OFFICE OF INSPECTOR GENERAL

Evaluation Report 2017-SR-C-016

The CFPB Can Improve Its Examination Workpaper Documentation Practices

September 27, 2017

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

Report Contributors

Charlene Fadirepo and Laura Shakarji, Project Managers
Saurav Prasad and Michael Zeitler, Project Leads
Safal Bhattarai, Auditor
Sam Withers, 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
CSI	confidential supervisory information
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
EIC	Examiner-in-Charge
Examination Manual	*CFPB Supervision and Examination Manual* (version 2.0)
FM	Field Manager
MRA	Matter Requiring Attention
OIG	Office of Inspector General
OSE	Office of Supervision Examinations
PII	personally identifiable information
Privacy Policy	*Privacy Policy, Our Commitment to Privacy*
RAO	Regional Administrative Officer
SEFL	Division of Supervision, Enforcement, and Fair Lending

Executive Summary:

The CFPB Can Improve Its Examination Workpaper Documentation Practices

2017-SR-C-016 September 27, 2017

Purpose

The Office of Inspector General conducted this evaluation to assess the Consumer Financial Protection Bureau's (CFPB) guidance and practices, including training and quality reviews, to promote effective and consistent examination workpaper documentation. Specifically, we reviewed workpaper documentation in each of the CFPB's four regions for compliance with the *CFPB Supervision and Examination Manual* and other policies that govern examination work.

Background

The Dodd-Frank Wall Street Reform and Consumer Protection Act established the CFPB to regulate the offering and provision of consumer financial products and services under federal consumer financial laws. As such, the CFPB is responsible for implementing, examining for compliance with, and enforcing federal consumer financial laws.

The CFPB's Division of Supervision, Enforcement, and Fair Lending (SEFL) conducts the agency's supervision activities.

Findings

We identified opportunities for SEFL to improve its workpaper documentation practices. We conducted our fieldwork for this evaluation in two phases, with phase 1 including examinations completed from 2013 through 2014, and phase 2 including examinations completed in 2016. Our testing in phase 1 included assessing compliance with certain expectations outlined in the *CFPB Supervision and Examination Manual* and assessing access rights to examination workpapers and supporting documentation. In phase 2, we assessed access rights to examination workpapers for compliance with recent policy and guidance expectations for safeguarding information.

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

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

We acknowledge the actions that SEFL management has taken to address some of the issues discussed in this report. Specifically, we understand that SEFL recently began using a new system of record for examination materials, which is intended to address SEFL's storage capacity needs and better protect personally identifiable information. In addition, SEFL implemented a new process to periodically review and restrict access rights to the new system of record and to the shared drive folders once an examination has been completed. SEFL has also taken steps to develop training for employees on examination workpapers and quality control. We have not performed testing to determine whether these actions fully address our recommendations.

Recommendations

Our report contains recommendations designed to improve SEFL's approach to documenting examination results and protecting sensitive information. In its response to our draft report, the CFPB concurs with our recommendations. The agency describes actions and planned activities to improve SEFL's practices related to examination workpapers. We will follow up to ensure that the recommendations are fully addressed.

Summary of Recommendations, OIG Report 2017-SR-C-016

Finding 1: The Division of Supervision, Enforcement, and Fair Lending's Approach to Access Rights Limited Its Ability to Safeguard Sensitive Information

Number	Recommendation	Responsible office
1	Reassess the open-access-within-each-region approach for the system of record and the relevant shared drives and identify other measures to restrict access to confidential supervisory information and personally identifiable information to only those who need access to perform specific roles and responsibilities.	Division of Supervision, Enforcement, and Fair Lending
2	Work with the Office of Technology and Innovation to provide training to reinforce the guidance outlined in relevant information security policies and standards and establish a communication strategy to periodically reinforce these policies and standards as well as the self-reporting approach for reporting computer security incidents related to examination files that contain confidential supervisory information and personally identifiable information.	Division of Supervision, Enforcement, and Fair Lending
3	Work with the Office of Technology and Innovation to ensure that detective and preventative controls for preventing unauthorized disclosures of sensitive information stored in the system of record and on the relevant shared drives are in place and operating.	Division of Supervision, Enforcement, and Fair Lending
4	Develop an action plan to ensure the adequate safeguarding of the Division of Supervision, Enforcement, and Fair Lending's existing confidential supervisory information and personally identifiable information on the relevant shared drives and in the system of record. For any drives or systems using the open-access-within-each-region approach, this action plan, or a short-term alternate solution, should be developed as quickly as possible.	Division of Supervision, Enforcement, and Fair Lending
5	Develop a process to determine whether the sensitive information that the Division of Supervision, Enforcement, and Fair Lending collects is required for recordkeeping purposes, and ensure that this information is securely retained in the system of record or on the appropriate shared drive.	Division of Supervision, Enforcement, and Fair Lending
6	Develop an approach to periodically assess whether all regions are operating in a manner that is consistent with relevant Division of Supervision, Enforcement, and Fair Lending policies, guidance documents, and standards related to access rights.	Division of Supervision, Enforcement, and Fair Lending

Finding 2: Initial System of Record Limitations Hindered Effective Records Management

Number	Recommendation	Responsible office
7	Ensure that the Division of Supervision, Enforcement, and Fair Lending's system of record for examination results meets current and future storage needs.	Division of Supervision, Enforcement, and Fair Lending
8	Develop an approach to review the contents of the shared drives, identify any confidential supervisory information and personally identifiable information, and ensure that the Division of Supervision, Enforcement, and Fair Lending securely retains only the confidential supervisory information and personally identifiable information necessary for recordkeeping purposes.	Division of Supervision, Enforcement, and Fair Lending

Finding 3: Examination Workpapers Were Not Consistently Available in the Initial System of Record

Number	Recommendation	Responsible office
9	Update the *CFPB Supervision and Examination Manual* to include a requirement that all documentation necessary to support findings and conclusions be stored in the appropriate location in the system of record for each examination before the examination is closed.	Division of Supervision, Enforcement, and Fair Lending
10	Develop an action plan to ensure that all supporting documentation created through internal consultations with non–Office of Supervision Examinations employees is saved in the appropriate location in the system of record.	Division of Supervision, Enforcement, and Fair Lending

Finding 4: Documentation of Supervisory Review Did Not Fully Comply With *CFPB Supervision and Examination Manual* Standards, Including the Optional Workpaper Checklist

Number	Recommendation	Responsible office
11	Reinforce the requirement that Examiners-in-Charge and Field Managers review and sign off on all workpapers developed during the examination by using the *Workpaper Table of Contents and EIC Signoff* document or another method developed for this purpose.	Division of Supervision, Enforcement, and Fair Lending
12	Enhance the Workpaper Checklist or develop another method of documentation to include all key steps of the examination process, such as documenting supervisory reviews and approvals and uploading workpapers to the system of record, and to specify the Examiner-in-Charge and Field Manager roles and responsibilities related to completing the checklist.	Division of Supervision, Enforcement, and Fair Lending
13	Update the *CFPB Supervision and Examination Manual* or other Division of Supervision, Enforcement, and Fair Lending policies, or develop another method, to clarify the roles and responsibilities of Examiners-in-Charge and Field Managers related to completing the Workpaper Checklist and to require examiners, Examiners-in-Charge, and Field Managers to use the checklist.	Division of Supervision, Enforcement, and Fair Lending

Finding 5: Sampling Processes Were Not Consistently Documented in Workpapers

Number	Recommendation	Responsible office
14	Reinforce the guidelines for documenting sampling methods used in examination reports.	Division of Supervision, Enforcement, and Fair Lending
15	Ensure that the internal quality control review process developed in response to recommendation 17 includes steps for assessing the documentation of the sampling methods used during an examination.	Division of Supervision, Enforcement, and Fair Lending

Finding 6: The Division of Supervision, Enforcement, and Fair Lending Did Not Have Formal Training on Examination Workpaper Practices

