MAYER | BROWN

May 20, 2024

Legal Update

SEC Adopts Amendments to Regulation S-P

The Amendments Will Require Updates to Covered Institutions' Cybersecurity Programs

On May 15, 2024, the U.S. Securities and Exchange Commission ("SEC") adopted amendments (the "Amendments") to Regulation S-P under the Securities Exchange Act of 1934 (the "Exchange Act"),[1] which governs the treatment of nonpublic personal information about consumers by certain financial institutions, to modernize and enhance the protections under the regulation.

The Amendments require broker-dealers, investment companies,[2] SEC-registered investment advisers[3] ("investment advisers"), funding portals, and transfer agents registered with the SEC or another appropriate regulatory agency as defined in Section 3(a)(34)(B) of the Exchange Act ("transfer agents," and collectively with the other institution types, "Covered Institutions") to adopt written policies and procedures for incident response programs to address unauthorized access to or use of "customer information" (defined below). Notably, the Amendments create broad federal consumer notification requirements by mandating timely notification to individuals affected by an information security incident involving "sensitive customer information" (defined below) with details about the incident and information designed to help affected individuals respond appropriately.

The Amendments also (i) extend the application of Regulation S-P's requirements to safeguard customer records and information to transfer agents, (ii) broaden the scope of information covered by the requirements for safeguarding customer records and information and for properly disposing of consumer report information, (iii) impose requirements to maintain written records documenting compliance with the Amendments, and (iv) conform annual privacy notice delivery provisions to the terms of an exception provided by a statutory amendment to the Gramm-Leach-Bliley Act ("GLB Act") in December 2015.

The following provides an overview of certain aspects of the Amendments and related guidance in the Adopting Release.

BACKGROUND

Regulation S-P, which includes the "safeguards" and "disposal" rules, was adopted by the SEC in 2000. Currently, the safeguards rule requires broker-dealers, investment companies and investment advisers (but not transfer agents) to adopt written policies and procedures that address administrative, technical, and physical safeguards to protect customer records and information. Additionally, the disposal rule, which applies to transfer agents registered with the SEC in addition to the institutions covered by the safeguards rule, requires proper disposal of consumer report information.

As stated in the Adopting Release, the Amendments are designed to modernize and enhance the protections that Regulation S-P provides by addressing the expanded use of technology and corresponding risks – including cybersecurity and other operational risks – that have emerged since the regulation's original adoption. In this regard, the SEC notes that the industry has observed increased exposure to cyberattacks that threaten not only the financial firms themselves, but also their customers. Moreover, the industry's trend toward digitization has increasingly turned the problem of safeguarding customer records and information into one of cybersecurity. The SEC believes the Amendments are needed to provide enhanced protection of customer or consumer information and help ensure that customers of Covered Institutions receive timely and consistent notifications in the event of unauthorized access to or use of their information, such as in a cyberattack or if customer information is improperly disposed of or stolen.

FINAL RULES

Incident Response Program

The Amendments require Covered Institutions 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*. Any instance of unauthorized access to or use of customer information (referred to herein as an "incident") will trigger a Covered Institution's incident response plan.

The incident response program must include policies and procedures to:

(1) Assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the *customer information systems*[4] and types of customer information that may have been accessed or used without authorization;

(2) Take appropriate steps to *contain and control* the incident to prevent further unauthorized access to or use of customer information; and

(3) Notify each affected individual whose *sensitive customer information* was, or is reasonably likely to have been, accessed or used without authorization in accordance with the customer notification requirements discussed below, unless the Covered Institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information,[5] that 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*.[6]

As defined under the Amendments, the term "***customer information***" means, for any Covered Institution other than a transfer agent, any record containing nonpublic personal information (as defined in 17 CFR § 248.3(t))[7] about a customer of a financial institution, whether in paper, electronic or other form, that is in the possession of a Covered Institution or that is handled or maintained by the Covered Institution or on its behalf regardless of whether such information pertains to (a) individuals with whom the Covered Institution has a customer relationship, or (b) to the customers of other financial institutions where such information has been provided to the Covered Institution. For purposes of the Amendments, the term "customer" has the same meaning as in 17 CFR § 248.3(j)[8] unless the Covered Institution is a transfer agent. For transfer agents, the term "customer" means any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent.

