LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Investment Funds and Privacy & Cyber Practices August 8, 2024 | Number 3285

SEC Imposes New Cybersecurity Requirements on Broker-Dealers, Investment Companies, Registered Investment Advisers, and Transfer Agents

Covered institutions will need to review their cybersecurity and incident response policies and procedures ahead of the applicable compliance deadline.

The Securities and Exchange Commission (SEC) recently[1] adopted amendments to Regulation S-P that expand the scope of requirements applicable to brokers, dealers, investment companies, SEC-registered investment advisers, and foreign (non-resident) SEC-registered brokers, dealers, investment companies, and investment advisers (together, Covered Institutions) in order to:

- bolster the protection of nonpublic personal information;
- help ensure that customers receive timely notification in the event of a security incident (this will likely result in many more notifications than required under existing US state data breach notification laws); and
- modernize the requirements of Regulation S-P (the Amendments).

The Amendments also expand the scope of Regulation S-P to extend a number of requirements to transfer agents.[2]

Compliance with the new rules will require:

- enhanced programs, policies, and procedures for protecting against and swiftly responding to cyber incidents;
- customer notification requirements;
- proactively supervising vendors and service providers; and
- properly disposing of customer and consumer information.

This Client Alert analyses the new rules and compliance dates in detail, and provides practical guidance to Covered Institutions for implementation.

Overview

In general, the Amendments supplement Regulation S-P's existing obligations regarding privacy notices, security policies, and proper disposal of consumer report information, and include key obligations on Covered Institutions with regard to:

A. **Incident Response Process.** Covered Institutions should respond appropriately to incidents that involve any unauthorized access to or use of customer information (defined broadly), including following certain response procedures established by the Amendments, undertaking a reasonable investigation of the facts and circumstances (including identifying the information systems and types of customer information that may have been compromised) and taking appropriate steps to contain and control the incident.

B. **Incident Response Program.** Covered Institutions should establish, maintain, and enforce an incident response program, including procedures for:

   (i) notifying affected individuals;

   (ii) oversight of service providers; and

   (iii) disposal of customer and consumer information in a manner that protects against unauthorized access to or use of such information,

C. **Notice to Affected Individuals.** Covered Institutions should notify affected individuals as soon as reasonably practicable, but no later than 30 days, after becoming aware of the unauthorized access to or use of customer information, unless a Covered Institution determines, after a reasonable investigation of the facts and circumstances of the incident, that: (i) sensitive customer information has not been compromised, and (ii) the information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.

D. **Record Keeping.** Covered Institutions should maintain certain written records related to the requirements imposed by the Amendments.

Background

Regulation S-P is a set of rules adopted in 2000 pursuant to the Gramm-Leach-Bliley Act (GLBA) and the Fair and Accurate Credit Transactions Act (FACT Act). It imposes certain obligations on Covered Institutions and governs the treatment of nonpublic personal information about consumers by such financial institutions. Prior to the Amendments, Regulation S-P has historically not specifically required Covered Institutions to have policies or procedures for responding to security incidents, nor has it required notification of data breaches to affected individuals.

Regulation S-P has historically imposed obligations on Covered Institutions (though with certain exceptions, such as in relation to transfer agents) under the following rules:

- "Safeguards Rule," namely to adopt written policies and procedures for administrative, technical, and physical safeguards to protect customer records and information

- "Privacy Rule," namely in relation to the treatment of nonpublic personal information about consumers

- "Disposal Rule," namely to properly dispose of consumer report information[3]

However, the risks of cyberattacks and unauthorized access to or use of information has increased significantly since 2000, which has resulted in many agencies, including the SEC, revisiting their approach to data security and protection.

The Amendments follow the SEC's new public company cybersecurity rules, which were finalized last year (see Latham's blog post) and were designed to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents.

However, while the public company cybersecurity rules are designed to benefit and protect investors, registrants, and other market participants (including to facilitate investor decision-making and reduce information asymmetry in the market), the Amendments are designed to protect investors and investor information to help ensure that investors receive timely and consistent notification in the event of unauthorized access to or use of their information, and to enable affected individuals to take steps to protect themselves as needed.

Thus, the Amendments represent a significant expansion of the protections afforded to customers of nonpublic companies and establish a new nationwide minimum standard for notifying investors affected by a security incident or data breach.

Written Policies and Procedures

The Amendments will require Covered Institutions to adopt policies and procedures to detect, respond to, and recover from an incident. Such policies and procedures should address incidents implicating "customer information," which is broader than "sensitive customer information" and generally includes any record, in any form, containing nonpublic personal information about a customer. In addition to establishing procedures to address the delivery of notices to affected individuals, the Amendments require Covered Institutions to adopt and implement procedures to:

- assess the nature and scope of an incident involving unauthorized access to or use of customer information;
- identify customer information systems and types of customer information accessed or used during the incident;
- take appropriate steps to contain and control an incident;
- notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization (unless, after a reasonable investigation, the Covered Institution determines that 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); and
- oversee, monitor, and perform due diligence with respect to service providers,[4] including to ensure that service providers take appropriate measures to: (i) protect against unauthorized access to or use of customer information, and (ii) provide notification to the Covered Institution within 72 hours of becoming aware of an incident.

