Orical LLC
May 2024

Regulation S-P Amendments: Privacy of Consumer Financial Information and Safeguarding Customer Information

On May 16, 2024, the Securities and Exchange Commission ("Commission" or "SEC") adopted[1] significant new rule amendments[2] that require brokers and dealers (or "broker-dealers")[3], investment companies, investment advisers registered with the Commission ("registered investment advisers"), funding portals, and transfer agents registered with the Commission or another appropriate regulatory agency ("ARA") as defined in the Securities Exchange Act of 1934 ("transfer agents") to adopt written policies and procedures for incident response programs to address unauthorized access to or use of customer information, including procedures for providing timely notification to individuals affected by an incident involving sensitive customer information with details about the incident and information designed to help affected individuals respond appropriately.

The compliance period is 18 months after the date of publication in the Federal Register for larger entities[4] and 24 months for smaller entities. Covered institutions may consider implementing these amendments on a more urgent basis as they may likely be required to satisfy similar state law or other similar regulatory requirements that are in effect now.

In addition, the amendments extend the application of requirements to safeguard customer records and information to transfer agents; broaden the scope of information covered by the requirements for safeguarding customer records and information and for properly disposing of consumer report information; impose requirements to maintain written records documenting compliance with the amended rules; and conform annual privacy notice delivery provisions to the terms of an exception provided by a statutory amendment to the Gramm-Leach-Bliley Act ("GLBA").

Regulation S-P is a set of privacy rules adopted pursuant to the GLBA and the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") that govern the treatment of nonpublic personal information about consumers by certain financial institutions. The Commission adopted rule amendments designed to modernize and enhance the protections that Regulation S-P provides by addressing the expanded use of technology and corresponding risks that have emerged since the Commission adopted Regulation S-P in 2000.[5] The amendments in particular update the requirements of the "safeguards" and "disposal" rules. The safeguards rule requires brokers, dealers, investment companies, and registered investment advisers to adopt written policies and procedures that address administrative, technical, and physical safeguards to protect customer records and information. The disposal rule, which applies to transfer agents registered with the Commission in addition to the institutions covered by the safeguards rule, requires proper disposal of consumer report information. In addition, under Regulation Crowdfunding, funding portals must comply with the requirements of Regulation S-P as they apply to brokers. Thus, funding portals are also required to comply with the applicable amendments to Regulation S-P.

---

[1] See https://www.sec.gov/news/press-release/2024-58 for access to the SEC's May 16, 2024 Press Release, Fact Sheet as well as Release Nos. 34-100155; IA-6604; IC-35193; File No. S7-05-23 (the "Release").
[2] The rule amendments are referred to herein as the Rules. The text of the Rules are included in this memorandum with annotations primarily from the Release for ease of reference.
[3] This category includes notice-registered broker-dealers that are futures commission merchants and introducing brokers registered with the CFTC that are permitted to register as broker-dealers by filing a notice with the Commission for the purpose of effecting security futures products. See Release footnote 375.
[4] See Release p. 129-130 and Table 3: Designation of Larger Entities. Registered Investment Advisers, for example, with $1.5 billion or more in assets under management are considered "larger entities."
[5] See Privacy of Consumer Financial Information (Regulation S-P), Exchange Act Release No. 42974 (June 22, 2000 [65 FR 40334 (June 29, 2000] https://www.federalregister.gov/documents/2000/06/29/00-16269/privacy-of-consumer-financial-information-regulation-s-p.

The SEC states that the Regulation S-P 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. In evaluating amendments to Regulation S-P, the Commission considered developments in how firms obtain, share, and maintain individuals' personal information since the SEC originally adopted Regulation S-P, which correspond with an increasing risk of harm to individuals.

The SEC adopted amendments to Regulation S-P substantially as proposed. The principal elements of the amendments include:

• *Incident Response Program*. The final safeguards rule requires covered institutions to develop, implement, and maintain written policies and procedures[6] for an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. The final amendments require that a response program include procedures to assess the nature and scope of any incident and to take appropriate steps to contain and control the incident to prevent further unauthorized access or use.

