RISK ALERT
OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

April 16, 2019

Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies

Key Takeaway: Through sharing some of the Regulation S-P compliance issues it observed, OCIE encourages registrants to review their written policies and procedures, including implementation of those policies and procedures, to ensure compliance with the relevant regulatory requirements.

I. Introduction

The Office of Compliance Inspections and Examinations ("OCIE")* is providing a list of compliance issues related to Regulation S-P, the primary SEC rule regarding privacy notices and safeguard policies of investment advisers and broker-dealers.[1] These issues were identified in recent examinations of SEC-registered investment advisers ("advisers") and brokers and dealers ("broker-dealers," and together with advisers, "registrants" or "firms").[2] The information in this Risk Alert is intended to assist advisers and broker-dealers in providing compliant privacy and opt-out notices, and in adopting and implementing effective policies and procedures for safeguarding customer records and information, under Regulation S-P.[3]

Privacy and Opt-Out Notices

Regulation S-P, among other things, requires a registrant to: (1) provide a clear and conspicuous notice to its customers that accurately reflects its privacy policies and practices generally no later than when it establishes a customer relationship ("Initial

* The views expressed herein are those of the staff of OCIE. The Securities and Exchange Commission ("SEC") has expressed no view on the contents of this Risk Alert. This document was prepared by OCIE staff and is not legal advice.

[1] *See* 17 CFR Part 248, Subpart A, and Appendix A to Subpart A. *See also* Privacy of Consumer Financial Information (Regulation S-P), Release Nos. 34-42974, IC-24543, IA-1883 (June 22, 2000) (adopting rules implementing the privacy provisions of Subtitle A of Title V of the Gramm- Leach-Bliley Act ("GLBA") with respect to financial institutions regulated by the SEC); Disposal of Consumer Report Information, Release Nos. 34-50781, IA-2332, IC-26685 (December 2, 2004) (adding rule requiring proper disposal of consumer report information (17 CFR 248.30(b), "Disposal Rule") and amending rule requiring policies and procedures reasonably designed to safeguard customer records and information (17 CFR 248.30(a), "Safeguards Rule") to require written policies and procedures); Final Model Privacy Form under the Gramm-Leach-Bliley Act, Release Nos. 34-61003, IA-2950, IC-28997 (November 16, 2009) (adding model privacy form and instructions in appendix).

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

[3] This Risk Alert does not discuss all requirements of Regulation S-P.

Privacy Notice"),[4] (2) provide a clear and conspicuous notice to its customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship ("Annual Privacy Notice,"[5] and together with the Initial Privacy Notice, "Privacy Notices"),[6] and (3) deliver a clear and conspicuous notice to its customers that accurately explains the right to opt out of some disclosures of non-public personal information about the customer to nonaffiliated third parties ("Opt-Out Notice").[7] Regulation S-P describes the information that must be included in Privacy Notices, including the categories of nonpublic personal information that the registrant collects and discloses, and in Opt-Out Notices.[8]

Written Safeguarding Policies and Procedures to Safeguard Customer Information

The Safeguards Rule of Regulation S-P requires registrants to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[9] These written policies and procedures must be reasonably designed to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of customer records and information, and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

II. Most Frequent Regulation S-P Compliance Issues

Below are examples of the most common deficiencies or weaknesses identified by OCIE staff in connection with the Safeguards Rule.

A. *Privacy and Opt-Out Notices.* OCIE staff observed registrants that did not provide Initial Privacy Notices, Annual Privacy Notices and Opt-Out Notices to their customers. When such notices were provided to customers, the notices did not accurately reflect firms' policies and procedures. The staff also noted Privacy Notices that did not provide notice

---

[4] 17 CFR 248.4. Regulation S-P defines "customer" to mean a consumer that has a customer relationship with a financial institution, and a "customer relationship" as a continuing relationship between a consumer and a financial institution and 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). As used in this Risk Alert, "customer" refers to brokerage customers and advisory clients as applicable.