Number	Recommendation	Responsible office
16	Develop and provide training on the CFPB's policies and standards for workpapers that conveys to examiners the agency's expected workpaper practices. Determine the appropriate frequency for that training.	Division of Supervision, Enforcement, and Fair Lending

Finding 7: The Division of Supervision, Enforcement, and Fair Lending Did Not Have an Ongoing Internal Quality Control Process to Assess Examination Workpapers		
Number	**Recommendation**	**Responsible office**
17	Establish an ongoing internal quality control review process to assess and improve examination workpaper practices. As part of this effort, the Division of Supervision, Enforcement, and Fair Lending should consider reviewing the observations, best practices, areas for improvement, and recommendations that resulted from the 2014 workpaper quality control assessment.	Division of Supervision, Enforcement, and Fair Lending

Office of Inspector General

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

September 27, 2017

MEMORANDUM

TO: Christopher D'Angelo
Associate Director, Division of Supervision, Enforcement, and Fair Lending
Consumer Financial Protection Bureau

FROM: Melissa Heist
Associate Inspector General for Audits and Evaluations

SUBJECT: OIG Report 2017-SR-C-016: *The CFPB Can Improve Its Examination Workpaper Documentation Practices*

We have completed our report on the subject evaluation. We conducted this evaluation to assess the Consumer Financial Protection Bureau's policies and practices to promote effective examination workpaper documentation by the Division of Supervision, Enforcement, and Fair Lending.

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

We appreciate the cooperation that we received from your staff during our evaluation. Please contact me if you would like to discuss this report or any related issues.

cc: David Bleicken, Deputy Associate Director, Division of Supervision, Enforcement, and Fair Lending
Paul Sanford, Assistant Director, Office of Supervision Examinations
Peggy Twohig, Assistant Director, Office of Supervision Policy
Patrice Ficklin, Assistant Director, Office of Fair Lending and Equal Opportunity
Jerry Horton, Chief Information Officer
Zachary Brown, Chief Information Security Officer, Office of Technology and Innovation
Claire Stapleton, Chief Privacy Officer, Office of Technology and Innovation
Tim Siwy, Deputy Assistant Director, Office of Supervision Examinations
Dana James, Acting Chief Financial Officer and Acting Assistant Director, Office of the Chief Financial Officer

Contents

Introduction

Objectives

We initiated this evaluation to assess the Consumer Financial Protection Bureau's (CFPB) guidance and practices to promote effective and consistent examination workpaper documentation by Division of Supervision, Enforcement, and Fair Lending (SEFL) employees. Our specific objectives for this evaluation were to assess SEFL's compliance with internal workpaper documentation standards and the effectiveness of policies and procedures, training programs, and other materials used to implement those standards.

To accomplish our objectives, we completed our testing in two phases. Our testing in phase 1 included assessing compliance with certain expectations outlined in the *Examination Manual* and assessing access rights to examination workpapers and supporting documentation. In phase 2, we assessed access rights to examination workpapers for compliance with recent policy and guidance expectations for safeguarding information. For additional information regarding our scope and methodology, see appendix A.

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 the federal consumer financial laws. Subject to the provisions of the Dodd-Frank Act, the CFPB is responsible for implementing, examining, and enforcing federal consumer financial laws. To carry out this mission, the Dodd-Frank Act granted the CFPB authority to supervise the following consumer financial market participants:

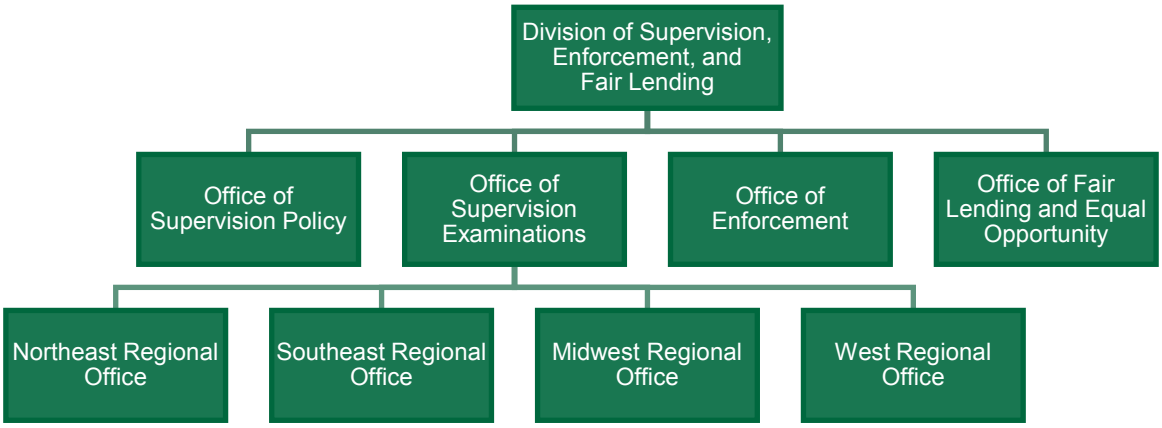
- insured depository institutions and insured credit unions with more than $10 billion in total assets, and their affiliates[1]
- certain nondepository institutions, including entities in the consumer mortgage, private-education lending, and payday lending markets; larger participants in markets for other consumer financial products or services as defined by the CFPB; and entities the CFPB has reasonable cause to determine, by order, are "engaging, or have engaged, in conduct that poses risks to consumers with regard to the offering or provision of consumer financial products or services"[2]

1. The institutions' prudential regulators retain primary consumer protection supervisory authority for depository institutions with total assets of $10 billion or less; however, the Dodd-Frank Act granted the CFPB authority to participate in examinations of these smaller depository institutions on a sampling basis.

2. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 1024(a)(1)(C), 124 Stat. 1376, 1987 (2010) (codified at 12 U.S.C. § 5514(a)(1)(C) (2010)).

SEFL conducts the agency's supervision activities. Within SEFL, the Office of Supervision Examinations (OSE) and the Office of Supervision Policy address depository and nondepository institution supervision. Figure 1 illustrates SEFL's overall organizational structure.

Figure 1: SEFL's Organizational Structure



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

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

OSE oversees the CFPB's examination activities and ensures that those activities remain consistent with the guidance outlined in policies and procedures. This office also manages the recruiting, training, and commissioning processes for CFPB examiners. The agency's four regional offices, located in New York (Northeast); Washington, DC (Southeast); Chicago (Midwest); and San Francisco (West), are components of OSE.

The CFPB's Examination Activities and Guidance Related to Examination Workpapers

During the course of an examination, CFPB examiners collect and review information from the supervised entity. Examiners may use this information to reach conclusions on the entity's practices, its compliance management program, and its compliance with specified federal consumer protection laws and regulations. Examiners analyze information obtained from the supervised entity as well as the work conducted by enforcement and fair lending employees, and they document this information and analysis in workpapers.

The *Examination Manual* is the agency's primary source of guidance related to examination workpapers.[3] The *Examination Manual*

- describes the agency's guidance for conducting its examination activities
- provides guidance on how to assess whether supervised institutions comply with federal consumer financial laws
- provides guidance on roles and responsibilities for examiners, Examiners-in-Charge (EICs), and Field Managers (FMs)

According to the *Examination Manual*, workpapers serve three purposes for CFPB examiners:

- to provide a record of the work performed during the examination that supports findings or recommendations made during the examination
- to maintain the evidence necessary to support supervisory agreements or formal enforcement actions
- to facilitate internal quality control reviews

> "During an examination, examiners collect and review information from the supervised entity to reach conclusions about its practices, its compliance management, and its compliance with specific laws and regulations. The records documenting the review are called workpapers. Workpapers should contain sufficient information and supporting documents to explain—to a knowledgeable reviewer—the basis for the examination conclusions."
>
> *—Examination Manual*

The *Examination Manual* also provides examiners with examples of specific types of documents to include in the workpapers, as well as guidance on the types of information workpapers should include for documentation or support. The manual provides guidance on the approval process that the examination team is expected to follow after workpapers have been drafted, which includes a review by the EIC and a sign-off by the FM. The manual also indicates that examination workpapers receive scrutiny through an internal quality control process. The quality control process requires that workpapers contain sufficient information so that an independent quality control reviewer can understand how examiners reached their final conclusions.