• *Notification Requirement*. The response program procedures in the final amendments also include a requirement that covered institutions provide a notification to individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. Notice will not be required if a 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, 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. Under the final amendments, a customer notice must be clear and conspicuous[7] and provided by a means designed to ensure that each affected individual can reasonably be expected to receive it. This notice must be provided as soon as reasonably practicable, but not later than 30 days, after the covered institution becomes aware that unauthorized access to or use of customer information has, or is reasonably likely to have, occurred. The final amendments will permit covered institutions to delay providing notice after the Commission receives a written request from the Attorney General that this notice poses a substantial risk to national security or public safety.

• *Service Providers*. The final amendments to the safeguards rule include new provisions that address the use of service providers by covered institutions. Under these provisions, covered institutions will be required to establish, maintain, and enforce written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring of service providers, including to ensure that affected individuals receive any required notices. The final amendments make clear that while covered institutions may use service providers to provide any required notice, covered institutions will retain the obligation to ensure that affected individuals are notified in accordance with the notice requirements. Service providers will have up to 72 hours to notify a covered institution after becoming aware of a breach.

• *Scope*. The final amendments more closely align the information protected under the safeguards rule and the disposal rule by applying the protections of both rules to "customer information," a newly defined term (definition included below). The final amendments also broaden the group of customers whose

[6] "Covered institutions need the flexibility to develop policies and procedures suited to their size and complexity and the nature and scope of their activities. Therefore, we did not propose, and are not adopting, specific steps a covered institution must take when carrying out its incident response program, and we are not specifically designating who must undertake oversight responsibilities, thus providing covered institutions flexibility to determine whether and how to appropriately assign or divide such responsibilities." Release p. 19.

[7] The term "clear and conspicuous" is defined in 17 CFR 248.3(c)(1) at https://www.law.cornell.edu/cfr/text/17/248.3; See also, Release footnote 198.

information is protected under both rules. Also, transfer agents will be required to comply with the safeguards rule.

• *Recordkeeping and Annual Notice Amendments*. The final amendments add requirements for covered institutions, other than funding portals, to make and maintain written records[8] documenting compliance with the requirements of the safeguards rule and the disposal rule. Further, the final amendments amend the existing requirement to provide annual privacy notices to codify a statutory exception.

What follows is an annotated version of the Rules produced and edited by Orical LLC. The references and notes provided herein represent selected statements made by the SEC in the 348 page Release that may assist the reader in understanding the amendments. Understanding the new requirements is not the end of the process—but the beginning. Each covered institution must then design and implement the required policies and procedures (including with respect to service providers) as well as implement a management, governance and supervisory structure and ensure compliance with required books and records. This is a complex and time-consuming process. Restricting or limiting access only to information and files required for a supervised person to do that person's assigned tasks may limit any potential notification requirements as will the use of state-of-the art encryption techniques for information at rest as well as in transit. Periodic reassessments of systems and communications and storage technology in light of developing cyber threats is also essential. Historically, Regulation S-P has been a focus of SEC regulatory scrutiny; we anticipate that this scrutiny will continue.[9]

STATUTORY AUTHORITY

The Commission is amending Regulation S-P pursuant to authority set forth in sections 17, 17A, 23, and 36 of the Exchange Act [15 U.S.C. 78q, 78q-1, 78w, and 78mm], sections 31 and 38 of the Investment Company Act [15 U.S.C. 80a-30 and 80a-37], sections 204, 204A, and 211 of the Investment Advisers Act [15 U.S.C. 80b-4, 80b-4a, and 80b-11], section 628(a) of the FCRA [15 U.S.C. 1681w(a)], and sections 501, 504, 505, and 525 of the GLBA [15 U.S.C. 6801, 6804, 6805, and 6825].

List of Subjects

17 CFR Parts 240, 270, and 275

Reporting and recordkeeping requirements; Securities.

17 CFR Part 248

Brokers, Consumer protection, Dealers, Investment advisers, Investment companies, Privacy, Reporting and recordkeeping requirements, Securities, Transfer agents.

TEXT OF RULE AMENDMENTS

For the reasons set out in the preamble, title 17, chapter II of the Code of Federal Regulations is amended as follows:

PART 240—GENERAL RULES AND REGULATIONS, SECURITIES EXCHANGE ACT OF 1934

---

[8] See Release p. 121-126 and Table 1 Recordkeeping Requirements.

