirm that access had been restricted appropriately.

Further, the Office of Enforcement's policies and procedures do not include any requirements to periodically monitor user access to its review tools. These policies and procedures also do not specify how Office of Enforcement employees should determine which employees have a need to access a particular matter folder because it is relevant to their assigned duties.

Management Action Taken During Evaluation

After we communicated the preliminary results of our access rights comparisons, in July 2016 the Office of Enforcement removed access to the three review tools for users identified as not requiring access to perform their assigned duties. A senior official stated that the Office of Enforcement determined who should have access to various matter folders in the review tools by seeking approval from Assistant Litigation Deputies and Litigation Deputies. After reviewing and updating the approvals and denials, the Office of Enforcement updated its matter management system to accurately reflect the users assigned to each matter.

The Office of Enforcement Improved Network Drive Access Restrictions but Opportunities Exist for Continued Improvement

As of December 2015, the Office of Enforcement generally allowed broad access to its matter folders on the network drive to all Office of Enforcement employees. Office of Enforcement officials were aware of the network drive's broad access issues and began discussing the concern with T&I in September 2015. In March 2016, the Office of Enforcement requested that T&I restrict access to the network drive matter folders and subsequently provided us with the network drive access data discussed below.

In April 2016, T&I, at the request of the Office of Enforcement, produced a report of over 66,000 folders on the Office of Enforcement's network drive. Although we could not conduct our access rights comparisons due to format limitations, we performed a brief review in April 2016 of the users with access to three of the Office of Enforcement's matter folders. We compared the number of users with access to the number of users who needed access to perform their assigned duties; we used the Office of Enforcement's new approach, implemented in May 2016, to determine which users needed access. We found that the number of users with access to the network drive matter folders exceeded the number of users who needed the information to perform their assigned duties (table 1).

Table 1: Number of Users[a] With Access to Selected Matter Folders on the Network Drive

Matter folder	Number of users with access	Number of users for whom the information is relevant to their assigned duties[b]
Matter A	133	29
Matter B	131	24
Matter C	59	27

Source: OIG compilation based on T&I's report on network drive access as of April 2016, the matter management system access report, and the Office of Enforcement's determination of users for whom the information was relevant to their assigned duties as of June 2016.

[a]Users include employees, contractors, and groups that have access to the matter folder. We counted each group as one user regardless of the number of users contained in the group.

[b]These users include (1) matter team members, (2) administrative staff, (3) the eDiscovery team, and (4) senior management.

The CFPB Requires Restricted Access to the Network Drive

The CFPB maintains general policies requiring restricted access to high-sensitivity information.[20] SEFL and the Office of Enforcement developed more detailed policies that require matter folder access to be restricted to those employees working on a matter. More specifically, the *SEFL Staff Memorandum 2014-01* requires information to be stored in limited-access folders on the network drive available only to the team members working on a particular investigation and the

20. As discussed above, the CFPB's *Information Sensitivity Leveling Standard* requires that access to high-sensitivity information be restricted to users with a demonstrated business need and recommends that high-sensitivity information be stored in a central, access-controlled location. The CFPB *Handbook for Sensitive Information* states that sensitive information should be stored electronically using restricted folders.

appropriate Office of Enforcement senior team members and support staff, unless materials are needed for use in the matter outside the Office of Enforcement. In addition, the Office of Enforcement's *Policies and Procedures Manual*, which was in effect during our fieldwork, required its employees to restrict access to matter folders on the network drive to those working on a matter.

The Office of Enforcement Implemented and Enhanced Its Network Drive Access Approach in May 2016

In May 2016, the Office of Enforcement completed a new group-based approach to restrict network drive access to only the matter team members, senior management, the eDiscovery team, and administrative staff.[21] The Office of Enforcement informed its employees that network access approval would be granted to only those assigned to the matter and clarified that employees must request access through Front Office employees. The office's new approach also requires the matter management system to reflect the employees' current assignments. We obtained new data and performed access rights comparisons for the new access settings for Office of Enforcement matter folders and found that the network drive matter folders were generally restricted to those employees who needed access to perform their assigned duties.[22] We found two employees who had access to a matter folder for which the information was not relevant to their currently assigned duties; we understand that the Office of Enforcement subsequently restricted access for those two employees.