The CFPB's Workpaper System of Record and Shared Drives

Until June 2017, SEFL used an Office of Thrift Supervision system as its system of record. SEFL employees used this initial system of record to document their examination results and retain supporting materials during all phases of the examination, from the planning process through completion. The *Examination Manual* requires that examiners post all examination workpapers in electronic form to the system of record.

We understand that the CFPB recently implemented a new system of record to store examination results and supporting materials that completely replaces the initial system of record. Agency officials indicated that SEFL migrated all files and data from the initial system of record to the

3. The CFPB issued the *Examination Manual* in October 2011 and updated it in October 2012. Since then, the CFPB has issued various supplements and revisions to certain portions of the manual.

new system of record, and that only a limited number of SEFL and Office of Technology and Innovation employees continue to have access to the initial system of record. SEFL and Office of Technology and Innovation employees began decommissioning the initial system of record in late July 2017.

SEFL examiners use shared drives, which include restricted network subfolders available to SEFL employees, as general-purpose document repositories to store documents during an examination. Examiners initially upload all documents provided by the supervised institution to these shared drives, and when the examination has been completed, they preserve the examination record by transferring to the system of record the workpapers and materials necessary to support the examination findings and conclusions.

Confidential Supervisory Information and Personally Identifiable Information in Examination Workpapers

Workpapers can include confidential supervisory information (CSI) and personally identifiable information (PII). According to its *Handbook for Sensitive Information*, the CFPB defines CSI broadly and references title 12, section 1070.2, of the *Code of Federal Regulations* for its full definition. Section 1070.2 defines multiple types of confidential information, including confidential consumer complaint information, confidential investigative information, and CSI, all of which the CFPB routinely handles. Among these types of information, our evaluation focused on the handling and use of CSI.[4] According to section 1070.2(i), CSI is defined as including reports of examination, inspection, and visitation; nonpublic operating, condition, and compliance reports; and any information contained in, derived from, or related to such reports.[5] This broad definition covers examination workpapers.

We also assessed SEFL's handling and use of PII obtained during its examination activities through requests made to supervised institutions.[6] The CFPB's *Privacy Policy, Our Commitment to Privacy* (*Privacy Policy*) cites the Office of Management and Budget's definition of PII, which states that "PII includes any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual," such as the individual's Social Security number or biometric records.

4. Our evaluation focused on CSI and PII, not confidential consumer complaint information or confidential investigative information.

5. 12 C.F.R. 1070.2(i)(1)(ii) covers materials obtained from other federal and state regulators. Our samples did not include any such information.

6. In its September 2014 report titled *CFPB: Some Privacy and Security Procedures for Data Collections Should Continue Being Enhanced*, the U.S. Government Accountability Office reviewed the CFPB's collection of consumer financial data. The report contains a general assessment of large-scale consumer financial data collections that the CFPB obtained under its supervisory or market monitoring authorities.

Finding 1: SEFL's Approach to Access Rights Limited Its Ability to Safeguard Sensitive Information

We conducted our fieldwork for this evaluation in two phases, in part because the CFPB implemented a new policy and guidance document related to access rights for examination materials during our evaluation. We reviewed a sample of completed examinations from 2013 and 2014 (phase 1) and a sample of examinations completed in 2016 that were initiated following the implementation of the new policy, *SEFL Policy on Supervisory & Examination System (SES) Access*, and an internal guidance document describing shared drive B (phase 2). Our testing in phase 1 included assessing compliance with certain expectations outlined in the *Examination Manual* and assessing access rights to examination workpapers and supporting documentation. In phase 2, we assessed access rights to examination workpapers for compliance with recent policy and guidance expectations for safeguarding information.

Phase 1 Testing Overview

In phase 1, we found that access rights for the initial system of record were centrally managed and were granted to examination teams in all four regions in a manner that was consistent with the guidance in the *Examination Manual*. Subject to certain conditions being met, we determined that examination staff in the four regions could receive open access to all examination workpapers for that region within the initial system of record. The regions separately managed shared drive A's access rights, and those responsible for granting shared drive access rights in the four regions had varying approaches, some of which did not align with the CFPB's information security guidance. We noted that one region used an open-access approach for shared drive A. We believe this approach of open access within each region created an opportunity for insider abuse of CSI or PII in examination materials or supporting materials stored in systems or on drives that had open access.

The CFPB's rules prohibit disclosure of confidential information to any CFPB employee when that disclosure is not relevant to the performance of that employee's assigned duties. The CFPB has issued several guidance and policy documents that address privacy and information security. For example, in December 2012 the CFPB issued the *Handbook for Sensitive Information at the CFPB*, which establishes the agency's expectation that employees maintain a high level of confidentiality and protection with respect to the sensitive information encountered in their work. The handbook defines *sensitive information* to include PII and CSI and notes that employees should "follow the 'need to know' rule when sharing sensitive information with CFPB colleagues" and should "store sensitive information electronically using restricted access folders."[7] In addition, the CFPB's *Privacy Policy*, also issued in December 2012, states that one of the CFPB's principles includes the agency only allowing "access to PII to authorized individuals with a legitimate need for access [to that PII]."

7. For the purposes of our report, *restricted access folders* are folders in shared drive B that are specifically intended for PII and CSI. According to the shared drive B guidance document we reviewed in our phase 2 testing, access to these folders should be limited to certain individuals after an examination has been completed. The guidance does not describe any requirements to restrict the folders during an examination.

Phase 2 Testing Overview

In late 2015, SEFL implemented a new policy to enhance the access and permissions processes for the initial system of record. SEFL also issued a guidance document that included an overview of shared drive B, its folder structure, and corresponding access rights information. Although shared drive B is centrally managed at headquarters, access rights on this drive also follow the open-access-within-each-region approach. From our phase 2 testing, we concluded that practices described in shared drive B's guidance document had not been consistently followed. Specifically, we noted the need to reinforce the new requirements, because access to PII had not been limited in accordance with expectations.

Phase 1 Testing Results

The Open-Access Approach to Shared Drive A and the Initial System of Record Created an Opportunity for Insider Abuse

Access to shared drive A was managed regionally. We found that one region had opted to provide examination employees in that region with access to all examination workpapers and supporting materials in shared drive A. This practice of open access was not consistently used across each of the four regions; at least two regions appeared to assign shared drive A access rights based on the employee's role.

An examination support staff member responsible for granting access in the open-access region stated that an alternative approach would not work because it potentially would require changing shared drive A access rights as employees move among examination teams. Further, during our interviews, employees and managers cited the training benefits of providing examination employees access to all the workpapers in a given region on shared drive A. These employees stated that open access reinforces the testing and documentation approaches used in prior examinations. Multiple interviewees stated that access to all the workpapers in a given region on shared drive A served as a guide that allowed examiners to review previously completed work. We believe that this region's open-access approach (1) contradicted the requirements outlined in the *Handbook for Sensitive Information at the CFPB* and (2) created the opportunity for insider abuse of CSI and PII, particularly for examination staff members who did not have assigned duties related to relevant examinations.