[9] See, for example, *Risk Alert: Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies* (April 16, 2019), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf; *Risk Alert: Safeguarding Customer Records and Information in Network Storage—Use of Third Party Security Features* (May 23, 2019) https://www.sec.gov/ocie/announcement/risk-alert-network-storage; *In the Matter of R.T. Jones Capital Equities Management, Inc.*, Advisers Act Release No. 4204 (Sept. 22, 2015) https://www.sec.gov/files/litigation/admin/2015/ia-4204.pdf.

1. The authority citation for part 240 and the sectional authority for § 240.17Ad-7 are revised to read, as follows:

Authority: 15 U.S.C. 77c, 77d, 77g, 77j, 77s, 77z-2, 77z-3, 77eee, 77ggg, 77nnn, 77sss, 77ttt, 78c, 78c-3, 78c-5, 78d, 78e, 78f, 78g, 78i, 78j, 78j-1, 78j-4, 78k, 78k-1, 78l, 78m, 78n, 78n-1, 78o, 78o-4, 78o-10, 78p, 78q, 78q-1, 78s, 78u-5, 78w, 78x, 78dd, 78ll, 78mm, 80a-20, 80a-23, 80a-29, 80a-37, 80b-3, 80b-4, 80b-11, 1681w(a)(1), 6801-6809, 6825, 7201 et seq., and 8302; 7 U.S.C. 2(c)(2)(E); 12 U.S.C. 5221(e)(3); 18 U.S.C. 1350; Pub. L. 111-203, 939A, 124 Stat. 1376 (2010); and Pub. L. 112-106, sec. 503 and 602, 126 Stat. 326 (2012), unless otherwise noted.

* * * * *

Section 240.17a-14 is also issued under Public Law 111-203, sec. 913, 124 Stat. 1376 (2010).

* * * * *

Section 240.17ad-7 is also issued under 15 U.S.C. 78b, 78q, and 78q-1.

* * * * *

2. Amend § 240.17a-4 by adding and reserving paragraph (e)(13), and adding paragraph (e)(14) to read as follows:

§ 240.17a-4 Records to be preserved by certain exchange members, brokers and dealers.

* * * * *

(e) * * *

(13) [Reserved]

(14)(i) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(a)(1) of this chapter until three years after the termination of the use of the policies and procedures;

(ii) The written documentation of any detected unauthorized access to or use of customer information, as well as any response to, and recovery from such unauthorized access to or use of customer information required by § 248.30(a)(3) of this chapter for three years from the date when the records were made;

(iii) The written documentation of any investigation and determination made regarding whether notification is required pursuant to § 248.30(a)(4) of this chapter, including the basis for any determination made, any written documentation from the United States Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination, for three years from the date when the records were made;

(iv) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(a)(5)(i) of this chapter until three years after the termination of the use of the policies and procedures;

(v) The written documentation of any contract or agreement entered into pursuant to § 248.30(a)(5) of this chapter until three years after the termination of such contract or agreement;

and

(vi) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(b)(2) of this chapter until three years after the termination of the use of the policies and procedures;

* * * * *

3. Redesignate §240.17Ad-7 as §240.17ad-7 and amend newly redesignated §240.17ad-7 by:

a. Revising the section heading;

b. Adding paragraph and reserving paragraph (j); and

c. Adding paragraph (k).

The revisions read as follows:

§ 240.17ad-7 (Rule 17Ad-7) Record retention.

* * * * *

(j) [Reserved]

(k) Every registered transfer agent shall maintain in an easily accessible place:

(1) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(a)(1) of this chapter for no less than three years after the termination of the use of the policies and procedures;

(2) The written documentation of any detected unauthorized access to or use of customer information, as well as any response to, and recovery from such unauthorized access to or use of customer information required by § 248.30(a)(3) of this chapter for no less than three years from the date when the records were made;

(3) The written documentation of any investigation and determination made regarding whether notification is required pursuant to § 248.30(a)(4) of this chapter, including the basis for any determination made, any written documentation from the United States Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination, for no less than three years from the date when the records were made;

(4) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(a)(5)(i) of this chapter until three years after the termination of the use of the policies and procedures;

(5) The written documentation of any contract or agreement entered into pursuant to § 248.30(a)(5) of this chapter until three years after the termination of such contract or agreement;

and

(6) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(b)(2) of this chapter for no less than three years after the termination of the use of the policies and procedures.

