KIRKLAND & ELLIS

Kirkland AIM

OCIE Risk Alert Relating to Safeguarding Customer Records and Information in Cloud-Based and Other Network Storage

30 May 2019

On May 23, 2019, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a Risk Alert regarding the storage of electronic customer records in network and cloud-based storage solutions. The Risk Alert signals OCIE's continued focus on cybersecurity and data privacy policies and practices of investment advisers and broker-dealers.[1]

Compliance Concerns

The Risk Alert details a number of OCIE Staff concerns observed in recent examinations of registered firms relating to the electronic and cloud-based storage of customer records, including failures to:

- adequately configure the security settings on the firm's network storage solution to protect against unauthorized access and to implement policies and procedures addressing the security configuration of the network storage solution;
- ensure (through policies, procedures, contractual provisions, or otherwise) that the security settings on vendor-provided network storage solutions are configured in accordance with the firm's standards; and
- properly identify the types of data stored electronically by the firm and the appropriate controls for each type of data.

Best Practices

The Risk Alert also sets forth examples of policies and practices that OCIE Staff has found to be effective in mitigating the risks associated with cloud-based and other network storage systems, including:

- policies and procedures designed to support the initial installation, ongoing 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 do not unintentionally change, weaken or otherwise modify the security configuration.

Key Considerations

As the SEC has demonstrated an ongoing focus on cybersecurity and data privacy compliance,[2] investment advisers and broker-dealers should:

- review their existing policies and procedures in light of the OCIE Staff observations set forth in the Risk Alert;
- evaluate the adequacy of the resources, including personnel and funding, that have been allocated to develop and implement the appropriate policies, procedures and oversight recommended in the Risk Alert; and
- review the appropriateness of the firm's training programs to ensure that firm personnel properly use and manage network security solutions.

For assistance with these or other items, please contact the Kirkland Investment Funds regulatory attorney with whom you usually work.

Regulatory: Norm Champ, Scott Moehrke, Kevin Bettsteller, Michael Chu, Matthew Cohen, Marian Fowler, Nicholas Hemmingsen, Alpa Patel, Jaime Schechter, Aaron Schlapoff, Christopher Scully, Robert Sutton, Ryan Swan, Jamie Lynn Walter, Josh Westerholm, Corey Zarse, Radhika Kshatriya

Enforcement: Neil Eggleston, Kenneth Lench, Robert Pommer, Erica Williams

Cybersecurity/Litigation: Sunil Shenoi

[1] The Safeguards Rule of Regulation S-P requires registered investment advisers and broker-dealers to adopt written policies and procedures designed to safeguard customer records and information. The Identity Theft Red Flags Rule of Regulation S-ID requires registered broker-dealers and certain investment advisers to implement an identity theft program to mitigate the risk of individual customers' identity theft.↩

[2] See In the Matter of Voya Financial Advisors Inc., Exchange Act Release No. 84288, Investment Advisers Act Release No. 5048 (Sept. 26, 2018), available at https://www.sec.gov/litigation/admin/2018/34-84288.pdf; In the Matter of Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415 (June 8, 2016), available at https://www.sec.gov/litigation/admin/2016/34-78021.pdf for SEC enforcement settlements including cybersecurity failures at registered firms.↩

Authors

Norm Champ, P.C.

Partner / New York

Scott A. Moehrke, P.C.

Partner / Chicago

Kevin R. Bettsteller

Partner / San Francisco

Michael Chu

Partner / Chicago

Matthew Cohen

Partner / San Francisco

Marian Fowler

Partner / Washington, D.C.

Nicholas A. Hemmingsen

Partner / Chicago

Alpa Patel

Partner / Washington, D.C.

Jaime Doninger Schechter

Partner / New York

Aaron J. Schlaphoff, P.C.

Partner / New York

Christopher J. Scully

Partner / Chicago

Robert H. Sutton

Partner / New York

Ryan P. Swan

Partner / Chicago

Jamie Lynn Walter, P.C.

Partner / Washington, D.C.

Josh Westerholm

Partner / Chicago

Corey Zarse

Partner / Chicago

W. Neil Eggleston

Partner / Washington, D.C.

Kenneth R. Lench

Partner / Washington, D.C.

Robert W. Pommer III

Partner / Washington, D.C.

Erica Williams, P.C.

Partner / Washington, D.C.

Radhika Kshatriya

Associate / Los Angeles

Sunil Shenoi

Partner / Chicago

Related Services

Practices

- Transactional
- Investment Funds

Suggested Reading

- 09 May 2019 Kirkland AIM SEC Settles with Private Fund Manager and its Principals Over Alleged Misuse of Fund Assets
- 07 January 2019 Kirkland AIM 2019 Private Fund Manager Compliance Update: U.S. SEC/CFTC Filing Deadlines and SEC Examination Priorities
- 20 December 2018 Kirkland AIM OCIE Risk Alert Relating to Electronic Messaging

This communication is distributed with the understanding that the author, publisher and distributor of this communication are not rendering legal, accounting, or other professional advice or opinions on specific facts or matters and, accordingly, assume no liability whatsoever in connection with its use. Pursuant to applicable rules of professional conduct, this communication may constitute Attorney Advertising.