Examination staff in each of the four regions could also receive open access to all examination materials for that region in the initial system of record. The system business owner is a SEFL employee at headquarters who centrally managed access rights to the initial system of record. After receiving a list of SEFL employees who had completed the required CSI training, the system business owner granted those individuals general access to the initial system of record. Additional permissions, also managed by the system business owner, that provide access to workpapers containing CSI and PII were based on the employee's actual job role and "business need." Thus, at the system business owner's discretion, employees could be granted access to view all the workpapers for all examinations conducted in their region. In addition, with manager approval, examiners could be granted access to workpapers for an examination in another region by submitting a request to the system business owner. Although we did not learn of any instances

of insider abuse, this open-access-within-each-region approach to the initial system of record also created an opportunity for insider abuse.[8]

Process for Maintaining Access to the Initial System of Record Contributed to Challenges in Limiting Access to Information on a Need-to-Know Basis

The system business owner faced challenges keeping access rights to the initial system of record current. Although the system business owner periodically reviewed and updated permissions, there was a period of time during our review when he or she did not receive notices of employees transferring between regions. The *SEFL Policy on Supervisory & Examination System (SES) Access* was updated in October 2015 to include a section on regional staffing changes. This section requires that the regional analyst inform the system business owner of any personnel changes, including transfer of employees, that may require adjustments to the initial system of record access and permissions. This section of the policy was not in effect during phase 1 of our testing. In addition to the guidance outlined in the *Handbook for Sensitive Information at the CFPB*, the CFPB's *Access Control Process (CS-P-03)* states that account access modifications may be required if an individual transfers departments, takes on additional duties, or relinquishes certain duties. Access rights do not expire; thus, when access rights are not kept current, the number of employees who can access CSI and PII when they no longer need that access increases.

SEFL's Shared Drive A Contained a High Volume of CSI and PII

Shared drive A contained a large amount of CSI and PII. To determine the extent to which SEFL stored PII on the shared drive, we nonrandomly selected three examinations and analyzed the files stored in those examinations' shared drive A folders. We found the following:

- One examination had 54 files containing names, addresses, dates of birth, and Social Security numbers for 25 individuals.
- Another examination included 56 audio files of collection calls for payday loans that included customers' names and addresses as well as 35 credit applications with accompanying adverse action letters that included names, addresses, dates of birth, phone numbers, Social Security numbers, identification card numbers, employer information, and bank account information.
- The third examination did not have any PII identified.

The 54 files that contained PII for 25 individuals were in the region that provided examination employees open access to all of the region's examination workpapers and supporting materials in the shared drive. Further, we also found that multiple audio files for the collection calls had been stored in the initial system of record. We believe that open access to workpapers in the shared drive and the initial system of record for all examination employees within a region heightens the risk of insider abuse.

8. Our scope did not include a review designed to identify insider abuse.

A senior SEFL official acknowledged that workpaper access should be on a need-to-know basis, given the extent of PII saved on shared drive A. Our testing results demonstrate the need for SEFL to follow the requirements in the *Handbook for Sensitive Information at the CFPB* and consistently limit access to sensitive materials to those with a need to know across all relevant drives and systems that contain examination workpapers.

Lack of Information Disposal Guidelines for Shared Drive A Limited SEFL's Ability to Protect Sensitive Information

Examination teams were not routinely purging unneeded files that contained sensitive information following the transfer of information from shared drive A to the initial system of record, as required by the *Handbook for Sensitive Information at the CFPB*. Examination files containing CSI and PII remained on shared drive A after the issuance of examination reports. We noted that SEFL had not developed division-specific guidelines for purging CSI and PII, including a process to determine whether the sensitive information SEFL collects is required for recordkeeping purposes. We believe that such guidelines would help reduce the risk of insider abuse of sensitive information and would help staff to follow the principle outlined in the CFPB's *Privacy Policy*, to "keep PII only as long as needed to fulfill its stated purpose."

Lack of Clear Access Rights Limited the Effectiveness of Self-Reporting of Potential Information Security Incidents

The Office of Technology and Innovation's *Cybersecurity Incident Response Plan, Version 2.0*, notes that the CFPB uses several approaches to detect and report computer security incidents.[9] For detecting and reporting privacy-related incidents within SEFL, the Privacy Office relies on the self-reporting of incidents to the division's designated Privacy Office point of contact. A Privacy Office official stated that SEFL ensures that employees "police themselves" with regard to unauthorized information access, and the Privacy Office also issues publicly available privacy impact assessments, including an assessment that describes the types of information collected by SEFL. Complete and consistent self-reporting is challenging, however, without a consistent approach for limiting access rights based on readily understandable criteria.[10]

9. Computer security incident response team analysts are responsible for tracking and analyzing all CFPB incidents. For example, the CFPB's computer security incident response team monitors the agency's network traffic and reviews audit logs for signs of incidents. Further, end users can report suspicious behavior directly to the CFPB's help desk.

10. We are aware that a peer financial regulator has implemented a data loss prevention monitoring system that aids in detecting potential data loss events. In our report titled *2016 Audit of the CFPB's Information Security Program* (OIG Report 2016-IT-C-012, November 11, 2016), we noted that the CFPB can strengthen its risk management program by formalizing its insider threat activities and evaluating options to develop an agencywide insider threat program that leverages planned activities around data loss prevention.

SEFL Employees Lacked Awareness of Existing Information Governance Standards

In September 2014, the CFPB's Chief Information Officer issued the Information Sensitivity Leveling Standard, one of the purposes of which is to expand on the guidance outlined in the *Handbook for Sensitive Information at the CFPB*. The standard defines the types of information that should be classified as *public*, *low sensitivity*, *medium sensitivity*, and *high sensitivity*, as well as the handling and use guidance for the information classified in those four sensitivity levels. According to the standard, raw data acquired through the examination process and PII with direct identifiers are considered *high sensitivity*.[11] The standard further notes that (1) users of *high sensitivity* information must have a demonstrated business need for access and (2) *high sensitivity* information should be stored in a central, access-controlled location. Among the employees we interviewed, we noted a need to reinforce the requirements outlined in this information governance standard. For example, we found that EICs and FMs did not have a clear understanding of shared drive A access rights associated with their job responsibilities.

Also in September 2014, the CFPB issued the Permissible Use Standard. This standard describes rules for the internal use of information, specifically across divisions and offices. For *medium sensitivity* and *high sensitivity* information, permissible uses are limited to the role-based need or demonstrated business need identified at the time of the access request. In addition, the standard mentions that SEFL may develop and maintain its own procedures for determining permissible uses of *medium sensitivity* and *high sensitivity* supervisory, enforcement, or fair lending information for individuals who have a role-based need or a demonstrated business need for such information.

Although they work in SEFL, Regional Administrative Officers (RAOs) were uncertain about SEFL's information governance standards related to access rights. We believe that training to reinforce existing guidance would increase SEFL employees' awareness of these standards and help mitigate the risk of insider abuse of sensitive information.

Phase 2 Testing Results

In September and October 2015, respectively, SEFL management implemented two initiatives to enhance SEFL's access controls for key supervisory systems: (1) the *SEFL Policy on Supervisory & Examination System (SES) Access* and (2) an internal guidance document describing shared drive B. We performed our phase 2 testing of specific examinations completed in 2016 to determine the effectiveness of these initiatives.

SEFL implemented the *SEFL Policy on Supervisory & Examination System (SES) Access* to "streamline the access and the permissions process, provide greater security, and increase accountability of [system of record] users." The policy indicates that the initial system of record's business owner will "assign employees a select set of permissions based on the tasks and responsibilities of their business role."

11. Agency officials stated that this raw data would be considered to be of *moderate sensitivity* under other federal information governance standards, such as the Federal Information Security Modernization Act of 2014.

The guidance document describing shared drive B states that the shared drive will serve as a restricted network drive for SEFL's sensitive information. Shared drive B's access is centrally managed at headquarters, and the drive functions as a document repository for information provided by the supervised institution and for work-in-progress examination team materials. The agency created this shared drive to improve its data governance capability by isolating and restricting access to sensitive information. The guidance describes a standardized folder structure approach on the shared drive, including a subfolder for PII, to improve the management of sensitive information. In addition, the guidance requires the EIC, upon completion of an examination, to request that associated folders with sensitive information in shared drive B be restricted to the EIC, the FM, the applicable regional analysts, and the headquarters points of contact.