PART 248—REGULATIONS S-P, S-AM, and S-ID

4. The authority citation for part 248 continues to read as follows:

Authority: 15 U.S.C. 78q, 78q–1, 78o–4, 78o–5, 78w, 78mm, 80a–30, 80a–37, 80b–4, 80b–11, 1681m(e), 1681s(b), 1681s–3 and note, 1681w(a)(1), 6801-6809, and 6825; Pub. L. 111–203, secs. 1088(a)(8), (a)(10), and sec. 1088(b), 124 Stat. 1376 (2010).

* * * * *

5. Amend §248.5 by revising paragraph (a)(1), and adding paragraph (e) to read as follows:

§ 248.5 Annual privacy notice to customers required.

(a)(1) *General rule*. Except as provided by paragraph (e) of this section, you must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the continuation of the customer relationship. Annually means at least once in any period of 12 consecutive months during which that relationship exists. You may define the 12-consecutive-month period, but you must apply it to the customer on a consistent basis.

* * * * *

(e) *Exception to annual privacy notice requirement.* (1) *When exception available*. You are not required to deliver an annual privacy notice if you:[10]

(i) Provide nonpublic personal information to nonaffiliated third parties only in accordance with §§ 248.13, 248.14, or 248.15; and

(ii) Have not changed your policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer under § 248.6(a)(2) through (5) and (9) in the most recent privacy notice provided pursuant to this part.

(2) *Delivery of annual privacy notice after financial institution no longer meets the requirements for exception*. If you have been excepted from delivering an annual privacy notice pursuant to paragraph (e)(1) of this section and change your policies or practices in such a way that you no longer meet the requirements for that exception, you must comply with paragraph (e)(2)(i) or (e)(2)(ii) of this section, as applicable.

(i) *Changes preceded by a revised privacy notice*. If you no longer meet the requirements of paragraph (e)(1) of this section because you change your policies or practices in such a way that § 248.8 requires you to provide a revised privacy notice, you must provide an annual privacy notice in accordance with the timing requirement in paragraph (a) of this section, treating the revised privacy notice as an initial privacy notice.

(ii) *Changes not preceded by a revised privacy notice*. If you no longer meet the requirements of paragraph (e)(1) of this section because you change your policies or practices in such a way that § 248.8 does not require you to provide a revised privacy notice, you must provide an annual privacy notice within 100 days of the change in your policies or practices that causes you to no longer meet the requirement of paragraph (e)(1) of this section.

(iii) *Examples*. (A) You change your policies and practices in such a way that you no longer meet the requirements of paragraph (e)(1) of this section effective April 1 of year 1. Assuming you define the 12-consecutive-month period pursuant to paragraph (a) of this section as a calendar year, if you were required to provide a revised privacy notice under § 248.8 and you provided that notice on March 1 of

[10] See Release p. 126-128.

year 1, you must provide an annual privacy notice by December 31 of year 2. If you were not required to provide a revised privacy notice under § 248.8, you must provide an annual privacy notice by July 9 of year 1.

(B) You change your policies and practices in such a way that you no longer meet the requirements of paragraph (e)(1) of this section, and so provide an annual notice to your customers. After providing the annual notice to your customers, you once again meet the requirements of paragraph (e)(1) of this section for an exception to the annual notice requirement. You do not need to provide additional annual notice to your customers until such time as you no longer meet the requirements of paragraph (e)(1) of this section.

§ 248.17 [Amended]

6. Amend § 248.17 by, in paragraph (b), replacing the words "Federal Trade Commission" with "Consumer Financial Protection Bureau"; and replacing the words "Federal Trade Commission's" with "Consumer Financial Protection Bureau's."

7. Revise § 248.30 to read as follows:

§ 248.30 Procedures to safeguard customer information, including response programs for unauthorized access to customer information and customer notice; disposal of customer information and consumer information.

(a) *Policies and procedures to safeguard customer information*. (1) *General requirements*. Every covered institution must develop, implement, and maintain written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information.

