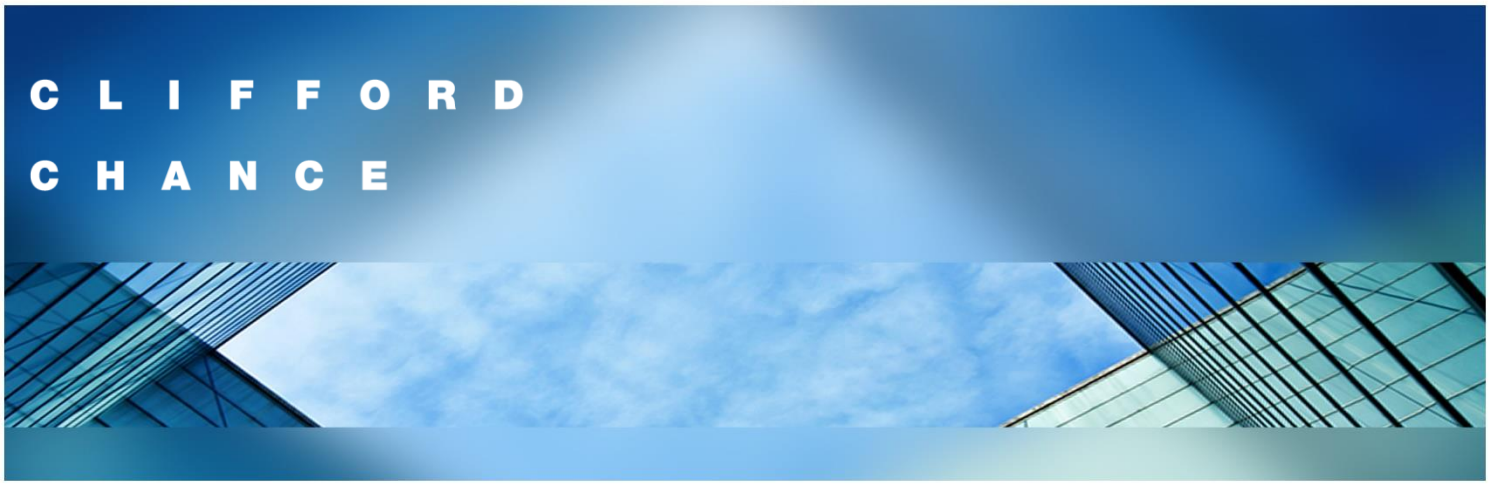

OCIE RISK ALERT HIGHLIGHTS KEY REGULATION S-P REQUIREMENTS FOR SEC REGISTERED ENTITIES

Last month, the US Securities & Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) released a risk alert highlighting the most common privacy-related issues that OCIE staff have observed in recent examinations of investment advisers and broker-dealers. Coupled with the recently-publicized cybersecurity sweep,[1] the risk alert is a timely reminder of the importance of instituting strong policies and procedures—and customer disclosures—that satisfy Regulation S-P, particularly those requirements highlighted by OCIE.

Background: OCIE & Regulation S-P

The Investment Advisers Act of 1940 (the "Advisers Act") requires all "investment advisers"[2] that manage more than $100 million in regulatory assets to register with the SEC, unless an exemption applies. SEC-registered advisers are subject to "periodic, special, or other examinations" by the SEC of their books and records "at any time" and "as the Commission…deems necessary…for the protection of investors."[3]

The SEC has increasingly dedicated significant resources to OCIE examinations while highlighting the importance of the examination program to the SEC's enforcement efforts. Between fiscal year 2013 and fiscal year 2018, OCIE almost doubled the percentage of investment advisers it examined, increasing the percentage from 9% to 17%.[4] For fiscal year 2019, the SEC has stressed that the

1 OCIE Deputy Director Kristin Snyder announced the sweep on March 19 at the Investment Company Institute's 2019 Mutual Funds and Investment Management Conference.

2 The Advisers Act defines an "investment adviser" as any person who, for compensation, provides advice to others or issues reports or analyses regarding securities. 15 U.S.C. § 80b-2(a)(11).

3 15 U.S.C. § 78q(b)(1).

