RISK ALERT
OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

May 23, 2019

Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features

Key Takeaway: *This Risk Alert highlights risks associated with the storage of electronic customer records and information by broker-dealers and investment advisers in the cloud and on other types of network storage solutions.*

I. Introduction

During recent examinations, the Office of Compliance Inspections and Examinations ("OCIE")* identified security risks associated with the storage of electronic customer records and information by broker-dealers and investment advisers in various network storage solutions, including those leveraging cloud-based storage.[1] Although the majority of these network storage solutions offered encryption, password protection, and other security features designed to prevent unauthorized access, examiners observed that firms did not always use the available security features. Weak or misconfigured security settings on a network storage device could result in unauthorized access to information stored on the device.

II. Summary of Examination Observations

OCIE staff has observed firms storing electronic customer records and information using various types of storage solutions, including cloud-based storage. During examinations, OCIE staff identified the following concerns that may raise compliance issues under Regulations S-P and S-ID:[2]

- *Misconfigured network storage solutions*. In some cases, firms did not adequately configure the security settings on their network storage solution to protect against unauthorized access. In addition, some firms did not have policies and procedures addressing the security configuration of

---

* The views expressed herein are those of the staff of OCIE. The Securities and Exchange Commission (the "SEC" or the "Commission") has expressed no view on the contents of this Risk Alert. This document was prepared by OCIE staff and is not legal advice.

1 Cloud storage refers to the electronic storage of information on infrastructure owned and operated by a hosting company or service provider. *See, e.g.*, *The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-145 (September 2011).

2 The Safeguards Rule of Regulation S-P requires every broker-dealer and investment adviser registered with the Commission to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. 17 C.F.R. 248.30(a).

The Identity Theft Red Flags Rule of Regulation S-ID requires broker-dealers and investment advisers registered or required to be registered with the Commission to develop and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. 17 C.F.R. 248.201. A covered account includes an account that a broker-dealer or investment adviser offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. 17 C.F.R. 201(b)(3).

their network storage solution. Often, misconfigured settings resulted from a lack of effective oversight when the storage solution was initially implemented.

- *Inadequate oversight of vendor-provided network storage solutions*. In some cases, firms did not ensure, through policies, procedures, contractual provisions, or otherwise, that the security settings on vendor-provided network storage solutions were configured in accordance with the firm's standards.

- *Insufficient data classification policies and procedures.* In some cases, firms' policies and procedures did not identify the different types of data stored electronically by the firm and the appropriate controls for each type of data.

III. Examples of Effective Practices

The implementation of a configuration management program that includes policies and procedures governing data classification, vendor oversight, and security features will help to mitigate the risks incurred when implementing on-premise or cloud-based network storage solutions. During examinations, OCIE staff has observed several features of effective configuration management programs, data classification procedures, and vendor management programs, including:

- Policies and procedures designed to support the initial installation, on-going maintenance, and regular review of the network storage solution;

- Guidelines for security controls and baseline security configuration standards to ensure that each network solution is configured properly; and

- Vendor management policies and procedures that include, among other things, regular implementation of software patches and hardware updates followed by reviews to ensure that those patches and updates did not unintentionally change, weaken, or otherwise modify the security configuration.

IV. Conclusion

In sharing these observations, OCIE encourages registered broker-dealers and investment advisers to review their practices, policies, and procedures with respect to the storage of electronic customer information and to consider whether any improvements are necessary. OCIE also encourages firms to actively oversee any vendors they may be using for network storage to determine whether the service provided by the vendor is sufficient to enable the firm to meet its regulatory responsibilities.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) 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.