PII Stored in Multiple Folders on Shared Drive B Reflects the Need to Reinforce Expectations

Our phase 2 testing revealed that shared drive B contained large amounts of PII that had not been stored in the designated folders in accordance with the expectations outlined in the shared drive B guidance document. Six of the eight examinations we reviewed had PII stored on shared drive B, and we identified numerous files with PII, such as individuals' Social Security numbers, dates of birth, and contact information, that were not stored in the appropriate PII subfolder in accordance with expectations. As a result, examiners in the region could view the sensitive files in this folder even if they did not have a business need to access that information.

Further, we found that the process to ensure that the PII subfolder is restricted after an examination has been completed was not understood by all interviewees. The guidance requires the EIC to request that the PII subfolder be restricted to the EIC, the FM, the regional analysts, and the headquarters points of contact following the completion of an examination. Consistent with the guidance, a SEFL employee confirmed that the shared drive is to be "locked down" to more restricted access permissions after an examination has been completed. However, several interviewees stated that they were unsure about the process to restrict access to the folders for shared drive B, including the subfolder for PII, after an examination is completed. This lack of understanding may lead to folders not being properly restricted, thereby increasing the risk of unauthorized disclosure or use of that information.

Examination Support Staff Were Uncertain About Managing Shared Drive B Access Rights

Through our correspondence with RAOs, we identified uncertainty about the roles and responsibilities for managing the access rights to shared drive B. Multiple RAOs cited that the appropriate point of contact is at headquarters; however, the initial system of record's business owner at headquarters stated that the regions control access rights to shared drive B. This apparent confusion may hinder the CFPB's ability to secure sensitive examination information.

The Open-Access-Within-Each-Region Approach to Shared Drive B Heightened the Risk of Insider Abuse

As part of our phase 2 testing, we obtained the shared drive B access lists for the eight examinations under review and confirmed that SEFL has implemented its open-access-within-each-region approach for shared drive B. We found that all examination employees within each region had access to all examination documents in that region's shared drive B folders. For example, FMs stated that they assign six to nine OSE employees to a typical examination, but we found that in each of the four CFPB regions, all examiners in each region had access to the shared drive B folders for their region's examinations. Further, during our interviews with CFPB officials, we learned that employees from the Office of Fair Lending and Equal Opportunity and the Office of Enforcement work closely on examinations and therefore have access to shared drive B's examination files to complete their procedures.

The shared drive B guidance states that initial access to examination folders is provided to employees in the region of the examination, suggesting that all employees in a particular region have a need to access the workpapers for examinations in that region. The CFPB's *Privacy Policy* states that one of the CFPB's principles includes the agency only granting "access to PII to authorized individuals with a legitimate need for access [to that PII]." Granting open access to all shared drive B folders to all examination employees in a region increases the risk of insider abuse of the PII contained in those folders. We believe that access should be granted to employees based on relevance to their assigned job duties.

Management Actions Taken

In 2015, a CFPB project team began planning to develop a replacement system for the initial system of record. In June 2015, the project team completed the first planning phase by obtaining approval from the CFPB's Office of Technology and Innovation to continue the system replacement process. By October 2015, the agency completed the second planning phase, which signaled that the project team could proceed with the system of record replacement. In May 2017, the project team received final clearance to deploy the new system of record. As previously noted, agency officials indicated that SEFL has migrated all files and data from the initial system of record to the new system of record, and only a limited number of SEFL and Office of Technology and Innovation employees have access to the initial system of record. In late July 2017, SEFL and Office of Technology and Innovation employees began to decommission the initial system of record.

In June 2017, the CFPB transitioned to the new system of record and developed a communications and training plan to teach employees about the new system. CFPB officials indicated that the new system provides a checkbox for each workpaper to convey whether the file contains sensitive information, such as PII. When the box is checked, that file should be further restricted after an examination has been completed, and the file will no longer be visible to all examiners in that region.[12]

12. For business purposes, the CFPB will allow those files to remain accessible to regional analysts, FMs, and those in positions above FMs in the region, and to analysts at CFPB headquarters.

In addition, the CFPB has implemented a process to further restrict shared drive B access once an examination has been completed. The CFPB began identifying examinations that have been completed and inactive for over 180 days in April 2017. We understand that more-restricted access will be applied to those examinations' shared drive folders by limiting the number of individuals who have access to these folders.

We understand that for the new system of record, a central point of contact updates access rights on a monthly basis, ensuring that employees who no longer need access to a specific examination have their access revoked.

Summary

Although SEFL management implemented two initiatives to enhance its access controls, we believe that SEFL can continue to improve the effectiveness of those initiatives by (1) reassessing the need for open access to workpapers and supporting materials within each region in the system of record and on shared drives, (2) reinforcing expectations and roles and responsibilities for managing and maintaining access rights, and (3) ensuring that the agency only retains the CSI and PII necessary for recordkeeping purposes.

Recommendations

We recommend that the Associate Director of SEFL

1. Reassess the open-access-within-each-region approach for the system of record and the relevant shared drives and identify other measures to restrict access to CSI and PII to only those who need access to perform specific roles and responsibilities.

2. Work with the Office of Technology and Innovation to provide training to reinforce the guidance outlined in relevant information security policies and standards and establish a communication strategy to periodically reinforce these policies and standards as well as the self-reporting approach for reporting computer security incidents related to examination files that contain CSI and PII.

3. Work with the Office of Technology and Innovation to ensure that detective and preventative controls for preventing unauthorized disclosures of sensitive information stored in the system of record and on the relevant shared drives are in place and operating.

4. Develop an action plan to ensure the adequate safeguarding of SEFL's existing CSI and PII on the relevant shared drives and in the system of record. For any drives or systems using the open-access-within-each-region approach, this action plan, or a short-term alternate solution, should be developed as quickly as possible.

5. Develop a process to determine whether the sensitive information that SEFL collects is required for recordkeeping purposes, and ensure that this information is securely retained in the system of record or on the appropriate shared drive.

6. Develop an approach to periodically assess whether all regions are operating in a manner that is consistent with relevant SEFL policies, guidance documents, and standards related to access rights.

Management's Response

In the response to our draft report, the CFPB concurs with each of the recommendations associated with this finding. For recommendations 1, 2, and 4, the agency notes that OSE will reassess its open-access-within-each-region approach for access to examination data, identify measures to limit access to sensitive information, and ensure compliance with CFPB-wide data governance. The response also highlights that SEFL is working with the Chief Privacy Officer to develop practices and guidance related to security and information handling. The CFPB notes that in addition to the annual training for information handling, (1) OSE staff are required to take additional annual training specifically for handling CSI material and (2) a SEFL/Office of Technology and Innovation working group recently distributed training materials to all employees attending an agencywide conference and will be distributing materials at all upcoming regional conferences.

For recommendation 3, the CFPB notes that OSE and the Office of Technology and Innovation are developing automated reports to monitor access to examination files. The agency's response indicates that the new enterprise platform containing the system of record was selected in part because of its extensive event and audit logging capabilities, which support continuous monitoring and forensic analysis.

For recommendation 5, the CFPB notes that SEFL will review its records management schedule in coordination with the Records Management Office and reassess which materials need to be stored for recordkeeping purposes. For recommendation 6, OSE will periodically assess whether all regions are operating in a manner that is consistent with the relevant SEFL policies.

OIG Comment

The actions described by the CFPB appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 2: Initial System of Record Limitations Hindered Effective Records Management

We found that the initial system of record did not provide adequate storage capabilities for examination files that supported findings and conclusions because of its restrictive file size limitations. The *Examination Manual* states that workpapers should be uploaded to the system of record along with the final examination report. To comply with this expectation, SEFL employees had to break down large files into smaller component files to upload them to the initial system of record. In some cases, SEFL employees saved large files on the relevant shared drives rather than in the initial system of record. The agency's system of record should have appropriate storage capacity to ensure that a complete record of examinations can be housed in the system of record.