The term "***sensitive customer information***" means 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.[9] The Amendments provide examples of what could constitute sensitive customer information, including information that can be *used alone* to authenticate an individual's identity, such as Social Security number, a driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, biometric records, a unique electronic identification number, address, or routing code, or telecommunication identifying information or access device. The Amendments also provide examples of customer identifying an individual or individual's account, including a name or online username that could be *used in combination* with the foregoing, or other authenticating information, such as a partial Social Security number, access code, or mother's maiden name.

Importantly, while the incident response program is generally required to address incidents involving any form of *customer information*, notification under the Amendments is only required when there has been unauthorized access to or use of *sensitive customer information*, a subset of customer information. As such, the incident response program's assessment and containment and control components cover a broader scope of information than the notification requirements.

Customer Notification Requirements

Timing, Content and Method of Notification

The Amendments require a Covered Institution to provide any required customer notices to affected individuals as soon as reasonably practicable, but not later than 30 calendar days, after the Covered Institution becomes aware that unauthorized access to or use of customer information has, or is reasonably likely to have, occurred.[10] The Amendments permit Covered Institutions to delay providing required notices only after the SEC receives a written request from the U.S. Attorney General that such notices pose a substantial risk to national security or public safety. In practice, delay under the exception is likely to be rare.

The notice must be clear and conspicuous, include details about the incident, the exposed data, and how affected individuals can respond to the incident to protect themselves. Specifically, the Covered Institution must:

(1) Describe in general terms the incident and the type of sensitive customer information that was or is reasonably believed to have been accessed or used without authorization;

(2) Include, if the information is reasonably possible to determine at the time the notice is provided, any of the following: the date of the incident, the estimated date of the incident, or the date range within which the incident occurred;

(3) Include contact information sufficient to permit an affected individual to contact the Covered Institution to inquire about the incident, including the following: a telephone number (which should be a toll-free number if available), an email address or equivalent method or means, a postal address, and the name of a specific office to contact for further information and assistance;

(4) If the individual has an account with the Covered Institution, recommend that the customer review account statements and immediately report any suspicious activity to the Covered Institution;

(5) Explain what a fraud alert is and how an individual may place a fraud alert in the individual's credit reports to put the individual's creditors on notice that the individual may be a victim of fraud, including identity theft;

(6) Recommend that the individual periodically obtain credit reports from each nationwide credit reporting company and that the individual have information relating to fraudulent transactions deleted;

(7) Explain how the individual may obtain a credit report free of charge; and

(8) Include information about the availability of online guidance from the FTC and usa.gov regarding steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the FTC, and include the FTC's website address where individuals may obtain government information about identity theft and report suspected incidents of identity theft.[11]

The Amendments permit Covered Institutions to include additional information, but do not permit omission of the prescribed information.

Covered Institutions must ensure that required notices are transmitted by a means designed to ensure that affected individuals can reasonably be expected to receive actual notice in writing. These written notifications may be provided electronically if certain conditions are met, such as if the customer has agreed to receive information electronically, and subject to other applicable law (*e.g.*, state-level notification requirements).

Situations Not Requiring Customer Notification

As stated above, there is no obligation to notify customers if a Covered Institution has determined, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information that occurred at such Covered Institution or one of its service providers that is not itself a Covered Institution, 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. This risk of harm threshold will enable Covered Institutions to avoid providing notification to customers when there is unauthorized access to their sensitive customer information but not harm is reasonably likely to occur.[12]

Scope of Affected Individuals

If an incident of unauthorized access to or use of customer information has or is reasonably likely to have occurred, but the Covered Institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization, such Covered Institution must provide notice to all individuals whose sensitive customer information resides in the customer information system that was, or was reasonably likely to have been, accessed or used without authorization. Notwithstanding the foregoing, if the Covered Institution reasonably determines that a specific individual's sensitive customer information that resides in the customer information system was not accessed or used without authorization, the Covered Institution is not required to provide notice to that individual.

Service Providers

The Amendments require that Covered Institutions' incident response programs include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring of "service providers,"[13] including to ensure that affected individuals receive any required notices.

Specifically, the policies and procedures must be reasonably designed to ensure service providers take appropriate measures to:

(1) Protect against unauthorized access to or use of customer information; and

(2) Provide notification to the Covered Institution as soon as possible, but no later than 72 hours after becoming aware of a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider.

