THOMPSON HINE

Privacy & Cybersecurity Update

May 2024

SEC Amends Regulation S-P to Address Information Security and Data Breach Response

On May 16, 2024, the Securities and Exchange Commission (SEC) announced the adoption of amendments to Regulation S-P to modernize and enhance the rules governing the treatment of consumers' nonpublic personal information by certain financial institutions. The amendments update the requirements for broker-dealers (including funding portals), investment companies, registered investment advisers, and transfer agents (collectively, "covered institutions") to address new technology development and cybersecurity risks. 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. The SEC's amendment information security requirements that mirror some of the requirements set forth in its cybersecurity regulation are also applicable to publicly traded companies.

Information Security Programs. The amendments require covered institutions to develop, implement, and maintain written policies and procedures for an incident response (IR) program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. In addition, the amendments expand and align the safeguards rules to cover both nonpublic personal information that a covered institution collects about its own customers and nonpublic personal information it receives from another financial institution about customers of that financial institution.

Incident Response (IR) Framework. The amendments require covered institutions to adopt an IR program as part of their written policies and procedures under the safeguards rule. The IR program must be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. The IR program must include procedures to assess the nature and scope of any such incident and to take appropriate steps to contain and control such incidents to prevent further unauthorized access or use. Covered institutions, other than funding portals, are required to make and maintain written records documenting compliance with the requirements of the safeguards rule.

Customer Data Breach Notification Requirement. The amendments also require covered institutions to notify affected individuals whose sensitive customer information was or is reasonably likely to have been, accessed or used without authorization. The amendments require a covered institution to provide the notice as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred, except under certain limited circumstances. A notice must include details about the incident, the breached data, and how affected individuals can respond to the breach to protect themselves. Notice is not required if a covered institution determines 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.

Oversight of Service Providers. The amendments also require the IR program to establish, maintain, and enforce

written policies and procedures reasonably designed for oversight of service providers. A service provider is 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. The policies and procedures must be reasonably designed to ensure that service providers take measures to protect against unauthorized access to or use of customer information and provide notification as soon as practicable, but not later than 72 hours, after becoming aware of a breach in security has occurred from unauthorized access to a customer information system maintained by the service provider. In addition, A covered institution may enter into a written agreement with its service provider to notify affected individuals on the covered institution's behalf of a security breach, provided however, the obligation to ensure that affected individuals are notified of a security breach rests with the covered institution.

Designation of Larger Entities. The SEC provides the following qualifications for different entities to be considered a "larger entity." Investment companies, together with other investment companies in the same group of related investment companies, must have a net asset of $1 billion or more as of the end of the most recent fiscal year. Registered investment advisers must have $1.5 billion or more in assets under management. This designation also applies to all broker-dealers or transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act.

Regulation S-P: Broker-Dealers, Investment Companies & Advisers, and Transfer Agents

Data Breach Requirements: 17 CFR § 248.30.

The numbering and internal citations herein are derived from the applicable federal regulation.

	Regulation S-P (Data Breach Requirements)
Personally Identifiable Financial Information	The term "personally identifiable financial information" means any information: (i) a consumer provides to you to obtain a financial product or service from you; (ii) about a consumer resulting from any transaction involving a financial product or service between you and a consumer; or (iii) you otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.
Sensitive Customer Information	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. (ii) Examples of sensitive customer information include: (A) Customer information uniquely identified with an individual that has a reasonably likely use as a means of authenticating the individual's identity, including (1) A Social Security number, official State- or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (2) A biometric record; (3) A unique electronic identification number, address, or routing code; (4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)); or, (B) Customer information identifying an individual or the individual's account, including the individual's account number, name or online user name, in combination with authenticating information such as information described in paragraph (d)(9)(ii)(A) of this section, or in combination with similar information that could be used to gain access to the customer's account such as an access code, a credit card expiration date, a partial Social Security number, a security code, a security question and answer identified with the individual or the individual's account, or the individual's date of birth, place of birth, or mother's maiden name".
Nonpublic Personal Information	(t) The term "nonpublic personal information" means (1) 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. (2) Nonpublic personal information does not include: (i) Publicly available information, except as included on a list described in paragraph (t)(1)(ii) of this section or when the publicly available information is disclosed in a manner that indicates the individual is or has been your consumer; or (ii) 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.
Customer Information	The term "customer information" for any covered institution other than a transfer agent registered with the SEC or another ARA means any record containing "nonpublic personal information" as defined in § 248.3(t) 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. (ii) With respect to a transfer agent registered with the SEC or another ARA, customer information means any record containing "nonpublic personal information" as defined in § 248.3(t) identified with any natural person, who is a securityholder of an issuer for which the transfer agent acts or has acted as transfer agent, that is in the possession of a transfer agent or that is handled or maintained by the transfer agent or on its behalf, regardless of whether such information pertains to individuals with whom the transfer agent has a customer relationship, or pertains to the customers of other financial institutions and has been provided to the transfer agent.
Notice Obligations	A covered institution must provide a clear and conspicuous notice, or ensure that such notice is provided, to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.
Risk of Harm Analysis	Unless 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 the 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*, it must comply with its security breach notice obligations.
Notification Timeline	A covered institution must provide the notice as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred.
Security and Investigation Exceptions	The notification timeline may be delayed if the U.S. Attorney General determines that the notice required under this rule poses a substantial risk to national security or public safety, and notifies the SEC of such determination in writing, in which case the covered institution may delay providing such notice for a time period specified by the Attorney General, up to 30 days following the date when such notice was otherwise required to be provided. The notice may be delayed for an additional period of up to 30 days if the Attorney General determines that the notice continues to pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing. In extraordinary circumstances, notice required under this section may be delayed for a final additional period of up to 60 days if the Attorney General determines that such notice continues to pose a substantial risk to national security and notifies the SEC of such determination in writing. Beyond the final 60-day delay, if the Attorney General indicates that further delay is necessary, the SEC will consider additional requests for delay and may grant such delay through SEC exemptive order or other action.
Notification Contents	The security breach notice must: (A) 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; (B) 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; (C) 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; (D) 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; (E) 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; (F) 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; (G) Explain how the individual may obtain a credit report free of charge; and (H) 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.
Delivery Methods	The notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing.
Data Processor Obligations	A covered institution's response program must 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, including to ensure that the covered institution notifies affected individuals of a security breach. The policies and procedures must be reasonably designed to ensure service providers take appropriate measures to: (A) Protect against unauthorized access to or use of customer information; and (B) 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 a customer information system maintained by the service provider. Upon receipt of such notification, the covered institution must initiate its incident response program. A covered institution may enter into a written agreement with its service provider to notify affected individuals on the covered institution's behalf of a security breach. Notwithstanding a covered institution's use of a service provider, the obligation to ensure that affected individuals are notified of a security breach rests with the covered institution.
Other Information	If an incident of unauthorized access to or use of customer information has occurred 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, the 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.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Andrew J. Davalla
216.566.5706
Andrew.Davalla@ThompsonHine.com

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Thora Knight, Ph.D.
212.908.3971
Thora.Knight@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)

Abigail L. Ophir
216.566.5682
Abigail.Ophir@ThompsonHine.com