Evolving Procedures, Legacy System, and Lack of an Office-Specific Standard for Determining Access Cause Network Drive Challenges

The absence of a clear, documented, office-specific standard for determining which employees have a need to access high-sensitivity information because it is relevant to their assigned duties contributed to instances of unrestricted access to the Office of Enforcement's network drive matter folders. CFPB officials indicated that the Office of Enforcement has construed the relevance requirement in the regulation covering confidential information to be consistent with the CFPB's demonstrated business need standard, and access to the office's sensitive information should be based on the relevancy of the information to employees' assigned duties. The CFPB has issued several guidance documents that address privacy and information security, yet the Office of Enforcement has not documented (1) its approach to employee access to the network drive or (2) its relevance standard interpretation. We found that access to the Office of Enforcement's sensitive information has generally been granted on a discretionary basis. For example, in June 2016, one Office of Enforcement attorney indicated that the onus for determining need to know had been on the person requesting access. This attorney believed that the Office of Enforcement worked under the presumption that if an employee asked for access, that person automatically had a need to know or a need to access that information.

21. The Office of Enforcement's current procedures require that matter team members gain access to the office's network drive by contacting the office's administrative staff. The administrative staff verify that the employees are assigned to the matter and then contact T&I to create the matter folder and grant access to only the team members.

22. We obtained a list of the new user groups for all open matters and verified that the users with access to each matter folder were listed in the Office of Enforcement's matter management system for the associated matter.

In addition, the Office of Enforcement's practices for restricting access to network drive matter folders have been evolving. The Office of Enforcement's *Policies and Procedures Manual*, which was in effect during our fieldwork, required individual team members to contact T&I to restrict access to matter folders to those working on a matter, relying on the discretion of these team members. The Office of Enforcement changed its practice in 2014 by designating one Front Office employee as responsible for approving access requests and communicating those access requests to T&I. The Office of Enforcement did not document this new procedure, however, and an Office of Enforcement official informed us that employees were not always following this procedure. We found that Office of Enforcement employees had various options for obtaining network drive access approval, including obtaining approval from the matter's lead attorney, Litigation Deputy, or Assistant Litigation Deputy and contacting T&I directly to request network drive access or to request that access to the network drive be restricted.

Further, according to Office of Enforcement management, the prior use of a legacy system and the subsequent migration away from that system caused network access restriction challenges. When the CFPB was first established, it used a shared drive hosted by the U.S. Department of the Treasury. According to an Office of Enforcement official, when the CFPB migrated from this shared drive, the access permission for the shared drive folders did not transfer accurately to the CFPB's new system. Additionally, Office of Enforcement employees were able to create new network drive folders for new matters but could not define the access restrictions. When employees created these folders to begin work on a new matter, access was automatically provided to all Office of Enforcement employees. One Office of Enforcement official explained that no one in the Office of Enforcement can directly restrict access to the network drive folders; employees rely on T&I to apply the requested permission settings to network drive folders.

Management Action Taken During Evaluation

During our evaluation, the Office of Enforcement began addressing its network access challenges. As of June 2016, the Office of Enforcement restricted closed matter folders to only the administrative staff. Further, in November 2016, the Office of Enforcement started preparing for the CFPB-wide migration to a new cloud environment, which is intended to replace the current network drive. In February 2017, Office of Enforcement officials indicated that the office has begun developing a policy for managing access to confidential information that is consistent with the CFPB's regulations.

