

SEC Issues Risk Alert on Safeguarding Customer Records and Information at Branch Offices

WRITTEN BY

Genna Garver | Ghillaine A. Reid | Jackson Buday | Stephanie Pindyck Costantino | Jay A. Dubow

On April 26, the SEC's Division of Examinations (EXAMS) issued a risk alert on the importance of broker-dealers and investment advisers (collectively, "firms") establishing and following written policies and procedures aimed at safeguarding customer records and information, particularly in branch offices. In its observations, the staff found that while many firms uphold their policies and procedures relating to the safeguard of customer records and information in their main offices, these firm policies and procedures are not implemented and/or adopted for remote or branch offices. This has resulted in heightened exposure to, and branch offices falling victim to, cybersecurity and data breaches.

The staff highlighted common issues raised, while assessing firms' compliance with Regulation S-P, which requires firms to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.

Vendor Management

Many firms failed to ensure that their branch offices perform proper due diligence and oversight of a vendor's use of the branch office when providing services, such as cybersecurity, technology operations, and business applications. In some instances, the staff found a firm provided no guidance or aid in assisting a branch office in the selection of vendors. This was found to result in weak or misconfigured security settings on systems and applications that could result in unauthorized access to customer records and information.

Email Configuration

Many firms use vendors to provide email services, oftentimes managed from the main office where accounts are provided for branch offices. Some firms, however, provide no guidance or assistance regarding email services from vendors and technical requirements needed to secure a branch office's email system. In some cases, this weak email configuration result in account takeover, business email compromise, and an inability to perform adequate incident responses.

Data Classification

The staff observed that firms failed to apply their data classification policies and procedures at branch offices concerning identifying where customer records and information are stored electronically. Firms' failure to implement such policies resulted in an inability to identify and control customer records and information at branch

offices.

Access Management

Many firms maintain policies that require password complexity and multifactor authentication for remote access at main offices but did not require and/or implement such controls at their branch offices. This resulted in branch offices experiencing breaches that could have been prevented if the controls observed at a firm's main office were in place.

Technology Risk

The staff observed that in some instances, branch offices were not subject to their main office's policies and procedures for inventory management, patch management, and vulnerability management. Such branch offices were prone to compromises as a result of running "end-of-life" operations no longer supported by the manufacturer, having out-of-date system patching, and running systems on the branch office networks of which the firm main office was not aware.

In light of this risk alert, broker-dealers and investment advisers should immediately review their policies and procedures for their branch offices and make any necessary changes to ensure compliance with the issues raised in the alert.

The SEC's risk alert is available at [Risk Alert: Safeguarding Customer Records and Information at Branch Offices \(sec.gov\)](#).

RELATED INDUSTRIES + PRACTICES

- [Investment Funds + Investment Management Services](#)
- [White Collar Litigation + Investigations](#)