Cybersecurity Law Report cslawreport.com

Jul. 24, 2024

SEC Enforcement

What Regulated Companies Need to Know About the SEC's Final Amendments to Regulation S-P

By Richard Borden and Andrew Folks, *Frankfurt Kurnit Klein & Selz*

As the SEC continues its focusing on federal financial privacy and cybersecurity regulation, on May 16, 2024, the agency adopted final amendments to Regulation S-P (Final Amendments). Regulation S-P is a set of privacy and security rules adopted pursuant to the Gramm-Leach-Bliley Act (GLBA) and the Fair and Accurate Transactions Act of 2003 (FACTA) that govern the handling of "nonpublic personal information" (NPI) about consumers by broker-dealers, investment companies, registered investment advisers, funding portals and transfer agents.

As Regulation S-P has not been updated since its initial adoption in 2000, in drafting the Final Amendments, the SEC was determined to account for many 21st-century technological advancements, and the complex privacy and cybersecurity regimes that have developed in their wake. The updates aim to strengthen data protection and enhance cybersecurity practices within the financial services sector and will significantly impact covered institutions' cybersecurity practices in a climate of data breaches that increase in frequency year over year.

Although the SEC has been busy regulating privacy and cybersecurity practices of institutions within its jurisdiction, it still has not finalized multiple proposed rules in this area. To date, the Final Amendments represent the greatest existing sea change in the SEC's regulation of cybersecurity by, among other significant updates, prescribing a novel incident response and notification regime that demands covered institutions thoroughly reconfigure current policies and procedures.

This article examines the Final Amendments' key requirements and offers practical compliance steps.

See "Key Implications and Practical Cyber Program Lessons From SEC's R.R. Donnelley Settlement" (Jul. 10, 2024).

Broader Reach With New Customer Information Definition

The Final Amendments work to homogenize the GLBA's Safeguards Rule and FACTA's Disposal Rule by applying the protections of both rules to "customer information," a new term that combines and replaces the Safeguards Rule's "customer records and information" and the Disposal Rule's "customer report information."

See "Fund Managers Must Ensure Adequate Security Measures Under Safeguards Rule or Risk SEC Enforcement Action" (Oct. 6, 2021).

Inclusion of Information Regardless of Relationship

"Customer information" is any record about a customer of a financial institution containing NPI, or personally identifiable financial information, or any list, description or other grouping of consumers derived using any personally identifiable financial information that is not publicly available. This change broadens the scope of information covered by the rules to all customer information, independent of the covered institution's relationship with that customer.

Information Tied to Risk of Harm

The Final Amendments also define "sensitive customer information" 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." Listed examples include a customer's Social Security and other identification numbers, biometric records, address, routing code, or unique device or telecommunication identifying information.

The SEC added this definition in order to require notification to individuals for breaches as described below. Not all incidents that include NPI will require notifications to the affected individuals. This means, however, that covered financial institutions need to have the ability to track the locations where "sensitive customer information" is stored, including with service providers.

What If a Business Does Not Collect Customer Information?

If a financial institution does not collect customer information, certain obligations will not apply and complying with others will be less complex, but the institution will not be relieved from Regulation S-P obligations. These institutions – often investment companies or transfer agents – may still have access to NPI about their investors or other institutions' customers that qualifies as customer information under the revised definition found in the Final Amendments, and thus will be subject to the enhanced requirements.

If an entity handles customer information that it has received from another institution, it may qualify as a service provider and would be subject to that covered institution's policies and procedures,

as well as the 72-hour deadline for notification of breach, discussed below. If the entity does not qualify as a service provider, however, it would be considered a third party and be subject to Regulation S-P obligations as if it collected the information directly from the customer.

Entities that do not handle any customer information will of course not be subject to the Final Amendments, but under this expanded universe of customer information, those entities will be fewer and further between.

New Written Incident Response Program Requirements

Program Mandates

The Final Amendments require covered institutions to develop and implement a written incident response and notification policy and procedure reasonably designed to detect, respond to and recover from unauthorized access to – or use of – customer information. The mandated response program must include procedures to assess the nature and scope of any incident and take appropriate steps to contain and control the incident to prevent further unauthorized use.

Practical Tips for Response Programs

The SEC does not detail in the Final Amendments what exactly an institution must include in its response program, but it has provided further detail in other proposed, but not final, rulemaking applicable to certain institution types, such as the proposed Outsourcing by Investment Advisers or Cybersecurity Risk Management (made up of three rule proposals: one, two and three) packages.