(2) *Objectives*. These written policies and procedures must be reasonably designed to:

(i) Ensure the security and confidentiality of customer information;

(ii) Protect against any anticipated threats or hazards to the security or integrity of customer information; and

(iii) Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

(3) *Response programs for unauthorized access to or use of customer information*. Written policies and procedures in paragraph (a)(1) of this section must include a program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures. This response program must include procedures for the covered institution to:

(i) Assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization;[11]

[11] See Release p. 21. "Information developed during the assessment process may also help covered institutions develop a contextual understanding of the circumstances surrounding an incident, as well as enhance their technical understanding of the incident, which should be helpful in guiding incident response activities such as containment and control measures. The assessment process may also be helpful for identifying and evaluating existing vulnerabilities that could benefit from remediation in order to prevent such vulnerabilities from being exploited in the future. Further, covered institutions generally should consider reviewing and updating the assessment procedures periodically to ensure that the procedures remain reasonably designed."

(ii) Take appropriate steps to contain and control[12] the incident to prevent further unauthorized access to or use of customer information; and

(iii) Notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization in accordance with paragraph (a)(4) of this section unless the covered institution determines[13], after a reasonable investigation[14] of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, 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.[15]

(4) *Notifying affected individuals of unauthorized access or use*. (i) *Notification obligation*. Unless a covered institution has determined[16], 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, the covered institution must provide a clear and conspicuous notice[17], or ensure that such notice is provided, to each affected individual whose sensitive

---

[12] See Release p. 22. ". . .[T]he objective of containment and control is to prevent additional damage from unauthorized activity and to reduce the immediate impact of an incident by removing the source of the unauthorized activity. Strategies for containing and controlling an incident vary depending upon the type of incident and may include, for example, isolating compromised systems or enhancing the monitoring of intruder activities, searching for additional compromised systems, changing system administrator passwords, rotating private keys, and changing or disabling default user accounts and passwords, among other interventions. Because incident response may involve making complex judgment calls, such as deciding when to shut down or disconnect a system, developing and implementing written containment and control policies and procedures will provide a framework to help facilitate improved decision making at covered institutions during potentially high-pressure incident response situations. Further, covered institutions generally should consider reviewing and updating the containment and control procedures periodically to ensure that the procedures remain reasonably designed."

[13] ". . . [I]f it is reasonably likely that a malicious actor gained access to a covered institution's information system containing sensitive customer information but the scope of the breach is unclear (i.e., the covered institution is unable to determine which specific individuals' sensitive customer information has been accessed or used without authorization and cannot make the determinations required under the rule to avoid sending notices), the covered institution would be required to provide notice to each individual whose sensitive customer information resides in the customer information system." See Release p. 30-31

[14] A covered institution is not able to "rebut the presumption of notification" without conducting a reasonable investigation. "Further, the rule's requirement that a covered institution provide notice to all affected individuals where it is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization should incentivize covered institutions to establish procedures (for themselves and their service providers) that provide robust protections for sensitive customer information. For example, it may encourage covered institutions to employ a principle of least privilege, so that users' access rights to sensitive customer information on a particular information system are limited to the information strictly required to do their jobs. Protections that limit the scope of any breaches reduce the investigation and notification costs (and as a consequence, the potential harm) resulting from a breach." See Release p. 36.

[15] While the SEC did not define "substantial harm or inconvenience" they did devote pages 46-49 of the Release discussing the phrase: "Given the wide variety of ways that a data breach can injure a customer, and the potentially varied nature of those harms and inconveniences, the range of harms outlined in the proposed definition may be a useful starting point for this determination. A personal injury, financial loss, expenditure of effort, or loss of time, each could constitute a substantial harm or inconvenience depending on the particular facts and circumstances. Some examples of these harms could include theft, fraud, harassment, physical harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the misuse of information identified with an individual to obtain a financial product or service, or to access, log into, effect a transaction in, or otherwise misuse the individual's account."

[16] ". . . [F]or any determination that a covered institution makes that notice is not required, covered institutions other than funding portals will be required to maintain a record of the investigation and basis for its determination." See Release p. 27.

[17] "While the incident response program is generally required to address information security incidents involving any form of customer information, notification is only required when there has been unauthorized access to or use of sensitive customer information, a subset of customer information, because it presents increased risks to affected individuals. This notice standard is designed to give affected individuals an opportunity to mitigate the risk of substantial harm or inconvenience arising from an information security incident that potentially implicates their sensitive customer information by affording them an opportunity to take timely responsive actions, such as monitoring credit reports for unauthorized activity, placing fraud alerts on relevant accounts,

customer information was, or is reasonably likely to have been, accessed or used without authorization. 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.