Summary

At the outset of our evaluation, we found that access to matter folders containing high-sensitivity, raw investigative information on the Office of Enforcement's three review tools and the network drive was not limited to employees who needed access to perform their assigned duties. Following the results of our review tool access rights comparisons, the Office of Enforcement removed access for users for whom the information was not relevant to their currently assigned duties and updated its matter management system accordingly. Similarly, the Office of Enforcement made improvements to its approach to network drive access restrictions in May 2016. As of February 2017, the office was in the process of developing a policy for managing access to its review tools and network drive; however, it needs to implement a process for monitoring access. The Office of Enforcement has provided guidance to its employees but has not

incorporated its access approval practices or its interpretation of the CFPB's demonstrated business need standard into the office's *Policies and Procedures Manual*. Further, the Office of Enforcement's *Policies and Procedures Manual* does not describe processes for monitoring or terminating network drive or review tool access. Not keeping access rights to CII limited to employees who have a current business need to access the information increases the risk of improper access, use, or disclosure of CII maintained by the Office of Enforcement.

Recommendations

We recommend that the Assistant Director of the Office of Enforcement

1. Formalize in policy that employees should be granted access to the Office of Enforcement's review tools and network drive matter folders only when such access is relevant to their assigned duties.

2. Update policies and procedures to specify the process for approving and updating matter folder access rights for the Office of Enforcement's review tools and network drive.

3. Expand existing training for Office of Enforcement employees to reinforce the guidance on

    a. the office's interpretation that *demonstrated business need* means relevance to performing assigned duties.

    b. the access approval and updating process for the Office of Enforcement's review tools and network drive.

4. Develop and implement a monitoring and testing approach to periodically confirm that the Office of Enforcement's matter folders are appropriately restricted.

5. Coordinate with the Chief Information Officer to ensure that the new cloud environment, which is intended to replace the network drive, includes access approval and monitoring capabilities that meet the current and future needs of the Office of Enforcement.

Management's Response

In the response to our draft report, the Associate Director of SEFL and the Assistant Director of the Office of Enforcement concur with recommendations 1, 2, 3, 4, and 5. The Associate Director and Assistant Director note that the Office of Enforcement has developed and is implementing a standard for access to confidential information that is consistent with the CFPB's regulations and has developed a procedure for approving and updating matter folder access rights for the office's review tools and network drives. The Associate Director and Assistant Director also state that the office has expanded its existing mandatory training and has implemented a monitoring and testing process to confirm that matter folders are properly restricted. Finally, the Associate Director and Assistant Director note that the Office of Enforcement will work with T&I to select and

implement a new cloud environment for the CFPB and will ensure that access rights will be granted in a manner that is consistent with the OIG's recommendations.

OIG Comment

The actions described by the Associate Director of SEFL and the Assistant Director of the Office of Enforcement appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 2: Inconsistencies in Safeguarding Sensitive Information Could Result in Unauthorized Disclosure

We found that Office of Enforcement employees do not consistently follow agency expectations for safeguarding printed sensitive information. Specifically, we found that Office of Enforcement employees (1) do not label information according to the CFPB's established sensitivity levels, (2) do not routinely use cover sheets for sensitive information, and (3) do not always store sensitive information in locked locations. The CFPB has established rules, guidance, and expectations for all employees and contractors concerning the storage, access, use, and disclosure of sensitive information in its *Information Sensitivity Leveling Standard* and its *Handbook for Sensitive Information*. We attribute the inconsistent safeguarding of printed sensitive information to a lack of awareness on the part of Office of Enforcement employees about the CFPB's guidelines for handling sensitive information and a lack of office-specific procedural guidance. As a result, Office of Enforcement employees use inconsistent practices for handling and safeguarding sensitive information, increasing the risk of inadvertent and unauthorized disclosures.

Office of Enforcement Attorneys and Paralegals Do Not Consistently Follow Internal Information Handling and Safeguarding Standards

We found that Office of Enforcement attorneys and paralegals do not label documents in accordance with the *Information Sensitivity Leveling Standard*. Instead, these employees label documents in various ways, often in accordance with requirements contained in litigation agreements. Examples of terminology that attorneys and paralegals currently use to label documents include *confidential*, *sensitive*, *PII*, *CII*, *CSI*, *deliberative*, and *privileged*.