In the Outsourcing by Investment Adviser proposal, the SEC includes parties such as nationally chartered banks, broker-dealers, stock exchanges and self-regulatory organizations in scope. As discussed below, the service provider oversight requirements likely apply to these and similar entities. The Cybersecurity Risk Management packages have a significant focus on disaster recovery and business continuity programs, including those of service providers. Even without finalization of those packages, it is likely that the SEC will apply the concepts to the substantive requirements for policies and procedures under the Final Amendments. Financial institutions should consider this in the revision of their cybersecurity and incident response policies and procedures.

Tight Notification Deadline With Harm Standard

Covered institutions must timely notify individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization at the financial institution or a service provider.

Harm Standard

Notice will not be required where a covered institution determines after reasonable investigation that sensitive customer information has not been, and is not reasonably likely to be, used in a way that would result in substantial harm or inconvenience. While the SEC does not elaborate upon what may satisfy this harm standard, certain security controls, such as encryption, could militate against a finding of harm considering the presence of similar safe harbors under comparable state data breach notification laws.

Thirty-Day Notification Requirement

Should a covered institution suffer a data breach that meets the risk-of-harm standard, it must provide notice to affected individuals as soon as reasonably practicable but not later than 30 days after the covered institution becomes aware that an incident has occurred. This timeline is considerably shorter than those under state data breach notification laws, which either do not mandate a specific deadline for notification or peg the 30-,45- or 60-day notification trigger to the conclusion of the investigation of an incident, rather than when an entity becomes aware of it.

To conduct an investigation within 30 days after becoming aware of an incident is no small task and will present a covered institution with considerable challenges in understanding the scope of a breach before it must provide notice to affected individuals. The SEC reasoned that a specific notification deadline of 30 days satisfies "the goal of providing customers . . . with early and consistent notification of data breaches so that they may take remedial action," noting that "30 days should be sufficient to conduct an initial assessment and notify affected individuals."

The Final Amendments do little to ameliorate the logistical concerns of such a hurried data breach response, offering solace only to the extent that a covered institution need not "describe what has been done to protect the sensitive customer information from further unauthorized access or use." All other requirements typical of data breach notification remain in effect.

Covered institutions may extend this deadline another 30 days in the limited instance when the U.S. AG determines and notifies the SEC in writing that the notice would pose a substantial risk to national security or public safety. In adding public safety as a reason for delay, the Final Amendments expand what was previously referred to as the "law enforcement exception" and give moderately more leeway for entities to delay notification, albeit still coming at the sole discretion of the AG.

In a data breach with a large number of affected individuals, it will be difficult, and may be impossible, to meet the 30-day notification period. Notifications are usually made in batches, after combining multiple consumer records and confirming current addresses. This, in and of itself, often takes weeks. Meeting this new requirement requires significantly different incident response plans.

Practical Tips on Notification

All financial institutions should tighten up their policies and procedures for notification. This means having lawyers and forensic investigators on retainer who are trained on the company and its systems. For financial institutions with large numbers of consumer records, this is even more urgent. Tabletop exercises of the incident response, with a specific focus on a ransomware deployment within the company and at key service providers, should be done at least yearly.

The SEC expects senior management and the board to be involved in cybersecurity oversight. An enterprise risk management approach to cybersecurity and incident response can be followed to satisfy those expectations. Setting up committee structures with policies and procedures that are tested for effectiveness is likely to satisfy regulatory and other auditors.

See "Navigating the SEC's Newly Adopted Cybersecurity Disclosure and Controls Regime" (Sep. 6, 2023).

Service Provider Oversight

Pursuant to the Final Amendments, Regulation S-P now defines a service provider as "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."

Onus on Covered Institutions

The Final Amendments do not require covered institutions to enter into a written contract with their service providers. Instead, they put the onus on covered institutions to enact policies and procedures reasonably designed to ensure that service providers protect against unauthorized access or use of customer information and notification to the covered institution should that access or use occur.

The Final Amendments' approach to service provider relationships differs from relevant provisions within the CCPA as amended by the California Privacy Rights and Enforcement Act of 2020 and similar state laws, which govern such relationships primarily through statutorily mandated contractual provisions. The SEC's approach more closely resembles the New York Department of Financial Services Cybersecurity Regulation, which requires a covered entity to implement written policies and procedures to ensure service provider compliance.

Many large service providers, including entities that are regulated by the SEC and the Federal Reserve, do not negotiate their agreements, and likely do not have language sufficient to allow covered institutions to comply with the Final Amendments.

Under the Final Amendments, a covered institution's obligations in the event of a cybersecurity incident that happens to a service provider will be the same as if the incident occurred on the covered institution itself, and the covered institution must account for that through its own

cybersecurity program. The Final Amendments require the covered financial institution to ensure that it is notified of applicable data breaches by a service provider as soon as possible but no later than 72 hours after becoming aware of it. This aligns with reporting requirements for entities that are part of critical infrastructure.

