RISK ALERT
DIVISION OF EXAMINATIONS

April 26, 2023

Safeguarding Customer Records and Information at Branch Offices

I. Introduction

The Division of Examinations (EXAMS) is issuing this risk alert* to highlight the importance of establishing written policies and procedures for safeguarding customer records and information at branch offices.[1] Many broker-dealers and investment advisers (collectively "firms") consist of a main office and multiple smaller offices ("branch offices"). Individuals in branch offices often have access to information technology systems that contain customer records and information. While many of these firms have implemented safeguarding policies and procedures at their main office, some firms did not adopt or implement written policies and procedures that address safeguards for their branch offices despite the existence of the same or similar risks. In some cases, this failure has resulted in firms falling victim to cybersecurity and data breaches.

II. Regulatory Framework

The Safeguards Rule of Regulation S-P (the "Safeguards Rule") requires firms to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[2] These written policies and procedures must be

---

* This Risk Alert represents the views of the staff of the Division of Examinations (the "Division"). This Risk Alert is not a rule, regulation, or statement of the Securities and Exchange Commission (the "SEC" or the "Commission"). The Commission has neither approved nor disapproved the content of this Risk Alert. This Risk Alert, like all staff statements, has no legal force or effect: it does not alter or amend applicable law, and it creates no new or additional obligations for any person. This document was prepared by Division staff and is not legal advice.

[1] FINRA Rule 3110(f) sets forth a definition for "branch office." FINRA Rule 3110(f) *available at* 3110. Supervision | FINRA.org. However, as used in this risk alert, the term "branch office" applies more broadly to include any location other than a firm's main office, including offices of any independent contractors through which the firm may offer investment products and services.

[2] See 17 C.F.R. Part 248, Subpart A—Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information. The Commission proposed rules to address registrant cybersecurity risk and related disclosures, amendments to Regulation S-P, and other enhancements related to the cybersecurity and resiliency of certain SEC registrants. See Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Securities Act Rel. No. 33-11028 (Feb. 9, 2022), 87 FR 13524 (Mar. 9, 2022); Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, Securities Act Rel. No. 34-97142 (Mar. 15, 2023), 88 FR 20212 (Apr. 5, 2023); and Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, Securities Act Rel. No. 34-97141 (Mar. 15, 2023).

reasonably designed to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of customer records and information, and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

III. Common Issues Related to Branch Office Governance

In assessing compliance with the Safeguards Rule, staff observed that while many firms implemented policies and procedures for safeguarding customer records and information for their main office, they often did not do so for branch offices. In particular, staff observed the following:

Vendor Management

Firms use vendors to provide services such as cybersecurity, technology operations, and business applications. In many instances firms did not appear to reasonably ensure that their branch offices performed proper due diligence and oversight of their vendors as required by the firms' own policies and procedures. In some of these instances, firms did not provide any guidance or recommendations to assist branch offices in the selection of vendors. This resulted in weak or misconfigured security settings on systems and applications at some firms, which could result in unauthorized access to customer records or information.

Email Configuration

Firms often use vendors to provide email services. Staff observed that in many instances, these services are managed from the main office where staff or vendors provide accounts for branches. However, in some instances, firms did not manage email accounts for branch offices. Moreover, some firms lacked policies and procedures addressing branch office email configurations and allowed branch office staff to obtain their own email services from vendors without specifying the technical requirements adequate to secure the branch offices' email solution. In some instances, weak email configuration resulted in account takeover or business email compromise. In other instances, default email configuration failed to capture all account activity, resulting in the inability to perform adequate incident response.

Data Classification

Staff observed that while firms often maintained data classification written policies and procedures to identify where customer records and information were stored electronically, firms did not always apply these policies and procedures to branch offices. We observed that this lack of data classification policies and procedures resulted in a failure to identify and control customer records and information in some instances.

Access Management

Staff observed that firms often maintain policies and procedures requiring password complexity and multi-factor authentication for remote access to firm systems. Although some firms required these controls for the main office, they did not require similar controls for branch offices. As a

result many branch offices did not apply any such controls and became victims of breaches. In these cases, multi-factor authentication, password complexity requirements, and other controls used at the main office may have prevented the breach.

Technology Risk

Staff observed that many firms focus on technology risk by implementing written policies and procedures for inventory management, patch management, and vulnerability management. In some instances, however, though the firms maintained reasonable technology policies and procedures for their main office, they did not apply any such policies and procedures in connection with their branch offices. As a result, multiple branch offices were not up to date with system patching. Some firms were not aware of the systems running on the branch office networks, and some branch offices were running end of life operating systems.[3] As a result, branch office systems were more prone to compromises.

IV. Conclusion

In response to these observations, many of the firms modified their written policies and procedures to mitigate the issues identified by EXAMS staff. Firms should consider their entire organization, including branch offices, when implementing written policies and procedures for the safeguarding of customer records and information to ensure they are compliant with Regulation S-P.

This Risk Alert is intended to highlight for firms risks and issues that Division staff has identified. In addition, this Risk Alert describes risks that firms may consider to (1) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (2) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.

[3] Operating systems that are "end of life" are no longer supported by the manufacturer. Thus, any new bugs or security weaknesses identified in the operating system will not be corrected or patched by the manufacturer of that operating system.