We also found that cover sheets are not used consistently, as recommended in the *Handbook for Sensitive Information*.[23] At headquarters, a standard cover sheet is automatically printed at the beginning of every printed document, regardless of the document's content and sensitivity level. We found that cover sheets are not automatically printed at one of the CFPB's regional offices, however, and none of the attorneys and paralegals we spoke with at that office currently use cover sheets for sensitive materials.

In addition, although the Office of Enforcement's office space is guarded and access to it is controlled, we learned during our interviews that many Office of Enforcement attorneys did not have office doors or cabinets in their offices that can be locked. As a result, attorneys sometimes leave sensitive information in unsecured places, such as on bookshelves and desktops or in nonlocking cabinets, despite their awareness that sensitive information should be stored in a secure, access-controlled location.

23. The *Handbook for Sensitive Information* states that CFPB employees and CFPB contractors should print a cover sheet at the beginning of any document containing sensitive information.

Internal Guidance Sets Forth Handling and Safeguarding Requirements

The CFPB's *Information Sensitivity Leveling Standard* requires that all information held by the agency be assigned a sensitivity level (*high*, *medium*, *low*, or *public*), which in turn determines storage, access, use, and disclosure requirements. The *Information Sensitivity Leveling Standard* states that all CII is considered high-sensitivity information and should be secured in an access-controlled location, with access limited to those with a demonstrated business need. Additionally, the *Handbook for Sensitive Information* recommends that employees print documents containing sensitive information only when necessary and that they print a cover sheet at the beginning of any document containing sensitive information.

Lack of Awareness of CFPB Guidelines and Absence of Specific Office of Enforcement Procedures Led to Inconsistent Practices

The Office of Enforcement attorneys and paralegals we interviewed were not aware of certain aspects of the guidance in the *Information Sensitivity Leveling Standard* and the *Handbook for Sensitive Information*. In addition, employees are unclear as to how these broad CFPB-wide policies apply to their daily work activities. In the absence of specific Office of Enforcement procedures, attorneys and paralegals have developed their own informal practices for handling and safeguarding sensitive information, which has led to inconsistent practices across the Office of Enforcement. For example, one Office of Enforcement attorney we interviewed explained that she routinely labels her internal work products as "attorney work product—privileged and confidential," but she did not know whether other attorneys in her office followed the same protocol.

Inconsistent Practices Increase Risk of Inadvertent and Unauthorized Disclosures

The nature of the Office of Enforcement's routine activities differs from other CFPB offices and may warrant creating additional guidance and procedures for the proper safeguarding of sensitive information. The CFPB's *Permissible Use Standard* gives SEFL the authority to develop and maintain its own procedures regarding the use of information for which it is responsible. Establishing clear Office of Enforcement standards for the labeling of documents and corresponding practices for handling each type of document, including the use of cover sheets, would help to ensure that Office of Enforcement employees properly handle and safeguard CII. Specific operational guidance may help to standardize practices and mitigate the risk of inadvertent and unauthorized disclosures of sensitive information.

Management Action Taken During Evaluation

During our evaluation, the Office of Enforcement began to address the issue of unsecured employee offices and cabinets with the CFPB's Facilities Office. The Office of Enforcement and the Facilities Office identified office door and cabinet locks without keys, obtained the appropriate keys for those locks, tested those keys, and issued the keys to the appropriate

employees. The Facilities Office also identified hallway cabinets that did not lock. As of October 2016, the Office of Enforcement has resolved these issues.

Recommendations

We recommend that the Assistant Director of the Office of Enforcement

6. Develop and implement operational procedures specific to the Office of Enforcement for handling printed high-sensitivity information, including but not limited to information labeling requirements and the use of cover sheets.