(ii) *Affected individuals*. 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 under this paragraph.

(iii) *Timing*. A covered institution must provide the notice as soon as practicable, but not later than 30 days[18], after becoming aware[19] that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred unless the United States Attorney General determines that the notice required under this rule poses a substantial risk to national security or public safety[20], and notifies the Commission 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[21] and notifies the Commission 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 Commission of such determination in writing. Beyond the final 60-day delay under this paragraph (a)(4)(iii), if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such delay through Commission exemptive order or other action.

(iv) *Notice contents*. The notice must:[22]

(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;

---

or changing passwords used to access accounts. At the same time, the final amendments provide a mechanism for covered institutions to avoid making unnecessary notifications in cases where, following a reasonable investigation, the 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 to the affected individual. Additionally, customer information that is not disposed of properly could trigger the requirement to notify affected individuals under final rule 248.30(a)(4)(i). For example, a covered institution whose employee leaves un-shredded customer files containing sensitive customer information in a dumpster accessible to the public would be required to notify affected customers, unless the institution has determined 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. See Release footnote 68 and related text.

[18] See Release p. 49-57.

[19] See Release footnote 177 for a discussion of the "becoming aware" standard. It is important to note that a covered institution would "become aware" of a breach long before the completion of a reasonable investigation and conclusion of the incident response process following an unauthorized access and well before making a "materiality determination."

[20] See Release p. 57-62.

[21] The delay for "national security or public safety is discussed on page 57 of the Release.

[22] See Release p. 62-68 for a discussion of the notice content and format.

(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 Federal Trade Commission 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 Federal Trade Commission, and include the Federal Trade Commission's website address where individuals may obtain government information about identity theft and report suspected incidents of identity theft.

(5) *Service providers*. (i) A covered institution's response program prepared in accordance with paragraph (a)(3) of this section 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[23], including to ensure that the covered institution notifies affected individuals as set forth in paragraph (a)(4) of this section. 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

[23] Service providers are discussed on pages 69-92 of the Release. "Further, while it may be helpful to a covered institution in achieving compliance with the final amendments to receive "reasonable assurances" from its service providers that they have taken appropriate measures to both protect customer information and provide timely notification to the covered institution in the event of a relevant breach of the service provider's customer information systems, reliance solely on such assurances may be insufficient depending on the facts and circumstances, for example when a covered institution knows, or has reason to know, that such assurance is inaccurate. Instead, the final rules require the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of the service provider to ensure the covered institution will be able to satisfy the obligations of paragraph (a)(4). Further, covered institutions generally should consider reviewing and updating these policies and procedures periodically throughout their relationship with a service provider, including updates designed to address any information learned during the course of their monitoring." "Consistent with this risk-based approach, covered institutions may wish to consider employing such tools as independent certifications and attestations obtained from the service provider, as suggested by some commenters, as part of their policies and procedures to require oversight, including through due diligence and monitoring, of the service provider."

(B) Provide notification to the covered institution as soon as possible, but no later than 72 hours[24] after becoming aware[25] 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 adopted pursuant to paragraph (a)(3) of this section.

(ii) As part of 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 in accordance with paragraph (a)(4) of this section.[26]

(iii) Notwithstanding a covered institution's use of a service provider in accordance with paragraphs (a)(5)(i) and (ii) of this section, the obligation to ensure that affected individuals are notified in accordance with paragraph (a)(4) of this section rests with the covered institution.[27]

(b) *Disposal of consumer information and customer information*.

(1) *Standard*. Every covered institution, other than notice-registered broker-dealers, must properly dispose of consumer information and customer information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

(2) *Written policies, procedures, and records*. Every covered institution, other than notice-registered broker-dealers, must adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information according to the standard identified in paragraph (b)(1) of this section.

(3) *Relation to other laws*. Nothing in this paragraph (b) shall be construed:

(i) To require any covered institution to maintain or destroy any record pertaining to an individual that is not imposed under other law; or

(ii) To alter or affect any requirement imposed under any other provision of law to maintain or destroy records.

