Securities Litigation Alert

Akin Gump
STRAUSS HAUER & FELD LLP

SEC OCIE Issues Guidance on Advisors' and Broker-Dealers' Cloud-Based and Other Network Storage of Customer Data

May 18, 2019

Key Points

- On May 23, 2019, the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert describing its observations in past examinations of weaknesses and best practices for addressing security risks associated with network storage of customer data.
- This Risk Alert fits with the SEC's increased focus on compliance in the face of evolving technology and cybersecurity threats, which prompted warnings within the past year on topics such as electronic messaging, email spoofing attacks and privacy-related matters.
- The Risk Alert encourages firms to review and update as needed their practices, policies and procedures regarding network storage of customer data. Importantly, it also encourages firms to take an active oversight role regarding third-party vendors they may be using for network storage to determine whether the storage meets the firms' security requirements and other regulatory responsibilities.

Background

With the advance of technology, many businesses and individuals alike have begun to store their data in cloud and other network storage solutions, such as Amazon Web Services, iCloud, Dropbox and Google Cloud Platform. Similarly, many investment advisors and broker-dealers have adopted network storage solutions for their data. This data may include customer records and information, which raises potential compliance concerns under Regulations S-P and S-ID. In particular, OCIE's Risk Alert identifies potential compliance issues under the Safeguards Rule of Regulation S-P and the Identity Theft Red Flags Rule of Regulation S-ID.[1]

Observations and Best Practices

The Risk Alert identifies multiple areas of concern associated with firms' network storage practices:

Contact Information

If you have any questions concerning this alert, please contact:

Peter I. Altman
Partner
paltman@akingump.com
Los Angeles
+1 310.728.3085

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

=Jason M. Daniel
Partner
jdaniel@akingump.com
Dallas
+1 214.969.4209

Diane E. Schaffner
Counsel
dschaffner@akingump.com
San Francisco
+1 415.765.9507

Kelly Handschumacher
Assocuate
khandschumacher@akingump.com
Los Angeles
+1 310.229.1071

- Firms that fail to adequately configure the security settings of their network storage to protect against unauthorized access, and relatedly lack policies and procedures to address the security configuration of their network storage.
- Firms that fail to ensure, through policies, procedures and contractual provisions or otherwise, that vendor-provided network security settings match the firm's security standards.
- Firms that fail to adopt policies and procedures to identify the types of data stored electronically by the firm and the appropriate controls for each type of data.

Having identified potential weaknesses, OCIE next identified effective practices its staff had observed in examinations:

- Implementing policies and procedures to support the installation, on-going maintenance and regular review of the firm's network storage system.
- Adopting guidelines for security controls and baseline security configuration standards to ensure proper configuration of each network solution.
- Implementing vendor management policies and procedures, including, 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.

Conclusion

Given OCIE's attention to this topic, as well as its ongoing attention to electronic communication and data management by broker-dealers and investment advisors, firms in future examinations are likely to face inquiries regarding their policies and procedures for safeguarding customer records and information in network storage and for overseeing activities by their network storage vendors.

1 Under the Safeguards Rule of Regulation S-P, every broker-dealer and investment advisor registered with the SEC must 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).

Under the Identity Theft Red Flags Rule of Regulation S-ID, broker-dealers and investment advisors registered or required to be registered with the SEC must 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 advisor 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).

akingump.com