7. Establish a strategy to periodically reinforce handling and safeguarding requirements and establish a monitoring approach to test compliance with information handling and safeguarding policies and procedures.

8. Monitor securable, access-controlled storage space, including but not limited to lockable cabinets and offices, to ensure that it meets the needs of all Office of Enforcement employees.

Management's Response

In the response to our draft report, the Associate Director of SEFL and the Assistant Director of the Office of Enforcement concur with recommendations 6, 7, and 8. The Associate Director and Assistant Director note that the Office of Enforcement will develop standard language for all cover sheets to reflect the sensitive nature of the printed information. The Associate Director and Assistant Director also state that the office has developed mandatory training on information handling and safeguarding requirements as well as a monitoring approach to test compliance with information handling and safeguarding policies and procedures. Finally, the Associate Director and Assistant Director note that the Office of Enforcement now has access-controlled storage available to all staff.

OIG Comment

The actions described by the Associate Director of SEFL and the Assistant Director of the Office of Enforcement appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 3: Lack of Naming Convention Hinders Access Monitoring and Maintenance Across Applications and Internal Drives

Our access rights comparisons revealed that the Office of Enforcement has inconsistent names for matter folders across its four main applications and two internal drives. The Office of Enforcement's *Policies and Procedures Manual*, "Document Maintenance and Retention Policies" section, states the importance of maintaining uniform, complete, and accurate matter files. We attribute these inconsistencies to the lack of a uniform naming convention for matter folders. Inconsistent matter folder names may hinder the ability of Office of Enforcement management to accurately and efficiently monitor and maintain access to the various applications and internal drives.

Folder Naming Conventions Were Not Uniform

When we compared the review tools and internal drives that contain documents and matter-related data with the matter management system to assess uniformity, we found that matter folder names were not uniform within or across applications and internal drives. Our comparisons revealed the following:

- 15 instances of duplicate matter folders in a single review tool or internal drive; these folders have the same matter number but different names.
- Over 400 instances of the same matter having a different name than the name in the matter management system; these folders have the same matter number in each application and internal drive, but the matter folder name itself is different.
- 72 instances in which the matter numbers differed for the same case across applications and internal drives.

In addition, as a result of our comparisons, the Office of Enforcement identified application-generated errors that resulted in discrepancies in matter numbers between applications and internal drives. In particular, the Office of Enforcement identified an issue in the matter management system that resulted in a new matter number being assigned to an existing matter when certain data were updated or revised. This issue resulted in the existing matter having two assigned matter numbers, which led to matter number discrepancies between applications and internal drives.

The Office of Enforcement's "Document Maintenance and Retention Policies" states,

> Maintaining uniform, complete, and accurate matter files that document relevant developments throughout the course of Enforcement matters is critical for information sharing, continuity (following personnel turnover), effective litigation management (including the maintenance of litigation holds), Bureau compliance with the Freedom of Information Act (FOIA) and discovery obligations, and file sharing with other law enforcement agencies.

This guidance notwithstanding, the Office of Enforcement did not have specific naming convention guidelines. Office of Enforcement employees had been creating matter folders and matter names on an ad hoc basis, which resulted in the inconsistencies we identified.
The existence of multiple names for the same matter folder within a single review tool or internal drive hinders senior management's ability to locate documents as well as assign and monitor access to matter folders. There is also a risk that neither of the duplicate folders for a single matter contains the complete documentation or data for that matter, which makes it more difficult for senior management to efficiently respond to Freedom of Information Act requests and share files with other law enforcement agencies. In addition, inconsistent folder names across applications and internal drives creates a risk that access to the wrong matter folder could be granted because of confusion over the matter name. Further, inconsistent folder names could hinder the Office of Enforcement's ability to verify, maintain, and terminate access to matter folders within the various applications and internal drives and efficiently locate documents and data within matter folders. A policy establishing a uniform naming convention to be used for all applications and internal drives would lead to more efficient access monitoring and complete matter folders.

