Simpson Thacher

Memorandum

SEC Risk Alert Highlighting Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P

April 22, 2019

On April 16, 2019, the Office of Compliance Inspections and Examinations ("OCIE") of the U.S. Securities and Exchange Commission ("SEC") issued a Risk Alert (the "Risk Alert")[1] highlighting OCIE's observations of common compliance issues relating to Regulation S-P ("Reg S-P"). Reg S-P is the primary SEC rule governing the privacy notices and privacy protection policies of registered investment advisers and broker-dealers ("Registrants").[2] This Risk Alert follows multiple SEC cybersecurity initiatives aimed at assessing Registrant cybersecurity preparedness.[3] Below is a summary of the Reg S-P compliance issues identified in the Risk Alert and some key takeaways for Registrants.[4]

Risk Alert

The Risk Alert focuses primarily on Reg S-P's requirements for Registrants to deliver privacy notices to "customers" and to adopt policies and procedures for safeguarding customer records and information.[5]

---

[1] *Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies*, SEC OCIE Risk Alert (Apr. 16, 2019).

[2] 17 C.F.R. §§ 248.1 – 248.31-248.100 app. A.

[3] Most recently, OCIE published a summary of the OCIE staff's observations from the "Cybersecurity 2 Initiative," following examinations of 75 Registrants to assess cybersecurity preparedness. The "Cybersecurity 2 Initiative" focused on: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response. *See* *Observations from Cybersecurity Examinations*, National Exam Program Risk Alert, Volume VI, Issue 5 (Aug. 7, 2017).

[4] This Risk Alert reflects issues identified in deficiency letters from broker-dealer and investment adviser exams completed during the past two years. The Risk Alert does not discuss all types of deficiencies or weaknesses related to Reg S-P that have been identified by OCIE staff.

[5] Reg S-P defines "customer" to mean a "consumer" that has a "customer relationship" with a financial institution, and defines "customer relationship" to mean a continuing relationship between a "consumer" and a financial institution and

Privacy Notices

Reg S-P requires a Registrant to provide a clear and conspicuous notice to its customers that accurately reflects its privacy policies and practices, generally no later than when a Registrant establishes a customer relationship.[6] OCIE staff observed Registrants that failed to provide these initial privacy notices as well as Registrants that provided initial privacy notices but failed to accurately reflect their policies and procedures in such initial privacy notices.

Policies and Procedures

Under Reg S-P, Registrants must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. OCIE staff asserted that certain Registrants failed to adopt written policies and procedures as required under Reg S-P. OCIE staff also noted that the written policies and procedures some Registrants did adopt either lacked sufficient safeguards or were not properly implemented.

Notably, OCIE staff observed that Registrant policies and procedures were not reasonably designed to safeguard customer information on personal devices, did not address the inclusion of customer personally identifiable information ("PII") in electronic communications, and did not prohibit employees from accessing unsecure networks and locations outside of the Registrant's network when sending or accessing PII. In addition, the staff noted that certain Registrants did not train employees on encryption methods and other safeguards for protecting customer information.

OCIE staff also observed a failure on the part of some Registrants to adequately monitor and maintain PII in secure locations, to properly inventory all systems on which PII was maintained, and to prevent the misuse or mishandling of customer login credentials. The staff further noted a failure on the part of some Registrants to adopt incident response plans that prescribe actions required to address a cybersecurity incident and set processes for assessing system vulnerabilities. Finally, the staff observed that certain

includes an individual who has a brokerage account with a broker-dealer or an advisory contract with an investment adviser (whether written or oral). 17 CFR §§ 248.3(j)-(k). The term "consumer" means an individual who obtains from a financial institution financial products or services that are to be used primarily for personal, family, or household purposes, or the legal representative of such an individual. 15 U.S.C. § 6809(9).

[6] Reg S-P also requires a Registrant to provide an annual privacy notice to a customer where the Registrant either (1) shares non-public personal information about the customer for certain purposes that trigger the customer's statutory right to opt out of such information sharing or (2) has changed its policies and practices with regard to disclosing non-public personal information from the policies and practices that were disclosed in its most recent privacy notice. In addition, Registrants that share non-public personal information about a customer with a non-affiliated third party must deliver a notice to the customer that explains the right to opt out of some disclosures of such information, subject to certain important exceptions; for example, a Registrant's disclosure of non-public customer personal information with its attorneys, accountants, and auditors does not trigger an opt-out notice requirement.

Registrants failed to follow their own policies and procedures regarding outside vendors and failed to restrict former employees from accessing customer information following their departure from the firms.

Key Takeaways for Investment Advisers and Broker-Dealers

For the past few years, the SEC staff has been focused on cybersecurity and the attendant risks associated with a failure to implement policies and procedures reasonably designed to safeguard customer records and information. Registrants should consider this Risk Alert to be a strong signal of the SEC's intent to continue to focus on this area. In response, Registrants should review their current privacy protection and cybersecurity policies and procedures and assess whether any enhancements should be made in light of the compliance issues identified in the Risk Alert.

For further information, please contact one of the following members of the Firm.

NEW YORK CITY

Michael W. Wolitzer
+1-212-455-7440
mwolitzer@stblaw.com

Allison Scher Bernbach
+1-212-455-3833
allison.bernbach@stblaw.com

Meredith J. Abrams
+1-212-455-3095
meredith.abrams@stblaw.com

Manny M. Halberstam
+1-212-455-2388
manny.halberstam@stblaw.com

WASHINGTON, D.C.

David W. Blass
+1-202-636-5863
david.blass@stblaw.com

Simpson Thacher Worldwide

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
600 Travis Street, Suite 5400
Houston, TX 77002
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
900 G Street, NW
Washington, D.C. 20001
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3901 China World Tower A
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino
Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000