The Amendments do not prescribe specific steps that a Covered Institution must undertake when carrying out incident-response activities, and instead provide flexibility so that a Covered Institution can create policies and procedures best suited to its particular circumstances (including size, sophistication, and the nature and scope of the activities and information it handles).

Service Provider Oversight

Under the Amendments, a Covered Institution's written policies and procedures must be reasonably designed to ensure that service providers take appropriate measures to protect against unauthorized access to or use of customer information and provide notification to the Covered Institution as soon as possible, but no later than 72 hours after becoming aware, that a breach in security has occurred resulting in unauthorized access to an information system maintained by the service provider.

The SEC considered numerous comments on this requirement, including the scope of incidents that service providers ought to notify a Covered Institution of, and rejected proposals to narrow the scope of reportable incidents to only breaches in security that result in unauthorized access to sensitive customer information held by a service provider, or alternatively only breaches that result in unauthorized access to customer information.

While ultimately the SEC decided not to require a Covered Institution to enter into a written contract with its service providers that imposes specific contractual requirements (in order to not burden smaller Covered Institutions with minimal resources), a Covered Institution may in practice contractually require service providers to implement certain security safeguards and to comply with breach notification obligations, so that the Covered Institution satisfies applicable legal requirements under Regulation S-P. Other privacy laws in the United States, such as the California Consumer Privacy Act (CCPA) and similar comprehensive state privacy laws, already impose similar requirements on covered businesses, although some of these laws do not apply to businesses or data subject to the GLBA or Regulation S-P.

Perhaps more importantly, Covered Institutions will need to devote time and resources to oversee their service providers throughout the relationship, and account for instances where the service provider failed to provide notice within 72 hours as required. The SEC's commentary is clear that Covered Institutions retain the obligation to ensure that affected individuals are notified in accordance with the Amendments, and cannot shift liability to their service providers for failure to notify them in time. Therefore, in addition to initiating its own incident-response program upon receipt of notice from a service provider, the Covered Institution should also reevaluate its policies and procedures governing its relationship with the service provider and adjust as necessary.

Finally, Covered Institutions may, as part of their incident-response program, contractually allow or require their service provider to notify affected individuals on the Covered Institution's behalf. However, because the Covered Institution remains responsible for ensuring that the Amendments' requirements regarding notification are met, Covered Institutions that take this step must have procedures in place to ensure that the service provider satisfies all customer notification obligations. In addition to maintaining a copy of any notice transmitted to affected customers (as required by the recordkeeping obligations under the Amendments, discussed below), Covered Institutions should consider whether it would be beneficial to take additional steps, such as:

- conducting timely due diligence to confirm that notification has been provided;
- requiring close coordination on the content of the notices, and method and timing of delivery;

- obtaining confirmation of delivery of notifications in the form of attestations or certifications made by the service provider;

- confirming with a sample of customers that they received notice from the service provider;

- establishing procedures designed to remedy non-compliances in advance of the required deadline; and

- implementing relevant contractual protections (e.g., indemnification).

Notice to Affected Individuals

The Amendments establish a presumption of notification, and Covered Institutions must (as soon as practicable, but no later than 30 days after becoming aware that unauthorized access to or use of any customer information has or is reasonably likely to have occurred) notify individuals whose "sensitive customer information" was, or is reasonably likely to have been, accessed or used without authorization, *unless* the Covered Institution determines upon reasonable investigation that such 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 to the affected individual. Given that data breaches can harm or inconvenience individuals in a wide variety of ways (described further below), and given the SEC's focus on cybersecurity to date, this presumption of notification may create significant enforcement risk for Covered Institutions that choose not to notify affected individuals.

Scope of Information Covered

Under the Amendments, "sensitive customer information" is defined broadly 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."[5] The SEC notes that this definition covers information that wouldn't otherwise trigger a notification under existing laws, and provides examples of sensitive customer information, including:

- Social Security number, official government-issued driver's license or identification number, alien registration number, passport number, employer or taxpayer identification number, biometric record, unique electronic identification number/address/routing code, telecommunication identifying information or access device, or other identifying information that can reasonably be used alone to authenticate an individual's identity; and

- customer information identifying an individual or individual's account (including account number, name, or online user name) in combination with authentication information or similar information that could be used to gain access to the account (e.g., access code, credit card expiration date, partial Social Security number, security code, security question and answer identified with the individual or their account, or the individual's date of birth, place of birth, or mother's maiden name).