Management Action Taken During Evaluation

During our evaluation, the Office of Enforcement started a new process across all applications and internal drives in which all matter folder names begin with the matter number followed by the matter name in parentheses. Senior management indicated, however, that review tool limitations have affected the Office of Enforcement's ability to implement this new strategy and correct current inconsistencies in matter names across applications and internal drives. Review tools A and C do not allow matter folders to be renamed, and review tool A has a character limit for folder names. Senior management expressed interest in overcoming the character limitation for review tool A and resolving inconsistencies going forward. Further, when we identified the issue in the matter management system that resulted in multiple matter numbers for the same matter, the Office of Enforcement used comparison reports generated during the evaluation to correct the inaccurate matter numbers in the matter management system.

Recommendation

We recommend that the Assistant Director of the Office of Enforcement

9. Develop a policy to establish a standard naming convention for matter folders and other relevant Office of Enforcement folders to be used across all Office of Enforcement applications and internal drives.

Management's Response

In the response to our draft report, the Associate Director of SEFL and the Assistant Director of the Office of Enforcement concur with recommendation 9. The Associate Director and Assistant Director note that the Office of Enforcement established a standard naming procedure and limited the ability to create new matter folders on the network drive to the Front Office staff.

OIG Comment

The actions described by the Associate Director of SEFL and the Assistant Director of the Office of Enforcement appear to be responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Appendix A
Scope and Methodology

We reviewed the Office of Enforcement's management and safeguarding of CII. In our review of the office's processes for obtaining matter-related information, we conducted a walk-through of the process and reviewed applicable documents, such as the data load request form. In our review of the office's process for sharing matter-related information with other government agencies and subject-matter experts, we reviewed applicable documentation, including information sharing agreements, memorandums of understanding, and nondisclosure agreements.

We interviewed Office of Enforcement officials, attorneys, paralegals, Front Office staff, training coordinators, and contractors to gain an understanding of how information is handled and maintained. We also interviewed employees in T&I to understand how data were extracted from the review tools and internal drives for our access rights comparisons.

We reviewed the CFPB's related policies and procedures, including the *Handbook for Sensitive Information*, the *Information Sensitivity Leveling Standards*, the *Policy on Information Governance at the CFPB*, and the Office of Enforcement's *Policies and Procedures Manual*. We also reviewed a SEFL and Office of Enforcement–specific memorandum and relevant training materials.

We conducted Office of Enforcement site visits in Washington, DC, and San Francisco, California. We conducted an onsite review in Washington, DC, (1) to verify the Office of Enforcement's data intake process and outgoing production in relation to information sharing practices, (2) to confirm installation of office drawer locks and cabinet locks in offices and hallways, and (3) to confirm acquisition of data disposition tools. We conducted interviews at the San Francisco regional office with Office of Enforcement employees to gain an understanding of policies and procedures and employees' individual practices for safeguarding CII.

To evaluate the Office of Enforcement's process for managing access to its key applications and internal drives, we compared access rights to data maintained in the Office of Enforcement's review tools and drives. We used the Office of Enforcement's matter management system as a baseline to determine the team members associated with each matter.[24] We compared user access data from the Office of Enforcement's three review tools and transfer shared drive to the identified team members in the matter management system as of April 2016 to determine whether access to matter information was restricted to matter team members. We also compared data from the Office of Enforcement's network drive as of June 2016, as access to the network drive folders changed throughout the evaluation from individual-based access to group membership access. We compared the employees included in a group membership to the team members listed in the matter management system.

We conducted our fieldwork from February 2016 through July 2016. We performed our evaluation in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

24. The Office of Enforcement agreed with our approach of using the matter management system as a baseline for our comparisons.

