KILPATRICK TOWNSEND

May 29, 2019

Cloud Storage and Use of Vendors for Records Management Flagged by OCIE in Alert

by Jeffrey T. Skinner , Lauren C. Jackson , Alexandra M. Fenno

---

Regulations regarding privacy, cybersecurity and the use of technology seem to be in constant flux. Compliance consultants and vendors do their best to stay on top of them, but ultimately neither are regulated by the SEC, FINRA or the states. Instead, it is the registrants who will be held accountable—both by their clients and their regulators—when data is lost, stolen or misused.

Adding to an increasingly long line of guidance,[1] the SEC's Office of Compliance Inspections and Examinations (the "OCIE") released a Risk Alert (the "Alert") last Thursday that highlighted risks associated with the storage of customer records and information by broker-dealers ("BDs") and registered investment advisers ("RIAs") in cloud-based systems and other network storage solutions.[2] In the Alert, the OCIE identified multiple storage practices that put customer information at risk of unauthorized access and raise concerns under Regulations S-P[3] and S-ID.[4]

The Alert

Key concerns identified by the OCIE in its Alert included firms' failure to:

- Configure security settings on network storage solutions to protect against unauthorized access, or to address such configuration in their policies and procedures;
- Ensure that security settings on vendor-provided network storage solutions were configured in accordance with the firms' standards; and
- Identify the different types, or the appropriate controls for each type, of electronically stored data.[5]

The OCIE noted that RIAs and BDs can help mitigate security risks through a strong configuration management program that includes policies and procedures governing data classification, vendor oversight and security features. It noted that effective programs included features such as:

- Policies and procedures supporting the initial installation, ongoing maintenance and regular review of network storage solutions;
- Guidelines for securities controls and baseline security configuration standards to ensure proper configuration; and

- Vendor management policies and procedures that include, among other things, regular software patches and hardware updates followed by reviews to ensure effectiveness of the security configuration.[6]

Finally, the OCIE encouraged BDs and RIAs to review their practices, policies and procedures with respect to the storage of electronic customer information; to actively oversee the vendors they use for network storage; and to consider whether any improvements are necessary. BDs and RIAs should consult with counsel with respect to these reviews. As an additional step, BDs and RIAs can review current and proposed vendor agreements to identify and understand risks they may present as well the applicability of indemnification provisions.

Practical Considerations

You have a variety of tools to help you meet the regulatory obligations outlined in the Alert. If you choose to use compliance consultants or vendors to help you meet your retention and security obligations, it is absolutely incumbent upon you to ensure the solution that you choose fully complies with all applicable state and federal rules. Often, vendors offer a range of products and services that are not compliant unless they are expertly configured and continuously maintained with specific attention to current requirements.

A few practical considerations to keep in mind:

- Products and services marketed to RIAs and BDs are often also sold to all sorts of other companies for document management purposes. As such, the products are designed for a variety of uses and configurations. You cannot assume that the products will be designed in a way that is regulatory-compliant. Regulatory-complaint usage is typically more expensive than other options. Further, procuring a storage solution from a provider that offers compliant storage is not the same as procuring and maintaining a compliant solution.
- Identifying and choosing the right product is only step one. You must also have policies in place to ensure that you and your employees use the product in a compliant manner, and that there are change management controls in place to ensure that down the road a compliant system is not accidentally altered in a way that renders it non-compliant.
- Review all vendor contracts carefully. For example, with respect to cloud-based storage, you should consider the following:
    - Do you maintain ownership, possession and control of your firm's records or can an employee or other authorized user take, alter or destroy your records?
    - What rights does the vendor have to purge or destroy your required regulatory records if, for example, your're unable to pay storage fees?
- Consider whether an old-fashioned option (e.g., paper files or microfiche) may work better for your business.

Further, while not specifically discussed in the Alert, the practices at issue also prompt concerns relating to

cybersecurity (a 2019 examination priority)[7] and compliance with FINRA's and the SEC's recordkeeping requirements, particularly SEC Rule 17a-4(f) (for BDs) and SEC Rule 204-2(g) (for RIAs). These rules prescribe the form and manner of record retention and regularly form the basis for enforcement proceedings and the assessment of large fines, even when no harm has resulted from the violations.

If you have any questions related to protecting your network storage solutions from security risks, or about any other aspect of the regulation of BDs and RIAs, please feel free to contact us.

*By the **Investment Management and Broker-Dealer Team** at **Kilpatrick Townsend & Stockton***

Footnotes

1] See, e.g., OCIE Risk Alert, Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies (April 16, 2019), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf; OCIE Risk Alert, Observations from Cybersecurity Examinations (Aug. 7, 2017), https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

[2] OCIE Risk Alert, Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features (May 23, 2019), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf (hereinafter, "Alert").

[3] Regulation S-P requires every registered BD and RIA to adopt written policies and procedures addressing the protection of customer records and information. 17 C.F.R. 248.30(a).

[4] Regulation S-ID requires BDs and RIAs to have a written identity theft prevention program that detects, prevents and mitigates identity theft in connection with the opening of an account maintained for personal, family or household purposes that involves or permits multiple payments or transactions. 17 C.F.R. 248.201.

[5] Alert, supra note 2.

[6] Id.

[7] Within the priority of cybersecurity, OCIE is focusing on: governance and risk assessments (particularly policies and procedures relating to retail client trading information security), access rights and controls (i.e., which employees are able to access confidential information and who controls those permissions), loss prevention, vendor management (both when a new vendor is hired, and when making changes with an existing vendor or changing from one vendor to another), training and incident response (i.e., how you respond when a breach has occurred to mitigate harm and enhance systems and procedures going forward). OCIE 2019 Examination Priorities (Dec. 20, 2018), https://www.sec.gov/files/OCIE%202019%20Priorities.pdf.