Upon receipt of such notification by the service provider, the Covered Institution must initiate its incident response program.

Covered Institutions are permitted, as part of their incident response programs, to enter into a written agreement with a service provider to notify affected individuals on the Covered Institution's behalf. However, Covered Institutions retain the obligation to ensure that affected individuals are notified in

accordance the notice requirements under Regulation S-P, as amended, even if such services are contracted to a service provider.

Other Changes

Transfer Agents

The Amendments extend both the safeguards rule and the disposal rule to apply to transfer agents. This is a significant change because, prior to the Amendments, the safeguards rule did not apply to any transfer agents, and the disposal rule applied only to those transfer agents registered with the SEC.

Additionally, as discussed above, the Amendments include a definition of "customer" that is specific to transfer agents (that is, for transfer agents, the term "customer" means any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent).

Recordkeeping

The Amendments require Covered Institutions (other than funding portals[14]) to make and maintain written records documenting compliance with the requirements of the safeguards rule and the disposal rule, for the time periods set forth in **Appendix A** to this Legal Update.

Exception to Annual Delivery of Privacy Notice

The Amendments modify Regulation S-P's annual privacy notice delivery provisions to conform to the terms of an exception added by the Fixing America's Surface Transportation (FAST) Act of 2015, which provides that a Covered Institution is not required to deliver an annual privacy notice if the Covered Institution (a) only provides non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies (*e.g.*, pursuant to 17 CFR 248.13, which provides an exception from Regulation S-P's opt-out requirements for service providers and joint marketing) and (b) has not changed its policies and practices with regard to disclosing non-public personal information from its most recent disclosure sent to customers.

Compliance Dates

The compliance period for the Amendments is either (a) 18 months from the date of publication in the Federal Register for Covered Institutions that are "larger entities" or (b) 24 months from the date of publication in the Federal Register for Covered Institutions that are "smaller entities." **Appendix B** to this Legal Update outlines which Covered Institutions will be considered "larger entities" for these purposes; Covered Institutions will be considered "smaller entities" if they do not meet the standards for "larger entities."

Conclusion

Covered Institutions should carefully review the Amendments against their existing privacy, incident response and information security policies and vendor agreements, and make appropriate updates, including updates to ensure timely notice of security incidents. In addition, when making updates, Covered Institutions should ensure that they navigate related requirements under other federal laws, as well as state laws. Moreover, Covered Institutions should carefully monitor developments regarding the SEC's proposed cybersecurity risk management rules. If you have any questions or would like to learn more about the Amendments and related SEC guidance, please contact the authors.

Appendix A

RECORDKEEPING REQUIREMENTS

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 (Business development companies and employee securities 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.
SEC-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.

Appendix B

DESIGNATION OF "LARGER ENTITIES"

Entity	Qualification to be Considered a "Larger 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[15]
Transfer agents	All transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act[16]

For more information about the topics discussed in this Legal Update, please contact any of the following authors.

The Free Writings & Perspectives, or FW&Ps, blog provides news and views on securities regulation and capital formation. The blog provides up-to-the-minute information regarding securities law developments, particularly those related to capital formation. FW&Ps also offers commentary regarding developments affecting private placements, mezzanine or "late stage" private placements, PIPE transactions, IPOs and the IPO market, new financial products and any other securities-related topics that pique our and our readers' interest. Our blog is available at: https://www.freewritings.law/.

Steffen Hemmerich
+1 212 506 2129
shemmerich@mayerbrown.com

Anna T. Pinedo
+1 212 506 2275
apinedo@mayerbrown.com

Jeffrey P. Taft
+1 202 263 3293
jtaft@mayerbrown.com

Adam D. Kanter
+1 202 263 3164
akanter@mayerbrown.com

Justin Herring
+1 212 506 2878
jherring@mayerbrown.com

Timothy B. Nagy
+1 202 263 3079
tnagy@mayerbrown.com

Leslie S. Cruz
+1 202 263 3337
lcruz@mayerbrown.com

Stephen Vogt
+1 202 263 3364
svogt@mayerbrown.com

Mark X. Zhuang
+1 212 506 2768
mzhuang@mayerbrown.com

[1] Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, Exchange Act Release No. 97141 (May 16, 2024) (the "Adopting Release"). The SEC initially published a proposal to amend Regulation S-P on March 15, 2023. Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, Exchange Act Release No. 97141 (Mar. 15, 2023), 88 FR 20616 (Apr. 6, 2023).

