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.