Timely Investigation Required

According to the SEC, the Amendments establish a rebuttable presumption of providing notice to affected individuals, *unless* the Covered Institution determines, after a reasonable investigation, that notice is not required. Notice can only be avoided if the Covered Institution determines upon reasonable investigation that 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 to the affected individual. While "substantial harm

or inconvenience" is a facts-and-circumstances inquiry, the SEC has emphasized that a data breach can injure a customer in a wide variety of ways, and harm or inconvenience could include, for example, personal injury, financial loss, expenditure of effort, loss of time, theft, fraud, harassment, physical harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the misuse of information to obtain a financial product or service or otherwise misuse an individual's account.

In addition, the notice requirement applies with respect to individuals who are direct customers of the Covered Institution and to individuals who are customers of other financial institutions where the individual's sensitive customer information was provided by such financial institution to the Covered Institution, and encompasses information maintained directly by the Covered Institution and information maintained at such Covered Institution's service providers that are not themselves Covered Institutions.

The Amendments also make clear that where the Covered Institution is unable to identify the specific individuals whose information is affected, the Covered Institution is required to provide notice to all potentially affected individuals whose sensitive customer information resides in the relevant customer information system.

Timing of Notice

Notice to affected individuals must be delivered as soon as practicable, but no later than 30 days after becoming aware that unauthorized access to or use of any customer information — a much broader concept than sensitive customer information — has or is reasonably likely to have occurred. It is not necessary that the Covered Institution be aware that the sensitive information has been compromised. Crucially, the 30-day timeline starts as soon as a Covered Institution becomes aware that there has been, or is reasonably likely to have been, unauthorized access to or use of any customer information, meaning that Covered Institutions will need to have clear processes in place prior to the incident to enable it to gather the relevant information needed in that timeframe.

In its comments, the SEC seemed unmoved by commenters suggesting that the notice requirements may pose logistical challenges, and specifically noted that Covered Institutions need to anticipate and prepare for the possibility that they may be denied access to a particular system, such as in the event of a ransomware attack, and have procedures in place for complying with the notice requirements in such circumstances.

In addition, if the incident has impacted a Covered Institution's service provider, the 30-day timeline starts as soon as the Covered Institution becomes aware of the incident, meaning that Covered Institutions need to be ready to carry out their incident-response program at any time, and have processes in place to enable close oversight of, and collaboration with, service providers.

Notwithstanding this timing requirement, the US Attorney General is authorized to effect a series of delays to the delivery of the required notice pursuant to an intra-governmental process whereby the US Attorney General provides written notice to the SEC that it has determined that a notice to an affected individual poses a substantial risk to national security or public safety. By broadening this exception to apply to risks to public safety (and not merely national security risks), the exception now covers additional risks such as alerting malicious actors targeting critical infrastructure that their activities have been discovered.

While the Amendments do not permit other government agencies to trigger a delay, other agencies are permitted to request that the US Attorney General determine whether disclosures pose a substantial risk to national security or public safety and communicate that determination to the SEC. In light of this, we

may see the US Attorney General or other agencies issue guidance on how to request delays (similar to guidance issued by the FBI in coordination with the Department of Justice on how to request disclosure delays in connection with the SEC's public company cybersecurity rules).

Content of Notice

Under the Amendments, notice to affected individuals must include a number of specific elements, including:

- a general description of the incident;
- the type of sensitive customer information that was or is reasonably likely to have been accessed or used without authorization;
- the date, estimated date, or range of dates of the incident (as applicable);
- contact information of the Covered Institution for inquiries concerning the incident, including a phone number (toll-free if available), an email address or equivalent method or means, a postal address, and the name of a specific office or contact;
- for an affected individual with an account at the Covered Institution, a recommendation to review account statements and immediately report suspicious activity;
- an explanation of fraud alerts and how the affected individual can include a fraud alert in their credit reports;
- a recommendation that the affected individual periodically obtains credit reports and that the individual has information relating to fraudulent transactions deleted from such reports;
- an explanation as to how the affected individual can obtain a free credit report; and
- statements on the availability of certain public information concerning steps to protect against identity theft and to encourage the affected individual to report incidents of identity theft to the Federal Trade Commission.

Covered institutions that operate nationally may already include many of these required elements in their existing notification processes and procedures. Yet, given that the content of notices differs on a state-by-state basis, Covered Institutions that take a state-by-state approach may need to update their notification processes, procedures, and templates to ensure alignment across federal and state (and potentially international) laws. Helpfully, unless otherwise required under state law, the Amendments do not require a particular method of delivery (e.g., first-class mail) or a particular form of the notice.