Practical Tips on Service Provider Contracts

Every covered financial institution should review its service provider contracts, including those of entities that it might otherwise exclude from detailed oversight (banks, broker-dealers, clearing companies, trust companies, SROs, etc.) to see if there are contractual provisions that allow the company to meet the Final Amendments' requirements. Where the contractual provisions do not exist, try to negotiate them and, barring that, document any discussions or other materials where the covered financial institution draws the conclusion that it will receive appropriate notification.

See "Considerations for Managing Third-Party Cyber Risks" (Oct. 4, 2023).

Recordkeeping Requirements

The Final Amendments enhance several requirements for a covered institution to make and maintain written records documenting compliance with the Safeguards Rule and Disposal Rule, including with respect to its incident response program.

Incident Response Documentation

Covered institutions must, among other things, further document in writing:

- any detected unauthorized access to or use of customer information;
- the institution's response to any such unauthorized access or use;
- any investigation and determination on whether customer notification is required or delayed; and
- policies and procedures, and contracts entered into, for service provider oversight.

Retention Requirements

Document retention requirements depend on entity type, ranging from three years for transfer agents to six years for investment companies.

Covered Institution	Rule	Retention Period
Registered Investment Companies	17 CFR 270.31a-1(b) 17 CFR 270.31a-2(a)	*Policies and Procedures*: A copy of policies and procedures in effect, or that at any time in the past six years were in effect, in an easily accessible place. *Other records*: Six years, the first two in an easily accessible place.
Unregistered Investment Companies	17 CFR 248.30(c)	*Policies and Procedures*: A copy of policies and procedures in effect, or that at any time in the past six years were in effect, in an easily accessible place. *Other records*: Six years, the first two in an easily accessible place.
Registered Investment Advisers	17 CFR 275.204-2(a)	All records for five years, the first two in an easily accessible place.
Broker-Dealers	17 CFR 240.17a-4(e)	All records for three years, in an easily accessible place.
Transfer Agents	17 CFR 240.17ad-7(k)	All records for three years, in an easily accessible place.

Following these retention periods, a covered institution must dispose of consumer and customer information, following its written policies and procedures crafted in compliance with the updated Disposal Rule.

Practical Tips on Recordkeeping

Covered institutions should review their records of compliance with the Safeguards and Disposal Rules, as well as those created and maintained as required by other regulators, such as FINRA, the Federal Reserve and the Commodity Futures Trading Commission, prior to the effective date of the Final Amendments. If a covered institution does not have a clear records retention and destruction policy that documents cybersecurity and incident response records, it should draft one.

Covered institutions should also plan for audits (whether internal or external) in advance. They should prepare compliance documentation as if someone will audit it, and aim to make the auditor's

job easier. That will make the auditor think more highly of the organization and its compliance function.

See "SEC and CFTC Continue to Penalize Firms for Electronic Communications Recordkeeping Violations" (Sep. 20, 2023).

Compliance Deadlines

Larger entities will have until December 21, 2025 – 18 months following the date of publication in the Federal Register on June 21, 2024 – to comply with the Final Amendments. Smaller entities will have an additional six months, until June 21, 2026. As set forth in the chart below, larger entities are those that meet monetary thresholds or fall under statutory designations, while smaller entities are all others.

Entity	**Qualification to Be Considered a "Large Entity"**
Investment Companies Together With Other Investment Companies in the Same Group of Related Investment Companies	Net assets of $1 billion or more as of the end of the most recent fiscal year.
Registered Investment Advisers	$1.5 billion or more in assets under management.
Broker-Dealers	All broker-dealers that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.
Transfer Agents	All transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.

Compliance with the Final Amendments' obligations will require an overhaul of incident response and notice protocols. Beyond just the modernization of federal financial privacy and cybersecurity, which these regulatory amendments intend to address, the truncated period now required of covered institutions facing a data incident adds fuel to the fire during an already demanding and stressful time. Obligations may differ depending on type of institution or information handled, but entities under SEC jurisdiction would be wise to begin Regulation S-P Final Amendments compliance efforts as soon as possible to mitigate future troubles.

Rick Borden is a partner in the privacy & data security group at Frankfurt Kurnit. He represents fintech, insurtech, software as a service, cloud computing and other tech-forward companies on technology transactions and privacy and data security issues, including compliance with the New York State Department of Financial Services' cybersecurity regulation and SEC cybersecurity rules. Previously, Borden held senior legal roles in cybersecurity, privacy and technology at The Hartford, Bank of America and Depository Trust and Clearing Corporation. He was also the chief legal officer at an infrastructure as a service startup.

Andrew Folks is a Westin Fellow at the International Association of Privacy Professionals and will be joining Frankfurt Kurnit as an associate following conclusion of the fellowship. He is a 2023 law school graduate and has previously worked at the California Privacy Protection Agency on its rulemaking.