Appendix B
Management's Response

Consumer Financial Protection Bureau

1700 G Street NW, Washington, DC 20552

April 14, 2017

Ms. Melissa Heist
Associate Inspector General for Audits and Evaluations
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau
20th and Constitution Avenue
Washington, DC 20551

Dear Ms. Heist,

Thank you for the opportunity to review and comment on the Office of Inspector General's draft report *The CFPB Can Improve Its Practices to Safeguard the Office of Enforcement's Confidential Investigative Information*.

The Bureau appreciates the OIG's review and notes that none of the identified opportunities for improvement ever resulted in any breach of confidential information outside the Bureau. Nonetheless, the Bureau appreciates the hard work of the Office of the Inspector General and believes their recommendations will further strengthen the Office of Enforcement's robust information controls. The Bureau agrees with each of the recommendations, has already implemented some of these recommendations, and will take steps to implement the remainder.

Thank you again for your review. We provide the following comments for each of the specific recommendations.

Sincerely,

Christopher D'Angelo

Digitally signed by Christopher D'Angelo
Date: 2017.04.20 16:17:41 -04'00'

Christopher D'Angelo
Associate Director,
Division of Supervision,
Enforcement, and Fair Lending

Anthony Alexis
Assistant Director for Enforcement,
Division of Supervision,
Enforcement, and Fair Lending

consumerfinance.gov

1. The Office of Enforcement developed and is implementing a standard for access to confidential information consistent with the Bureau's regulations, which prohibit access to confidential information except where it is relevant to the performance of the employee's, contractor's or consultant's assigned duties.

2. During the audit by the OIG, Enforcement developed a procedure for approving and updating matter folder access rights to the Office's review tools and network drives. That procedure was communicated to all staff in a May 2016 email and is incorporated into the standard for access to confidential information referenced in our response to recommendation one. As noted in the report, the matter management system has been updated to accurately reflect the users assigned to matters and all matter folders now are restricted to those who need access to perform their assigned duties.

3. The Office of Enforcement expanded its existing mandatory training for all staff to educate them on these two topics as well as to reinforce the knowledge of the different types of confidential information handled by staff.

4. The Office of Enforcement recently implemented a monitoring and testing process to confirm matter folders are properly restricted.

5. Along with T&I, the Office of Enforcement's Special Counsel for eDiscovery has been tasked with selecting and implementing a new cloud environment for the Bureau and will ensure that access rights in that cloud environment are consistent with the recommendations of the OIG.

6. Working with T&I, the Office of Enforcement has implemented automatic cover sheet printing on all printers regularly accessed by Enforcement staff. Enforcement will develop a standard language for all cover sheets to reflect the sensitive nature of the printed information.

7. As part of its mandatory training, which is referenced in the Bureau's response to recommendation three, the Office of Enforcement now includes, training on information handling and safeguarding requirements. Further, for monitoring and compliance purposes, periodic reminders will be sent to all staff and random compliance checks will be performed.

8. The Office of Enforcement, as noted in the report, now has in place access-controlled storage available to all staff. Training on the need to properly use access-controlled storage and a method for reporting inoperable access-controlled storage is included in the mandatory training referenced in our response to recommendation three.

9. As noted in the report, the Office of Enforcement established a standard naming procedure and has implemented controls that prevent anyone outside of the Enforcement Front Office Staff from creating new matters within the internal drive.

The Office of Enforcement also established a standard operating procedure for the creation of new matters in the applications platforms, which now requires the use of the standard naming procedure. The process of creating a new matter is included in the mandatory training referenced in our response to recommendation three and includes a description of the required standard naming procedure for each matter.

consumerfinance.gov

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

HOTLINE

1-800-827-3340

OIGHotline@frb.gov

Report Fraud, Waste, and Abuse

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, e-mail, fax, or telephone.

Office of Inspector General, c/o Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW, Mail Stop K-300, Washington, DC 20551
Attention: OIG Hotline

Fax: 202-973-5044

Questions about what to report?

Visit the OIG website at www.federalreserve.gov/oig
or
www.consumerfinance.gov/oig