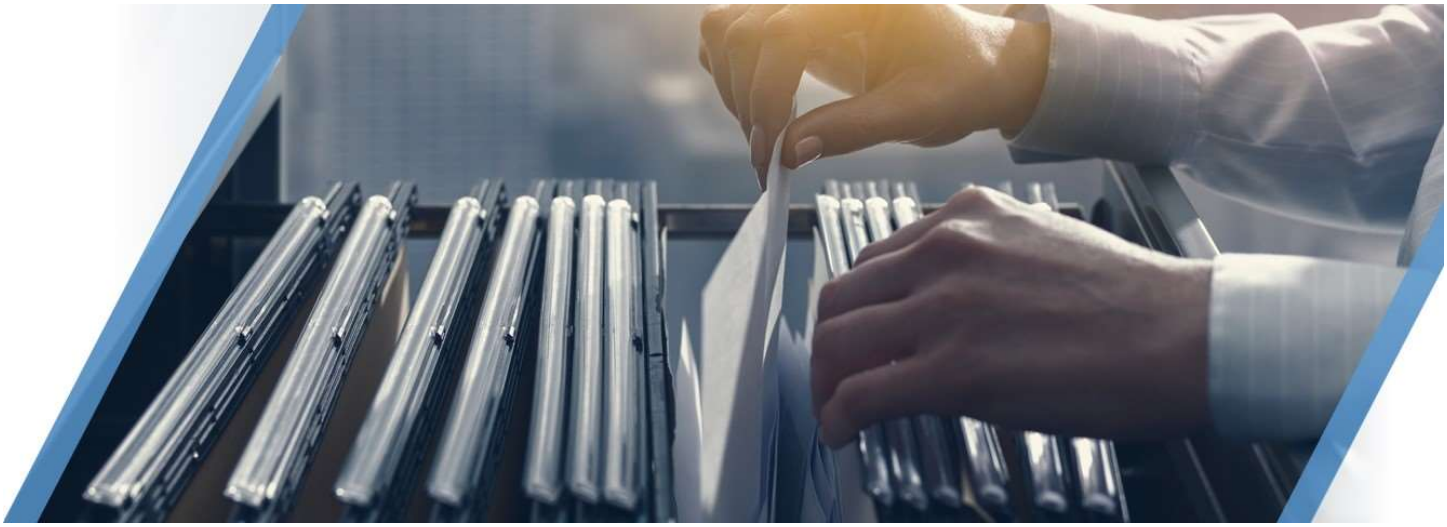
DINSMORE COMPLIANCE SERVICES

AN AFFILIATE OF DINSMORE & SHOHL LLP

Special Alert

May 5, 2023

SEC Division of Examinations Risk Alert April 26, 2023: Safeguarding Customer Records and Information at Branch Offices



The SEC Division of Examinations ("Examinations") issued a Risk Alert on April 26, 2023 to highlight the importance of establishing written policies and procedures for safeguarding customer records and information at branch offices. Examinations provides that a branch office includes any location other than a firm's main office, including offices of any independent contractors through which a firm may offer investment products and services.

The Risk Alert notes that some firms failed to adopt or implement written policies and procedures that address information security for their branch offices, even though such offices have access to technology systems that contain customer records and information.

Regulation S-P requires firms to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information. In assessing compliance with the requirements of Regulation S-P relating to branch office locations, Examinations highlights the following compliance issues:

Vendor Management

Examinations notes instances of firms not ensuring that their branch offices performed proper due diligence and oversight of their vendors as required by the firms' policies and procedures. This includes instances of firms not providing any guidance or recommendations to assist branch offices in the selection of vendors. These failures may result in weak or incorrect security settings and applications relating to implemented vendor systems.

Email Configuration

While firms generally manage email for all offices from the main office location, Examinations notes instances of firms not managing email accounts for branch offices. In addition, some firms lacked policies and procedures addressing branch office email configurations and permitted branch offices to obtain their own email services from vendors. Often in such situations, the branch office email services were configured incorrectly and subject to compromise. In addition, in various instances, the email configuration failed to capture account activity.

Data Classification

Examinations notes that firms did not consistently apply data classification policies and procedures to branch offices. Data classification generally refers to procedures to identify where customer records and information are stored electronically. In these instances, firms failed to identify and control customer records and information.

Access Management

Examinations notes firms that maintained password complexity, two factor authentication and related requirements for the main office, but not for branch offices. As a result, branch office systems became susceptible to breaches.

Technology Risk

The Risk Alert notes firms that implemented policies and procedures for inventory management, patch management and vulnerability management, but did not apply these policies and procedures to branch offices. As a result, branch offices were not up to date with system patching, and in some instances were running end of life systems. Also, Examinations notes firms not being aware of systems running on branch office networks.

For additional information regarding compliance policies, procedures and issues relating to branch offices, please refer to DCS' Alert regarding the November 9, 2020 OCIE/Division of Examinations Risk Alert: Supervision, Compliance and Multiple Branch Offices.

Here is the link to the Risk Alert: https://www.sec.gov/exams/announcement/safeguarding-customer-records-and-information-branch-offices