[5] 17 CFR 248.5. Section 75001 of the Fixing America's Surface Transportation Act, Pub. L. No. 114-94, 129 Stat. 1312 (2016), ("FAST Act") amended the GLBA by adding subsection 503(f) to provide an exception to the Annual Privacy Notice requirement. Under this exception, a financial institution is not required to provide an Annual Privacy Notice if the financial institution (1) does not share nonpublic personal information about the customer except for certain purposes that do not trigger the customer's statutory right to opt out and (2) has not changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed in the most recent Privacy Notice.

[6] The SEC has adopted a model form to satisfy Privacy Notice disclosure requirements. Use of the form provides a "safe harbor" for the required disclosures under Regulation S-P. 17 CFR 248.2. *See also* Final Model Privacy Form under the Gramm-Leach-Bliley Act, *supra* note 1.

[7] 17 CFR 248.7. Under the exceptions in 17 CFR 248.13, 248.14 and 248.15, however, an Opt-Out Notice is not required if the registrant shares nonpublic personal information with a non-affiliated third party for certain purposes.

[8] 17 CFR 248.6, 248.7.

[9] 17 CFR 248.30(a).

to customers of their right to opt out of the registrant sharing their nonpublic personal information with nonaffiliated third parties.

B. *Lack of policies and procedures.* OCIE staff observed registrants that did not have written policies and procedures as required under the Safeguards Rule. For example, firms had documents that restated the Safeguards Rule but did not include policies and procedures related to administrative, technical, and physical safeguards. The staff observed written policies and procedures that contained numerous blank spaces designed to be filled in by registrants. There were also firms with policies that addressed the delivery and content of a Privacy Notice, but did not contain any written policies and procedures required by the Safeguards Rule.

C. *Policies not implemented or not reasonably designed to safeguard customer records and information.* OCIE staff observed registrants with written policies and procedures that did not appear implemented or reasonably designed to (1) ensure the security and confidentiality of customer records and information, (2) protect against anticipated threats or hazards to the security or integrity of customer records and information, and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to customers. For example, staff observed:

- Personal devices. Policies and procedures that did not appear reasonably designed to safeguard customer information on personal devices. For example, staff observed registrants' employees who regularly stored and maintained customer information on their personal laptops, but the registrants' policies and procedures did not address how these devices were to be properly configured to safeguard the customer information.

- Electronic communications. Policies and procedures that did not address the inclusion of customer personally identifiable information ("PII") in electronic communications. For example, staff observed registrants that did not appear to have policies and procedures reasonably designed to prevent employees from regularly sending unencrypted emails to customers containing PII.

- Training and monitoring. Policies and procedures that required customer information to be encrypted, password-protected, and transmitted using only registrant-approved methods were not reasonably designed because employees were not provided adequate training on these methods and the firm failed to monitor if the policies were being followed by employees.

- Unsecure networks. Policies and procedures that did not prohibit employees from sending customer PII to unsecure locations outside of the registrants' networks.

- Outside vendors. Registrants failed to follow their own policies and procedures regarding outside vendors. For example, staff observed registrants that failed to require outside vendors to contractually agree to keep customers' PII confidential, even though such agreements were mandated by the registrant's policies and procedures.

- PII inventory. Policies and procedures that did not identify all systems on which the registrant maintained customer PII. Without an inventory of all such systems, registrants may be unaware of the categories of customer PII that they maintain, which could limit their ability to adopt reasonably designed policies and procedures and adequately safeguard customer information.

- Incident response plans. Written incident response plans that did not address important areas, such as role assignments for implementing the plan, actions required to address a cybersecurity incident, and assessments of system vulnerabilities.[10]

- Unsecure physical locations. Customer PII that was stored in unsecure physical locations, such as in unlocked file cabinets in open offices.

- Login credentials. Customer login credentials that had been disseminated to more employees than permitted under firms' policies and procedures.

- Departed employees. Instances where former employees of firms retained access rights after their departure and therefore could access restricted customer information.

III. Conclusion

In response to these observations, many of the registrants modified their written policies and procedures to mitigate the issues identified by OCIE staff. OCIE encourages registrants to review their written policies and procedures, including implementation of those policies and procedures, to ensure that they are compliant with Regulation S-P.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.

[10] For a discussion of related cybersecurity compliance issues, please see the OCIE Risk Alert Observations from Cybersecurity Examinations, August 7, 2017.