(c) *Recordkeeping*. (1) Every covered institution that is an investment company under the Investment Company Act of 1940 (15 U.S.C. 80a), but is not registered under section 8 thereof (15 U.S.C. 80a-8), must make and maintain:

(i) The written policies and procedures required to be adopted and implemented pursuant to paragraph (a)(1) of this section;

---

[24] See Release p. 77 for a discussion of the service provider deadline to provide notice.
[25] The "becoming aware" of standard is discussed on pages 83-85 and is contrasted with a "having a reasonable basis to conclude" standard or a "determining" standard both of which could result in undue delays and frustrate the investor protection goals of the final amendments.
[26] See Release p. 85.
[27] See Release p. 86-87. ". . . [W]here the covered institution has entered into a written agreement with its service provider to provide notice on the covered institution's behalf pursuant to paragraph (a)(5)(ii), and the covered institution determines that the service provider has not provided such notifications in a manner that satisfies the conditions of paragraph (a)(4), the covered institution must still ensure that notification is provided to the customer, and the covered institution's policies and procedures generally should be designed to address these instances. To accomplish this, the covered institution generally should conduct timely due diligence to identify any lack of notification by the service provider to the customer and remedy the matter in advance of the deadline set out in paragraph (a)(4)."

(ii) The written documentation of any detected unauthorized access to or use of customer information, as well as any response to, and recovery from such unauthorized access to or use of customer information required by paragraph (a)(3) of this section;

(iii) The written documentation of any investigation and determination made regarding whether notification is required pursuant to paragraph (a)(4) of this section, including the basis for any determination made, any written documentation from the United States Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination;

(iv) The written policies and procedures required to be adopted and implemented pursuant to paragraph (a)(5)(i) of this section;

(v) The written documentation of any contract or agreement entered into pursuant to paragraph (a)(5) of this section; and

(vi) The written policies and procedures required to be adopted and implemented pursuant to paragraph (b)(2) of this section.

(2) In the case of covered institutions described in paragraph (c)(1) of this section, such records, apart from any policies and procedures, must be preserved for a time period not less than six years, the first two years in an easily accessible place. In the case of policies and procedures required under paragraphs (a) and (b)(2) of this section, covered institutions described in paragraph (c)(1) of this section must maintain a copy of such policies and procedures in effect, or that at any time within the past six years were in effect, in an easily accessible place.

(d) *Definitions*. As used in this section, unless the context otherwise requires:

(1) ***Consumer information*** means any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report, or a compilation of such records, that a covered institution maintains or otherwise possesses for a business purpose regardless of whether such information pertains to (i) individuals with whom the covered institution has a customer relationship, or (ii) to the customers of other financial institutions where such information has been provided to the covered institution. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.

(2) ***Consumer report*** has the same meaning as in section 603(d) of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)).

(3) ***Covered institution*** means any broker or dealer, any investment company, and any investment adviser or transfer agent registered with the Commission or another appropriate regulatory agency ("ARA") as defined in section 3(a)(34)(B) of the Securities Exchange Act of 1934.

(4)(i) ***Customer*** has the same meaning as in § 248.3(j) unless the covered institution is a transfer agent registered with the Commission or another ARA.

(ii) With respect to a transfer agent registered with the Commission or another ARA, for purposes of this section, *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.

(5)(i) ***Customer information***[28] for any covered institution other than a transfer agent registered with the Commission 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 Commission 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.

(6) ***Customer information systems*** means 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.

(7) ***Disposal*** means:

(i) The discarding or abandonment of consumer information or customer information; or

(ii) The sale, donation, or transfer of any medium, including computer equipment, on which consumer information or customer information is stored.

(8) ***Notice-registered broker-dealer*** means a broker or dealer registered by notice with the Commission under section 15(b)(11) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(b)(11)).

(9)(i) ***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.[29]

(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

---

[28] See Release p. 93.

[29] See Release p. 39-45 for a discussion of the definition of Sensitive customer information. Of particular interest is the discussion of "encryption." ". . . [W]e are not excepting encrypted information from the rule's definition of sensitive customer information. . . . Specifically, in applying the final rule, a covered institution may consider encryption as a factor in determining whether the compromise of customer information could create a reasonably likely harm risk to an individual identified with the information. Specifically, we acknowledge that encryption of information using current industry standard best practices is a reasonable factor for a covered institution to consider in making this determination. To the extent such encryption minimizes the likelihood that the cipher text could be decrypted, it would also reduce the likelihood that the cipher text's compromise could create a risk of harm, as long as the associated decryption key is secure." "Accordingly, while the final amendments provide illustrative examples of information (such as a customer's Social Security number) that can constitute sensitive customer information when unencrypted, a covered institution could nevertheless determine that the encrypted representation of that information is not sensitive customer information if the encryption renders the cipher text sufficiently secure, such that the compromise of that encrypted information does not create a reasonably likely risk of substantial harm or inconvenience to an individual."

(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.

(10) ***Service provider*** means 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.[30]

(11) ***Transfer agent*** has the same meaning as in section 3(a)(25) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(25)).

PART 270—RULES AND REGULATIONS, INVESTMENT COMPANY ACT OF 1940

8. The authority citation for part 270 is revised to read as follows:

Authority: 15 U.S.C. 80a-1 et seq., 80a-34(d), 80a-37, 80a-39, 1681w(a)(1), 6801-6809, 6825, and Pub. L. 111-203, sec. 939A, 124 Stat. 1376 (2010), unless otherwise noted.

* * * * *

Section 270.31a-2 is also issued under 15 U.S.C. 80a-30.

9. Amend § 270.31a-1 by adding paragraph (b)(13) to read as follows:

§ 270.31a-1 Records to be maintained by registered investment companies, certain majority-owned subsidiaries thereof, and other persons having transactions with registered investment companies.

* * * * *

(b) * * *

(13)(i) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(a)(1);

[30] See Release p. 87-92. This definition includes affiliates of covered institutions. "Where financial counterparties receive, maintain, or otherwise are permitted access to customer information through the provision of services directly to the covered institution, they meet the service provider definition as adopted."

(ii) The written documentation of any detected unauthorized access to or use of customer information, as well as any response to, and recovery from such unauthorized access to or use of customer information required by § 248.30(a)(3);

(iii) The written documentation of any investigation and determination made regarding whether notification is required pursuant to § 248.30(a)(4), including the basis for any determination made, any written documentation from the United States Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination;

(iv) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(a)(5)(i);

(v) The written documentation of any contract or agreement entered into pursuant to § 248.30(a)(5); and (vi) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(b)(2).

* * * * *

10. Amend § 270.31a-2 by:

a. In paragraph (a)(7), removing the period at the end of the paragraph and adding "; and" in its place; and

b. Adding paragraph (a)(8) to read as follows:

§ 270.31a-2 Records to be preserved by registered investment companies, certain majority-owned subsidiaries thereof, and other persons having transactions with registered investment companies.

(a) * * *

(8) Preserve for a period not less than six years, the first two years in an easily accessible place, the records required by § 270.31a-1(b)(13) apart from any policies and procedures thereunder and, in the case of policies and procedures required under § 270.31a-1(b)(13), preserve a copy of such policies and procedures in effect, or that at any time within the past six years were in effect, in an easily accessible place.

* * * * *

PART 275— RULES AND REGULATIONS, INVESTMENT ADVISERS ACT OF 1940

11. The authority citation for part 275 is revised to read as follows:

Authority: 15 U.S.C. 80b-2(a)(11)(G), 80b-2(a)(11)(H), 80b-2(a)(17), 80b-3, 80b-4, 80b-4a, 80b-6(4), 80b-6a, 80b-11, 1681w(a)(1), 6801-6809, and 6825, unless otherwise noted.

* * * * *

Section 275.204-2 is also issued under 15 U.S.C. 80b-6.

* * * * *

12. Amend § 275.204-2 by adding paragraph (a)(25) to read as follows:

§ 275.204-2 Books and records to be maintained by investment advisers.

(a) * * *

(25)

(i) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(a)(1);

(ii) The written documentation of any detected unauthorized access to or use of customer information, as well as any response to, and recovery from such unauthorized access to or use of customer information required by § 248.30(a)(3) of this chapter;

(iii) The written documentation of any investigation and determination made regarding whether notification is required pursuant to § 248.30(a)(4) of this chapter, including the basis for any determination made, any written documentation from the United States Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination;

(iv) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(a)(5)(i) of this chapter;

(v) The written documentation of any contract or agreement entered into pursuant to § 248.30(a)(5) of this chapter; and

(vi) The written policies and procedures required to be adopted and implemented pursuant to § 248.30(b)(2) of this chapter.

* * * * *