Recordkeeping

Amended Regulation S-P includes a number of recordkeeping requirements related to other provisions of the Amendments, including to maintain written records of: (i) adopted policies and procedures required under the Amendments, (ii) unauthorized access to or use of customer information, and the Covered Institution's response to, and recovery from such unauthorized access, (iii) investigations and determinations made regarding whether the Covered Institution is required to provide notice to an affected individual, (iv) documentation from the US Attorney General in connection with the delay of notice to an affected individual, (v) each notice provided to an affected individual, and (vi) any agreement

with a service provider that has access to customer information.[6] The duration that such records must be maintained varies depending on the type of Covered Institution, the type of record, and the specific facts and circumstances, but generally ranges from three to six years after the occurrence of certain events. In certain cases, such records must be maintained for a period of time in an easily accessible place.

Other Key Amendments

The Amendments also:

- Expand the Safeguards and Disposal Rules to cover not only nonpublic personal information that the Covered Institution collects about its own customers, but also nonpublic personal information it receives from another financial institution about customers of that separate financial institution.

- Extend the applicability of the Safeguards Rule to cover transfer agents registered with the SEC or another appropriate regulatory agency, and define "customer" with respect to transfer agents to include individuals who are securityholders of an issuer that has engaged the transfer agent.

- Impose obligations on Covered Institutions (other than notice-registered broker-dealers) to adopt and implement written policies and procedures that address proper disposal of customer and consumer information as to protect against unauthorized access to or use of such information. Consumer information generally includes consumer reports, records derived from consumer reports, or a compilation of such records.

- Incorporate an existing statutory exception to the requirement to deliver an annual privacy notice to customers. Under the Amendments, broker-dealers, investment companies, and registered investment advisers can forgo providing notice if these Covered Institutions have not changed their policies and practices in relation to the disclosure of nonpublic personal information since their last privacy notice and such Covered Institutions do not disclose nonpublic personal information in a way that requires them to provide individuals the ability to opt out.

Compliance Dates

The deadline for compliance with the Amendments is June 3, 2026, for small Covered Institutions and December 3, 2025, for large covered entities. Large covered entities include:

- investment companies that together with related investment companies have net assets of $1 billion or more as of the end of the most recent fiscal year;

- registered investment advisers with $1.5 billion or more in assets under management; and

- all broker-dealers and transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.

Conclusion

Regulation S-P, as amended, is likely to increase the compliance burden on broker-dealers, investment companies, investment advisers, and transfer agents — particularly transfer agents who are not currently subject to the majority of Regulation S-P. Such Covered Institutions will need to review and revise their policies and procedures (including cybersecurity and incident-response policies and procedures) or implement new policies and procedures to the extent these do not already exist, including implementing appropriate customer notification procedures. Covered institutions should also assess their safeguards

and controls, train employees, assess their use of service providers, and consider implementing a vendor management program to enable them to address the new requirements ahead of the applicable compliance deadline.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Robert Blamires
robert.blamires@lw.com
+1.415.395.8142
San Francisco

Laura Ferrell
laura.ferrell@lw.com
+1.312.876.7616
Chicago

Daniel Filstrup
daniel.filstrup@lw.com
+1.312.876.6511
Chicago

Jennifer Howes
jennifer.howes@lw.com
+1.858.523.5400
San Diego / San Francisco

Sarah Zahedi
sarah.zahedi@lw.com
+1.415.395.8069
San Francisco

You Might Also Be Interested In

SEC and FinCEN's Proposed AML Rule Could Increase Compliance Burden on Investment Advisers

Key Takeaways From SEC's First "Off-Channel Communications" Settlement With Stand-Alone Registered Investment Adviser

SEC Announces First-Ever Enforcement Actions for "AI Washing"

Endnotes

[1] On May 16, 2024.

[2] Historically, only transfer agents registered with the SEC were subject to Regulation S-P's "disposal rule," and not its "safeguards rule" or "privacy rule." The Amendments extend both the disposal rule and the safeguards rule to all transfer agents, even if the transfer agent is registered with another appropriate regulatory agency. The Amendments also introduce a new definition of "customer" with respect to transfer agents to account for the fact that transfer agents' clients generally are the issuers whose securities are held by investors, not the individual investors themselves.

[3] Under Regulation Crowdfunding, funding portals are required to comply with the requirements of Regulation S-P as they apply to brokers, and funding portals will therefore also need to comply with the amendments to Regulation S-P.

[4] "Service provider" is broadly defined to include "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a Covered Institution."

[5] The SEC acknowledged that it has intentionally defined "sensitive customer information" in a manner that is broader than many state data breach notification laws and the 2005 guidance issued by the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the former Office of Thrift Supervision, and the National Credit Union Administration: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 FR 15736 (Mar. 29, 2005).

[6] Note that the recordkeeping requirements established by the Amendments do not apply to funding portals, which are subject to other recordkeeping requirements under amended Regulation S-P.