[2] Regulation S-P applies to investment companies as that term is defined in Section 3 of the Investment Company Act of 1940 (the "ICA"), whether or not the investment company is registered with the SEC. For example, a business development company, which is an investment company but is not required to register as such with the SEC, is subject to Regulation S-P; similarly, employee securities' companies are also covered. In contrast, an issuer that is excluded from the ICA's "investment company" definition (*e.g.*, a private fund that is able to rely on Section 3(c)(1) or 3(c)(7) of the ICA) is not subject to Regulation S-P but would be subject to the Federal Trade Commission's ("FTC") GLB Act privacy regulations (12 C.F.R. Part 313) and safeguards regulation (12 C.F.R Part 314).

[3] Exempt reporting advisers not subject to Regulation S-P would be subject to the FTC's GLB Act privacy regulations (12 C.F.R. Part 313) and safeguards regulation (12 C.F.R Part 314).

[4] The Amendments define the term "customer information systems" to mean the information resources owned or used by a Covered Institution, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of customer information to maintain or support the Covered Institution's operations.

[5] As stated in the Adopting Release, whether an investigation is reasonable will depend on the particular facts and circumstances of the unauthorized access or use. For example, unauthorized access or use that is the result of intentional intrusion by a threat actor may warrant more extensive investigation than inadvertent unauthorized access or use by an employee.

[6] The Amendments do not define the term "substantial harm or inconvenience." Pursuant to the Adopting Release, determining whether a given harm or inconvenience rises to the level of a substantial harm or inconvenience would depend on the particular facts and circumstances surrounding an incident.

[7] Pursuant to 17 CFR § 248.3(t), the term "nonpublic personal information" means: (i) personally identifiable financial information; and (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available information. Nonpublic personal information does not include publicly available information, except as included on a list described in clause (ii) above or when the publicly available information is disclosed in a manner that indicates the individual is or has been your consumer, or any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available information.

[8] Pursuant to 17 CFR § 248.3(j) , the term "customer" means "a consumer who has a customer relationship with you."

[9] As described in the Adopting Release, the "sensitive customer information" definition is calibrated to include types of information that, if exposed, could put affected individuals at a higher risk of suffering substantial harm or inconvenience through, for example, fraud or identity theft enabled by the unauthorized access to or use of the information.

[10] The federal banking agencies impose a similar customer notification obligation under their GLB Act safeguards regulations. 12 C.F.R. Parts 30, 208, 211, 225, 263, 308 and 364. The FTC's GLB Act safeguards regulation requires notification to the FTC but not customers. 12 C.F.R. Part 314. State data breach notification laws, which exist in all 50 states and the District of Columbia, also impose consumer notification requirements.

[11] While the FTC's GLB Act regulations do not apply to Covered Institutions, the FTC's guidance regarding identity theft is a helpful resource for individuals who have been the subject of unauthorized access to their personal information.

[12] The federal banking agencies' GLB Act safeguards regulation and some of the state data breach notification laws have a similar risk of harm threshold for notification.

[13] The Amendments define the term "service provider" to mean 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.

[14] Pursuant to Regulation Crowdfunding under the Exchange Act, funding portals must comply with the requirements of Regulation S-P as they apply to broker-dealers. However, funding portals are not subject to the recordkeeping obligations for broker-dealers set forth in Rule 17a-4 under the Exchange Act.

[15] A broker or dealer is a small entity if it: (i) had total capital of less than $500,000 on the date in its prior fiscal year as of which its audited financial statements were prepared or, if not required to file audited financial statements, on the last business day of its prior fiscal year; and (ii) is not affiliated with any person that is not a small entity.

[16] A transfer agent is a small entity if it: (i) received less than 500 items for transfer and less than 500 items for processing during the preceding six months; (ii) transferred items only of issuers that are small entities; (iii) maintained master shareholder files that in the aggregate contained less than 1,000 shareholder accounts or was the named transfer agent for less than 1,000 shareholder accounts at all times during the preceding fiscal year; and (iv) is not affiliated with any person that is not a small entity.