OCIE Risk Alert Helps Firms Safeguard Customer Records and Information In Network Storage

June 25, 2019

On May 23, 2019, the SEC's Office of Compliance Inspections and Examinations ("OCIE") published a Risk Alert addressing safeguarding of customer records and information in network storage. OCIE's Risk Alert identified a number of security risks that arise from the electronic storage of customer records and information by broker-dealers and registered investment advisers ("RIAs") when using various network storage solutions, including firms utilizing cloud-based storage. With cloud-based storage solutions, electronic information is stored on infrastructure owned and operated by a hosting company or service provider.

The Risk Alert is based on recent cybersecurity examinations, which focused on RIAs using cloud service providers. Examiners looked closely at firms' practices when dealing with cloud providers. According to the June, 2019 edition of *IAA Newsletter*, these examinations were separate from OCIE's Cyber 3 Initiative, which targeted firms with multiple branch offices. The Cyber 3 Initiative also focused on how firms that merged combined their cybersecurity processes.

Although most network storage solutions utilized by RIAs and broker-dealers offer encryption, password protection, and other security features intended to prevent unauthorized access, examiners found that the firms did not always employ the available security features. Weak or misconfigured security settings on a network storage device may lead to unauthorized access to information.

Firms were duly warned that OCIE is concerned about network storage. In its 2019 Examination Priorities, OCIE said, "Examinations will focus on, among other things, proper configuration of network storage devices, information security governance generally, and policies and procedures related to retail trading information security."

What examiners learned about network storage solutions

Examiners observed that firms storing customer records and information electronically use different methods, including cloud-based storage. Examiners were particularly concerned about several areas, which could give rise to compliance problems under Regulations S-P and S-ID. Regulation S-P is the SEC's primary rule governing the privacy notices and safeguarding policies of RIAs and broker-dealers. Regulation S-ID, better known as the "Identity Theft Red Flags Rule," requires certain companies to take steps to detect, prevent, and mitigate the impact of identity theft.

According to the Risk Alert, examiners discovered the following potential problems:

Misconfigured network storage solutions. Certain firms did not adequately configure the security settings on their network storage solution to guard against unauthorized access. Some firms did not have policies and procedures in place to address the security configuration of their network storage solution. Frequently, misconfigured settings arose from ineffective oversight at the time the storage solution was implemented.

Inadequate oversight of vendor-provided network storage solutions. In some instances, firms' policies and procedures, as well as contracts, did not ensure that the security settings on the vendor-provided network storage solutions were configured properly.

Insufficient data classification policies and procedures. Some firms' policies and procedures did not identify the various types of data stored electronically and the appropriate controls needed to protect customers' information.

Examples of effective practices gleaned from the Risk Alert

In the Risk Alert, OCIE offered several examples of effective configuration management programs, data classification procedures, and vendor management programs. Firms may benefit by implementing:

- Policies and procedures intended to support the initial installation, ongoing maintenance, and regular review of the network storage solution;
- Security controls guidelines and baseline security configuration

standards to make certain that each network solution is configured properly; and
- Vendor management policies and procedures to ensure the regular implementation of software patches and hardware updates, which are followed by reviews to determine if those patches and updates unintentionally changed, weakened, or otherwise modified the security configuration.

OCIE's Risk Alert can be found at https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf?_cldee=bGFicm9tb3ZpdHpAZm9yZXNpZGUuY29t&recipientid=contact-ad35a968ed1ee71180ebc4346bacfbbc-d71d3663cca54a529fa084a90b291d14&utm_source=ClickDimensions&utm_medium=email&utm_campaign=Member%20Alerts&esid=4c1617fb-9e7d-e911-a844-000d3a178fc7.

Conclusion

When OCIE publishes Risk Alerts like this one, RIAs and broker-dealers should review their own policies and procedures to determine if they are following the SEC's recommendations. This specific Risk Alert encouraged RIAs and broker-dealers to actively oversee any vendors on which they may be relying for network storage to determine whether the services will enable them to satisfy their regulatory responsibilities.

Broker-dealers should also look to FINRA for guidance when outsourcing activities or functions to third-party vendors. FINRA's Notice to Members 05-48 addresses outsourcing to third-party vendors.

Even if firms are SEC-registered, they may benefit from a review of the North American Securities Administrators Association ("NASAA") new model rule related to cybersecurity. These practices may prove beneficial for most firms. Among other requirements, NASAA's model rule requires state-registered advisers to adopt policies and procedures governing physical security of information and cybersecurity, as well as to deliver their privacy policy annually to clients. NASAA's model rule package can be found at http://www.nasaa.org/47808/nasaa-members-adopt-investment-adviser-information-security-model-rule-package/.

Firms should also examine at OCIE's Regulation S-P Risk Alert, which discussed a number of deficiencies or weaknesses related to Regulation S-P. The purpose of that Risk Alert was to assist RIAs and broker-dealers with adopting and implementing effective policies and procedures for safeguarding customer records and information. The Risk Alert was also intended to help RIAs and broker-dealers distribute compliant privacy and opt-out notices. The Risk Alert is available at https://www.sec.gov/ocie/announcement/ocie-risk-alert-regulation-s-p.

This article is not a solicitation of any investment product or service to any person or entity. The content contained in this article is for informational use only and is not intended to be and is not a substitute for professional financial, tax or legal advice..