File Size Limitations Led to Reliance on Shared Drives

File size limitations prevented examination teams from uploading to the initial system of record all supporting documentation stored on the relevant shared drives upon completion of the examination. These limitations caused examination teams to use shared drives A and B as alternative repositories for workpapers. The *Examination Manual* states that workpapers should be uploaded to the system of record along with the completed examination to be preserved as part of the examination record and made available for future reference.

The initial system of record had a 15 megabyte file size limitation for individual files and a 40 megabyte file size limitation for zipped files. EICs told us that when an examination team received a file that was too large to store in the initial system of record, the team either broke the large file into multiple smaller files or stored the complete file on the relevant shared drives. When files were stored on the relevant shared drives rather than the initial system of record, the initial system of record held incomplete examination records that did not reflect the record of the work performed or adequately support examination findings and recommendations.

Management Actions Taken

CFPB officials stated that the new system of record, implemented in June 2017, provides examination teams with the ability to store considerably larger files. The file size limit increased from 15 megabytes per file to approximately 2 gigabytes per file. An analysis conducted by the CFPB indicates that the new system of record will be able to accommodate 99 percent of the files received during the examination process. As of July 2017, the CFPB had not determined how it would identify and handle any files that contain CSI or PII that were stored on the shared drives because they were too large to store in the initial system of record.

Recommendations

We recommend that the Associate Director of SEFL

7. Ensure that SEFL's system of record for examination results meets current and future storage needs.

8. Develop an approach to review the contents of the shared drives, identify any CSI and PII, and ensure that SEFL securely retains only the CSI and PII necessary for recordkeeping purposes.

Management's Response

In the response to our draft report, the CFPB concurs with recommendations 7 and 8. The agency notes that OSE is working with the Office of Technology and Innovation to plan for current and future storage needs for all examination-related data. The response indicates that the new system of record is built on an enterprise platform that the Office of Technology and Innovation actively manages to support CFPB-wide business requirements, such as file storage needs. For recommendation 8, SEFL will develop an action plan to review the contents of the shared drives and identify any CSI and PII and will ensure that SEFL securely retains only the CSI and PII necessary for recordkeeping purposes.

OIG Comment

The actions described by the CFPB appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 3: Examination Workpapers Were Not Consistently Available in the Initial System of Record

We found that for some of the examination reports we reviewed that contained Matters Requiring Attention (MRAs),[13] certain examination workpapers were difficult to locate because examiners did not consistently store the workpapers in the initial system of record location specified in the *Examination Manual*. Further, support for some examination conclusions provided through consultations with non-OSE offices in SEFL had not been saved in the initial system of record. The *Examination Manual* states that workpapers (1) provide a record of the work performed during the examination that supports findings or recommendations made during the examination, (2) maintain the evidence necessary to support supervisory agreements or formal enforcement actions, and (3) facilitate internal quality control reviews. In addition, the manual states that workpapers should be uploaded to the system of record along with the complete examination so that they are preserved as part of the examination record and are available for future reference. If left unaddressed, these inconsistencies could result in the appearance that the examination results are not adequately supported.

Examiners Did Not Consistently Store Workpapers in the Appropriate Location in the Initial System of Record

We encountered difficulties locating supporting workpapers for some MRAs because examiners did not consistently store the workpapers in the appropriate location in the initial system of record. Two of the examinations in our sample had supporting workpapers for the MRAs that were not stored in their respective initial system of record folder; for one of the examinations, supporting documents for an MRA were on an examiner's CFPB hard drive, and for the other, the examination team incorrectly saved a workpaper in the initial system of record in an examination file for a different examination.

Support for Examination Work Performed in Coordination With Other CFPB Offices Was Stored Outside the Initial System of Record

Consulting internally, which is defined in the *Examination Manual* as coordination with other CFPB offices, appeared to create challenges related to compiling a complete record of examination results. For example, during our review of one examination that contained an MRA, we found that the EIC did not upload to the initial system of record the supporting documentation from another internal office. As a result, we had to assemble information from multiple locations and conduct additional follow-up interviews with SEFL officials to compile a complete record of the examination results.

13. According to the CFPB Supervisory Report Template, "Matters Requiring Attention (MRAs) describe corrective actions for the supervised entity to take to address violations or weaknesses discussed in the report." Examination conclusions sometimes include MRAs, and because our goal was to test whether examination conclusions were supported by workpapers, we focused on MRAs.

Recommendations

We recommend that the Associate Director of SEFL

9. Update the *Examination Manual* to include a requirement that all documentation necessary to support findings and conclusions be stored in the appropriate location in the system of record for each examination before the examination is closed.

10. Develop an action plan to ensure that all supporting documentation created through internal consultations with non-OSE employees is saved in the appropriate location in the system of record.

Management's Response

In the response to our draft report, the CFPB concurs with recommendations 9 and 10. The agency's response notes that OSE will update the *Examination Manual* to include a requirement that all documentation necessary to support findings and conclusions be stored in the appropriate location in the system of record. SEFL will also develop an action plan to ensure that all supporting documentation created through internal consultations with non-OSE employees is saved in the appropriate location in the system of record.

OIG Comment

The actions described by the CFPB appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 4: Documentation of Supervisory Review Did Not Fully Comply With *Examination Manual* Standards, Including the Optional Workpaper Checklist

We found that for each of the eight examinations we reviewed in our phase 1 testing, the records in the initial system of record did not include a required sign-off document evidencing supervisory review by the EIC and the FM. The *Examination Manual* requires supervisory review and documentation of all workpapers. Specifically, the manual states that EICs must use a specific document called the *Workpaper Table of Contents and EIC Signoff* to record their supervisory review of all workpapers. The FM must review and sign off on this document after the EIC reviews and signs off. In addition, the *Examination Manual* states that the optional Workpaper Checklist can help ensure that workpapers are sufficient. The EICs and FMs we interviewed used inconsistent approaches to document their supervisory review and demonstrated limited awareness of the *Workpaper Table of Contents and EIC Signoff* document requirements. Further, none of the employees we interviewed used the optional Workpaper Checklist. If the EICs and FMs do not complete the *Workpaper Table of Contents and EIC Signoff* document, SEFL cannot be assured that all workpapers that support findings and conclusions have been reviewed and approved, which may affect the credibility of examination results.

EICs and FMs Inconsistently Executed Their Supervisory Review of Workpapers

During our interviews with a sample of EICs and FMs, we learned that the interviewees did not have a consistent understanding of the documentation requirements for performing supervisory review of workpapers. Further, our interviews and documentation reviews revealed inconsistent execution of required supervisory reviews and approvals of workpapers. For example, we noted that some EICs and FMs used the comment and track changes functions in Microsoft Word to document their review of workpapers, and other EICs and FMs stated that they added their initials in the header of the workpaper as evidence of supervisory review and sign-off. We also found workpapers that identified the preparer of the document but not the reviewer, and workpapers that listed neither the preparer nor the reviewer. One interviewee was not aware of the *Workpaper Table of Contents and EIC Signoff* document. We believe that a lack of consistent documentation of supervisory review raises the risk that examination activities, findings, and conclusions may not be properly documented.

Optional Workpaper Checklist Was Not Used

We found that examination teams did not use the optional Workpaper Checklist for any of the eight examinations in our sample. The Workpaper Checklist is designed to ensure, among other things, the documentation of key examination steps, such as scope, sampling process, findings and violations, and recommendations. Further, in our interviews with the EICs and the FMs, we learned that they did not use any type of checklist during their reviews of workpapers. We believe that by using the optional Workpaper Checklist, examination teams, the EICs, and the FMs will be more likely to detect instances in which examiners may have omitted key steps of the examination process.