4 U.S. Securities and Exchange Commission, *2019 Examination Priorities: Office of Compliance Inspections and Examinations* 1, 5 (2018), https://www.sec.gov/files/OCIE%202019%20Priorities.pdf.

examination schedule will have a particular "emphasis" on the almost 35 percent of advisers who have never been examined by OCIE.[5]

One of the issues that OCIE examines is compliance with Regulation S-P, a series of regulations enacted by the SEC in 2000 to implement the privacy provisions of the Gramm-Leach-Bliley Act (GLBA). Regulation S-P contains a variety of overlapping requirements for investment advisers. First, the "Safeguards Rule" requires that investment advisers adopt policies that are reasonably designed to safeguard customers' nonpublic personal information, protect that information against anticipated threats, and prevent unauthorized access and use of nonpublic material information that could result in significant harm to the customer. Second, Regulation S-P requires that investment advisers provide customers with a notice of their privacy policies and practices at the time the customer relationship is established and annually thereafter. Third, Regulation S-P prohibits registered entities from disclosing nonpublic personal information about a customer to nonaffiliated third parties under most circumstances unless the institution has informed customers about its proposed uses and provided the customer with the opportunity to opt out of such disclosure.

The OCIE Risk Alert: Most Frequent Regulation S-P Compliance Issues

OCIE's observations are not unexpected and focus on non-compliance issues that should be obvious to firms. These include:

- **Failures related to the provision and content of privacy notices**. Notices were criticized for not accurately reflecting the firms' policies and procedures or not providing notice of a customer's right to opt out of disclosure of their nonpublic personal information to nonaffiliated third parties.
- **Inadequate policies and procedures**. OCIE identified a number of issues with policies and procedures, including (i) lack of written policies and procedures; (ii) policies and procedures that were clearly deficient, (including policies that simply restated the Safeguards Rule); and (iii) policies with gaps, including "numerous blank spaces" that had not been filled in.
- **Inadequate employee training and monitoring**. The risk alert noted that employees should receive training on the firm's obligations to protect client data and that the firm must enforce its rules regarding client data.

The OCIE notice also described specific deficiencies that regulated entities should address in designing, documenting, implementing, and verifying their data privacy and retention policies and procedures, including:

- **Physical storage of customer data**. Customer data should be stored in locked file cabinets and buildings with access controls.

[5] U.S. Securities and Exchange Commission, *Fiscal Year 2019: Congressional Budget Justification Annual Performance Plan & Fiscal Year 2017 Annual Performance Report* 28 (2018), https://www.sec.gov/files/secfy19congbudgjust.pdf.

- **Storage of customer data on personal devices**. If customer data is stored on personal devices, those devices should be properly configured to safeguard the data (e.g., by requiring antivirus software).
- **Transmission of customer data in electronic communications**. Customer data transmitted in electronic communications should be encrypted.
- **Transmission of customer data on and to unsecure, external networks**. Customer data should not be transmitted to unsecure locations outside of the investment advisers' networks.
- **Customer data inventory**. All systems on which investment advisers maintain customer data should be inventoried and included in policies and procedures.
- **Incident response plans**. Written incident response plans should include clear role assignments for implementing a plan, key actions required to address a cybersecurity incident, and reassessment of system vulnerabilities following a breach.
- **Vendors**. Investment advisers should include contract provisions with vendors that require them to maintain the confidentiality of customer data.
- **Limiting Access**. Investment advisers should limit the number of customer login credentials provided to employees and ensure that those limits are maintained. They should also make sure to terminate access to customer data for departed employees.

Conclusions & Takeaways

OCIE's 2019 Examination Priorities released in December 2018 specifically listed cybersecurity as one of the six key risk areas on which it would focus its efforts.[6] The priorities, however, were light on detail—particularly for cybersecurity and data privacy. OCIE's recent notice puts more flesh on the bone, emphasizing the importance of Regulation S-P compliance and OCIE's areas of greatest interest.

Data privacy compliance is increasingly important, generating major SEC enforcement actions and fines exceeding $1 million. Data privacy compliance is also becoming increasingly complex, with overlapping state and federal requirements—such as the California Consumer Privacy Act and the FTC's Red Flags Rule—as well as non-US regulatory requirements that apply to many US companies, such as the General Data Protection Regulation. Finally, data privacy and cybersecurity are a differentiator, with customers migrating towards service providers who they trust to secure their information and assets. Investment advisers and other financial service providers are well-advised to revisit their data privacy policies, procedures, and customer disclosures to ensure compliance with applicable requirements, including Regulation S-P (and OCIE's focal areas) to drive their business forward.

6 U.S. Securities and Exchange Commission, *2019 Examination Priorities: Office of Compliance Inspections and Examinations* 5, 11 (2018), https://www.sec.gov/files/OCIE%202019%20Priorities.pdf.

CONTACTS

Steven Gatti
Partner

T +1 202 912 5095
E steven.gatti
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP