Proskauer

SEC Adopts Rule Amendments to Regulation S-P to Enhance Protection of Customer Information

May 24, 2024

On May 16, 2024, the U.S. Securities and Exchange Commission ("SEC") announced the adoption of amendments to Regulation S-P that were proposed last year ("Final Amendments").[1] The Final Amendments impose enhanced requirements on registered investment advisers, investment companies, broker dealers and transfer agents ("covered firms") with respect to handling of consumer financial information.

The Final Amendments principally focus on the responsibilities of covered firms with respect to data security incidents that impact customer non-public personal information ("customer information"). As amended, Reg S-P now requires:

- ***Incident Response Program***: Covered firms are now required to develop, implement and maintain written policies and procedures for an incident response program that is "reasonably designed to detect, respond to and recover from unauthorized access to or use of customer information." The program must include procedures to:
  - assess the nature and scope of an incident involving unauthorized access to or use of customer information;
  - identify the types of customer information that may have been subject to such unauthorized access or use;
  - take "appropriate steps" to contain and control the incident and to prevent further unauthorized access to or use of customer information; and
  - notify each affected individual whose "**sensitive** customer information"[2] was, or is reasonably likely to have been, accessed or used without authorization "*unless the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in* ***substantial harm or inconvenience***."[3]
  - ***Incident Notification***: Where a covered firm experiences a data security incident impacting sensitive customer information that is or is reasonably likely to be used in a manner that would result in substantial harm or inconvenience, the covered firm must notify affected individuals within **30**

days. The Final Amendments include prescriptive rules for what needs to be contained in incident notifications that covered firms should carefully review.

- The only exception to the 30 day notice requirement is a written notice from the U.S. Attorney General to the covered firm that the required notice poses a substantial risk to national security or public safety.

Notably, the Final Amendments do not include rules proposed in the draft amendments that would have imposed prescriptive requirements for written agreements with service providers with respect to data security and incident notification. However, the amended rules do impose requirements on covered firms to ensure they exercise thorough oversight and monitoring of service providers and implement policies and procedures to ensure service providers protect customer information and notify covered firms of a security breach impacting customer information within 72 hours of becoming aware of a breach — all requirements which, as a practical matter, will necessitate that service provider agreements have appropriate provisions around data security protections and breach response.

The amendments will become effective 60 days after publication in the Federal Register. Larger entities will have 18 months after the date of publication in the Federal Register to comply with the amendments, and smaller entities will have 24 months after the date of publication in the Federal Register to comply.

Please contact one of our Private Funds Group or Privacy & Cybersecurity partners for more information.

---

[1] Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, SEC Release Nos. 34-100155; IA-6604; IC-35193 (May 16, 2024. For a summary of the proposed amendments, see our previous Alert, *SEC Revisits Regulation S-P After Twenty Years of Innovation to Information Technology* (April 4, 2023).

[2] “sensitive customer information” is defined as “any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.” The final definition provides examples of sensitive customer information, including: (a) identification numbers such as SSNs, driver’s license and passport numbers and employer or taxpayer ID numbers; (b) biometric records; (c) unique electronic identification numbers, addresses or routing codes; (d) telecommunications identifying information or access devices that can be used to obtain money, goods or services or to initiate a transfer of funds and (e) customer account information in combination with account access information.

[3] The Final Amendments delete the draft amendments’ proposed definition of “substantial harm or inconvenience” which included a new standard not used in GLBA of “more than trivial” with various examples such as theft, fraud and physical harm. The final rule leaves “substantial harm or inconvenience” undefined consistent with GLBA.

Related Professionals

- **Robert H. Sutton**
  Partner