We also noted that the checklist could be improved. The checklist does not include the documenting of supervisory review and approval or the uploading of workpapers to the system of record as steps to be taken and verified. The checklist also does not include clear instructions for its proper use, including the roles and responsibilities of the EICs and the FMs related to completing the checklist. In addition, the *Examination Manual* does not explain the roles and responsibilities of the EICs and the FMs regarding the use of the checklist.

Recommendations

We recommend that the Associate Director of SEFL

11. Reinforce the requirement that EICs and FMs review and sign off on all workpapers developed during the examination by using the *Workpaper Table of Contents and EIC Signoff* document or another method developed for this purpose.

12. Enhance the Workpaper Checklist or develop another method of documentation to include all key steps of the examination process, such as documenting supervisory reviews and approvals and uploading workpapers to the system of record, and to specify the EIC and FM roles and responsibilities related to completing the checklist.

13. Update the *Examination Manual* or other SEFL policies, or develop another method, to clarify the roles and responsibilities of EICs and FMs related to completing the Workpaper Checklist and to require examiners, EICs, and FMs to use the checklist.

Management's Response

In the response to our draft report, the CFPB concurs with recommendations 11, 12, and 13. The agency notes that OSE will reinforce the requirement that EICs and FMs review and sign off on all workpapers developed during the examination by using a *Workpaper Table of Contents and EIC Signoff* document or another method developed for this purpose. Further, the response indicates that OSE will document all key steps of the examination process by enhancing the existing Workpaper Checklist or by using another method to capture that information. OSE also intends to clarify the roles, responsibilities, and requirements of EICs and FMs related to completing the Workpaper Checklist or other records with a similar function.

OIG Comment

The actions described by the CFPB appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 5: Sampling Processes Were Not Consistently Documented in Workpapers

Several of the examinations we reviewed contain documentation that referred to the examination team's use of sampling, but the associated workpapers did not include support for the sampling methods used or a complete record of the work performed. The *Examination Manual* states that generally, workpapers should document or support the sampling process used. The optional Workpaper Checklist that examination teams can use to help confirm their completion of key examination steps contains a section on the sampling process; however, none of the interviewees with whom we spoke about the checklist used it. The checklist section on the sampling process reminds examiners to document data sets selected for review, explain why those items were selected, and confirm whether they have documented the logic for the sample selection. If examiners do not document the sampling approaches taken during their examinations, the resulting examination workpapers will not be a complete record of the work performed or detail how the team arrived at its conclusions.

Sampling Methods Were Not Consistently Documented

Seven of the eight examinations we reviewed in phase 1 used sampling techniques, and four of those seven examinations did not sufficiently document or support the sampling process used by the relevant examination teams. Examples of important omissions from the workpapers for those examinations include the following:

- the population sampled
- the type of sample—random, judgmental, or statistical
- the sampling method used
- the rationale for the sampling method selected

For example, with regard to one of the four examinations for which the sampling process was not sufficiently documented, an FM stated that another internal office determined the sampling method. This instance is another example of how consulting internally appeared to create coordination challenges related to compiling a complete record of the examination results.

Recommendations

We recommend that the Associate Director of SEFL

14. Reinforce the guidelines for documenting sampling methods used in examination reports.

15. Ensure that the internal quality control review process developed in response to recommendation 17 includes steps for assessing the documentation of the sampling methods used during an examination.

Management's Response

In the response to our draft report, the CFPB concurs with recommendations 14 and 15. The agency notes that OSE will reinforce the guidelines for documenting sampling methods used in examination reports. OSE will also ensure that the internal quality control review process developed in response to recommendation 17 includes steps for assessing the documentation of the sampling methods used during an examination.

OIG Comment

The actions described by the CFPB appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 6: SEFL Did Not Have Formal Training on Examination Workpaper Practices

We found that SEFL employees did not have a consistent understanding of the definition of a workpaper and the preferred practices for documenting completed examination procedures, interviews, and detailed testing results. We attribute this inconsistent understanding to a lack of formal training on workpaper documentation. The U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government* notes that operational success for an organization is only possible when employees receive appropriate training. During our interviews, several EICs and FMs noted that informal on-the-job training was the primary means to convey workpaper practices. The lack of a clear understanding among SEFL employees of expected workpaper practices increases the risk that examination conclusions may not be adequately documented.

Examiners Were Not Trained on Workpaper Practices

Ten of the 14 EICs and FMs we interviewed stated that training related to examination workpapers would be beneficial. For example, one EIC stated that having more training on examination workpapers would help to promote consistency among teams. In addition, one EIC stated that formalized training on examination workpapers would be helpful in holding examiners accountable for their work. This same EIC also recommended that any prospective training clearly address the process for uploading workpapers to the system of record. Further, one FM stated that it would be helpful to include examples of effective workpapers and summaries in any prospective training.

According to one FM, the examination staff comprises employees with diverse professional backgrounds. In the absence of clear, consistent workpaper practices and formal workpaper training, these individuals often try to learn the office's workpaper practices on the job; the practices they glean from their colleagues, however, may not align with agency practices. The absence of a formal training program for workpaper documentation may lead to inconsistent or inadequate workpapers.

Management Actions Taken

SEFL provided us with documentation about a training session held in October 2015. This documentation shows that the training addressed the transition from shared drive A to shared drive B, including details of the shared drive B folder structure and storage expectations for PII. One section of the training detailed how examiners can create and edit important examination documents, such as workpapers. We did not note any detailed guidance in the training concerning the documentation of completed examination procedures, interviews, or detailed testing results.

Recommendation

We recommend that the Associate Director of SEFL

16. Develop and provide training on the CFPB's policies and standards for workpapers that conveys to examiners the agency's expected workpaper practices. Determine the appropriate frequency for that training.

Management's Response

In the response to our draft report, the CFPB concurs with recommendation 16. The agency notes that SEFL will further develop and provide training on the CFPB's policies and standards for workpapers to reinforce expected documentation practices. The agency also indicated that SEFL will determine the appropriate method for and frequency of that training.

OIG Comment

The actions described by the CFPB appear to be responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Finding 7: SEFL Did Not Have an Ongoing Internal Quality Control Process to Assess Examination Workpapers

We found that examination workpapers were not undergoing internal quality control reviews at regular intervals. The *Examination Manual* indicates that workpapers should be reviewed through an internal quality control process. In mid-2014, one of the four CFPB regions initiated its own quality control review of examination workpapers in an effort to improve the examination process. An official involved with this effort stated that the quality control review resulted in higher-quality examination work. Despite these positive results, such reviews did not become recurring activities in the region, and SEFL has not developed or implemented an internal quality control review process that would apply across all four regions. In our opinion, a regularly scheduled internal quality control review process for examination workpapers would help SEFL to identify and mitigate many of the issues we noted during our evaluation and identify areas in which additional training is needed.

> "Workpapers will also be reviewed through an internal quality control process. Workpapers should be sufficiently detailed so that an internal quality control reviewer will understand what the examiner did, follow the logic of the examiner's analyses, and understand how the examiner reached his or her conclusion(s). The level of documentation should be commensurate with the risks and problems associated with the areas under review."
>
> —*Examination Manual*

SEFL Has Not Established an Ongoing Internal Quality Control Review Process

According to the *Examination Manual*, one of the three principal purposes for examiners to develop and maintain workpapers is "to facilitate internal quality control reviews." EICs and FMs from each of the four CFPB regions noted during interviews that they did not know whether their respective regions had any internal quality control processes in place to assess examination workpapers. Some interviewees noted that designated "review examiners" in the respective regions read the examination reports to confirm that examination teams have adequate support for the findings and conclusions in the examination reports. These review examiners only focus on findings and conclusions, however, and do not assess the adequacy of workpaper documentation.

One of the four CFPB regions initiated its own quality control review of examination workpapers in mid-2014. A SEFL headquarters official stated that the division had not established an ongoing internal quality control process to evaluate whether examination workpapers meet the requirements outlined in the *Examination Manual*.

