HIGHCAMP

Compliance at a Higher Elevation

SEC Adopts Cybersecurity Amendments to Enhance Protection of Customer Information

On May 16, 2024, the SEC **finalized** the adoption of cybersecurity amendments to Regulation S-P, aimed at expanding protections available to customers of institutional securities market participants, including registered investment advisors ("RIAs").[1] These new amendments establish a federal minimum standard for data breach notifications, requiring the implementation of an incident response program "reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information."

Outlined within the new regulations are specific protocols for incident response, including assessment, containment or control, and notifications. The rule requires an assessment of the nature and scope of the breach and identification of the customer information accessed or used without authorization. Next, appropriate steps must be taken to contain and control the incident from any further unauthorized access, and lastly, each affected individual whose sensitive information was, or is reasonably likely to have been, accessed or used without authorization must be notified. However, an RIA is not required to notify customers if sensitive information "has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience." Harm could also include any notification that would "pose a substantial risk to national security or public safety." The response procedures may be tailored to the individual facts and circumstances of each program.

Sensitive customer information encompasses personally identifiable information, such as Social Security Numbers or biometric identifiers, as well as any information enabling access to private customer accounts (i.e., K1s, capital statements, subscription agreements). Affected individuals may have an existing customer relationship with the RIA managing the private fund, or they may be clients of other financial institutions where such information has been disclosed. Accordingly, RIA's must notify affected individuals even if there is no customer relationship. The Safeguards and Disposal Rules now extend to customer information from third-party financial institutions and terminated customer relationships. This expanded definition of "customer" must be considered when adhering to the new notification requirements.

Within 30 days of becoming aware of the unauthorized access or use of customer information, RIAs must issue individual notices. These may be transmitted by any means designed to ensure that each affected individual can "reasonably be expected to receive actual notice in writing." The notifications should include the nature and date of the incident, the data involved, and multiple means for the affected individuals to contact the RIA. In cases where specific individuals cannot

[1] *Institutional securities market participants, as defined in the **Securities Exchange Act of 1934**, encompass broker-dealers, investment companies, registered investment advisors, funding portals, transfer agents, or other appropriate regulatory authorities.*

be identified, a general notification must be issued to all individuals whose customer information is stored in the breached customer information system.

Stringent oversight by service providers is necessary to ensure compliance with these standards, necessitating thorough due diligence, robust processes, and continuous monitoring of RIAs. Under the amendments RIAs should have reasonably designed policies and procedures in place to ensure their respective service providers are equipped to protect the RIA against unauthorized access and, in the event of an incident, notify the RIA no later than 72 hours after becoming aware that an incident has occurred.

To sustain compliance under the adopted amendments, adhere to existing best practices, maintain written policies for incident management, document unauthorized access, report findings, and monitor customer notifications. Ensure oversight of service providers and protocols for your respective incident response plan. Associated costs may present themselves while implementing and upholding these new cybersecurity measures.

The amendments go on to conform Regulation S-P to certain aspects of the FAST Act passed by Congress in 2015 which exempts RIAs from providing the privacy policy notice annually as originally required by the rule. RIAs are eligible for the exception if (1) the RIA only provides non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies and (2) the RIA has not changed its policies or practices from its most recent privacy notice disclosures.

The effective date for the amended rules begins 60 days after publication in the Federal Register. Larger RIAs, with $1.5 billion or more in AUM, have 18 months to comply. Smaller entities, comprising RIAs with less than $1.5 billion AUM, have 24 months to comply.[2]

In the eyes of regulators, the SEC's adoption of these cybersecurity amendments to Regulation S-P is viewed as a pivotal move in bolstering the safeguarding of sensitive customer information within the securities market. Through the establishment of a federal minimum standard, these amendments are perceived to effectively reduce the risks linked with unauthorized access to information and/or accounts.

About HighCamp Compliance

HighCamp is a boutique compliance consulting and outsourcing firm helmed by former SEC examiners, CCOs and proven consulting professionals. The firm specializes in regulatory compliance and operational support for SEC-registered private equity, real estate, venture capital, hedge fund, and institutional alternative managers. HighCamp is 100-percent employee owned, with a gender-balanced leadership team. The company has locations in New York City (Metro), Los Angeles, Denver, Dallas, Milwaukee and Bozeman.

[2] ***RIN 3235-AN26.* P.129**