Private Equity Alert

Weil

April 22, 2019

OCIE Issues Risk Alert Regarding Regulation S-P

By David Wohl

On April 16, 2019, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert wherein it provided a list of compliance issues related to Regulation S-P that it had identified in recent examinations of SEC-registered investment advisers[1] and broker-dealers.[2] Regulation S-P, among other things, requires that an investment adviser to a private fund provide (i) a notice to its "customers" (*i.e.*, investors[3]) that accurately reflects its privacy policies and practices generally no later than when the adviser establishes a business relationship with such investor (*i.e.*, when the investor makes a contractual commitment to a fund), and (ii) in certain cases, annual privacy notices thereafter.[4] In addition, the so-called "Safeguards Rule" of Regulation S-P requires advisers to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. 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.

Examples of common deficiencies or weaknesses found by OCIE examiners in connection with Regulation S-P are as follows:

1. **Privacy Notices -** Registrants did not provide initial or annual privacy notices as required, or provided notices that did not accurately reflect firms' policies and procedures or did not notify customers of their right to opt out of the registrant sharing their nonpublic personal information with nonaffiliated third parties.

2. **Lack of Policies and Procedures -** Registrants 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. 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.

3. **Policies Not Implemented or Properly Designed -** Registrants had written policies and procedures that did not appear implemented or reasonably designed to (i) ensure the security and confidentiality of customer records and information, (ii) protect against anticipated threats or hazards to the security or integrity of customer records and information, and (iii) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to customers. For example:

Personal devices. Policies and procedures that did not appear reasonably designed to safeguard customer information on personal devices. OCIE 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. OCIE 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. OCIE 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.

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.

****

In light of this Risk Alert, private fund advisers should review their written policies and procedures regarding Regulation S-P and the implementation thereof, as it is likely that such policies and procedures will be an area of focus for future OCIE examinations.

ENDNOTES

[1] Exempt reporting advisers are not subject to Regulation S-P.

[2] The Risk Alert can be found here.

[3] Regulation S-P only applies to nonpublic personal information of individuals (not entities) who obtain financial products or services primarily for personal, family or household purposes.

[4] An adviser is not required to provide an annual privacy notice if it (i) 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 of such sharing and (ii) has not changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed in its most recent privacy notice.

* * *

Private Equity Alert is published by the Private Equity practice group of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

The Private Equity group's practice includes the formation of private equity funds and the execution of domestic and cross-border acquisition and investment transactions. Our fund formation practice includes the representation of private equity fund sponsors in organizing a wide variety of private equity funds, including buyout, venture capital, distressed debt, and real estate opportunity funds, and the representation of large institutional investors making investments in those funds. Our transaction execution practice includes the representation of private equity fund sponsors and their portfolio companies in a broad range of transactions, including leveraged buyouts, merger and acquisition transactions, strategic investments, recapitalizations, minority equity investments, distressed investments, venture capital investments, and restructurings.

If you have questions concerning the contents of this issue, or would like more information about Weil's Private Equity practice group, please speak to your regular contact at Weil or to the author:

Author(s)

David Wohl (NY) View Bio david.wohl@weil.com +1 212 310 8933