The *Examination Manual* requires an internal quality control review process for examination workpapers and states that such a process should be a key control in the examination process. The one-time quality control review conducted in 2014 provided valuable insight in the form of observations, best practices, areas for improvement, and recommendations for the next steps needed to develop an effective workpaper program.

Management Actions Taken

In April 2015, a senior OSE official provided an overview of a supervision quality-management program during a SEFL manager training seminar. The overview included a description of intended quality control activities. In January 2017, senior OSE officials reviewed and approved the quality-management program approach. The approach states that the key focus of the quality management program in 2017 will be, among other items, ongoing reviews of high-risk and high-priority areas, timely corrective action recommendations and implementation, and stakeholder feedback. We understand that the quality-management program is moving forward; the plan is being fully implemented, and the division is conducting periodic reviews of targeted areas of the supervision program.

Recommendation

We recommend that the Associate Director of SEFL

17. Establish an ongoing internal quality control review process to assess and improve examination workpaper practices. As part of this effort, SEFL should consider reviewing the observations, best practices, areas for improvement, and recommendations that resulted from the 2014 workpaper quality control assessment.

Management's Response

In the response to our draft report, the CFPB concurs with recommendation 17. The agency notes that OSE will establish an ongoing internal quality control review process to assess and improve examination workpaper practices.

OIG Comment

The actions described by the CFPB appear to be responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Appendix A
Scope and Methodology

To accomplish our objectives, we reviewed relevant documentation, including the CFPB's *Examination Manual*; the *Handbook for Sensitive Information at the CFPB*; the CFPB's Permissible Use Standard; and Dodd-Frank Act title X, Bureau of Consumer Financial Protection.

We conducted our initial fieldwork from December 2014 to January 2016. We selected a nonrandom sample of eight examinations completed in 2013 and 2014. The sample included two examinations from each of the four CFPB regions and examinations of both depository institutions and nondepository institutions. Further, the sample consisted of examinations of varying types, such as baseline compliance management system reviews and continuous supervision reviews, and examinations with different EICs and FMs. Three examinations in our sample resulted in enforcement actions. In addition, for MRAs, we selected and reviewed the first two MRAs listed on each of the examinations in our sample against the guidance outlined in the *Examination Manual*.[14]

We reviewed the examination reports and workpaper documentation associated with each of the eight examinations in our sample. We assessed compliance with certain expectations outlined in the *Examination Manual*, for example, whether the workpapers generally demonstrate supervisory review and explain the sampling approach.

We interviewed the EICs and FMs assigned to these examinations. We also interviewed Regional Directors or other senior leaders from each of the four CFPB regions, senior officials and information technology employees from SEFL, RAOs from each of the four CFPB regions, the Chief Privacy Officer, and the Chief Information Security Officer.

We conducted additional fieldwork from June 2016 to December 2016 to assess the new policy and guidance document related to the new shared drive for supervision examinations and the initial system of record. Our testing included reviewing eight additional examinations that were completed in 2016 to determine whether examination teams were complying with both the new policy and the guidance document. The eight additional examinations consisted of depository and nondepository institutions covering the four CFPB regions. We interviewed FMs and RAOs from each of the four CFPB regions, as well as CFPB officials from the Office of Fair Lending and Equal Opportunity and the Office of Enforcement. During those interviews, we sought to understand the process for requesting, providing, and maintaining access rights to sensitive information in shared drive B and to determine whether each interviewee understood the expectations for restricting access to PII and CSI stored in the system of record and in shared drive B.

We conducted this evaluation in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency in January 2012.

14. One of the eight examinations that we reviewed had no MRAs.

Appendix B
Management's Response

Consumer Financial Protection Bureau

1700 G Street NW, Washington, DC 20552

September 15, 2017

Ms. Melissa Heist
Associate Inspector General for Audit 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 Examination Workpaper Documentation Practices*.

The Bureau appreciates the OIG's review and agrees with the recommendations for improving practices related to examination workpapers. As noted in the report, the Bureau made significant improvements to its policies, procedures, and capabilities around workpaper management since the beginning of the review period and continues to do so. Accordingly, some of the recommendations have already been implemented, and the Bureau is committed to taking steps toward implementing the remainder.

Thank you again for your review and the opportunity to provide comments on this report.

Sincerely,

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

Paul Sanford
Assistant Director,
Office of Supervision Examinations
Division of Supervision,
Enforcement, and Fair Lending

Consumer Financial Protection Bureau

1700 G Street NW, Washington, DC 20552

Responses to Specific Recommendations:

1. The Office of Supervision Examinations will reassess its open-access-within-each-region approach for access to examination data, identify measures to limit access to sensitive information, and ensure compliance with Bureau-wide data governance.

2. SEFL is working with the Chief Privacy Officer (within T&I) to develop practices and guidance related to security and information handling that are responsive to this recommendation. In addition to the annual training on information handling that all CFPB staff receive, OSE staff are required to take additional annual training specifically for handling CSI material. The SEFL/T&I working group recently distributed materials at the CFPB All Hands conference and is distributing materials at all upcoming regional conferences.

3. OSE and T&I are developing automated reports to monitor access to examination files. The new enterprise platform, upon which the system of record was built, was selected in part because of its extensive event and audit logging capabilities that support continuous monitoring and forensic analysis. OSE will work with T&I to make use of these tools in line with best practices. OSE is also a major stakeholder in the Bureau's collaboration and document management effort which aims to bring similar capabilities to shared drives.

4. OSE will develop an action plan as recommended. As noted in the report, the new system of record includes enhancements that will provide additional capabilities regarding tailoring of access restrictions. As also noted in the report, OSE is already working with T&I to implement a process to routinely restrict exam data on shared drives once an exam is closed.

5. In coordination with the CFPB's Records Management Office, SEFL will review its records management schedule and reassess which materials are required to be stored for record-keeping purposes. SEFL will continue to ensure sensitive information is securely retained in the appropriate system of record or shared drive.

6. OSE will periodically assess whether all regions are operating consistently with relevant SEFL directives, policies, guidance, and standards related to access rights.

7. OSE is working with T&I to plan for current and future storage needs for all examination-related data. The new system of record is built on an enterprise platform which T&I actively manages to support Bureau-wide business requirements, such as file storage needs. Additionally, the shared drive is supported by a dedicated T&I team which plans storage capacity according to OSE's requirements.

8. SEFL will develop an approach to review the contents of the shared drives, identify any CSI and personally identifiable information, and ensure that SEFL securely retains only the confidential supervisory information and personally identifiable information necessary for recordkeeping purposes.

9. OSE will modify the CFPB Supervision and Examination Manual to require that all documentation necessary to support findings and conclusions be stored in the appropriate location in the system of record for each examination before the examination is closed.

10. SEFL will develop an action plan to ensure that all supporting documentation created through internal consultations with employees outside of OSE is saved in the appropriate location in the system of record.

11. OSE will reinforce the requirement that examiners-in-charge and the field managers review and sign off on all workpapers developed during the examination by using a Workpaper Table of Contents and EIC Signoff document or another method developed for this purpose.

12. OSE will document all key steps of the examination process by enhancing the existing Workpaper Checklist or by using another method to capture that information.

13. OSE will develop a method to clarify the roles, responsibilities, and requirements of the Examiners-in-Charge and the Field Managers related to completing the Workpaper Checklist or other records with a similar function.

14. OSE will reinforce the guidelines for documenting sampling methods used in examination reports.

15. OSE will ensure that the internal quality control review process developed in response to Recommendation 17 includes steps for assessing the documentation of the sampling methods used during an examination.

16. SEFL will further develop and provide training on the CFPB's policies and standards for workpapers that conveys to examiners the CFPB's expected workpaper practices. SEFL will also determine the appropriate method for and frequency of that training.

17. Through OSE's Quality Management Program, OSE will establish an ongoing internal quality control review process to assess and improve examination workpaper practices.

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