This document is scheduled to be published in the
Federal Register on 04/06/2023 and available online at
federalregister.gov/d/2023-05774, and on **govinfo.gov**

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 240, 248, 270, and 275

[Release Nos. 34-97141; IA-6262; IC-34854; File No. S7-05-23]

RIN 3235-AN26

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

AGENCY: Securities and Exchange Commission.

ACTION: Proposed rule.

SUMMARY: The Securities and Exchange Commission ("Commission" or "SEC") is proposing rule amendments that would require brokers and dealers (or "broker-dealers"), investment companies, and investment advisers registered with the Commission ("registered investment advisers") 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 Commission also is proposing to broaden the scope of information covered by amending requirements for safeguarding customer records and information, and for properly disposing of consumer report information. In addition, the proposed amendments would extend the application of the safeguards provisions to transfer agents. The proposed amendments would also include requirements to maintain written records documenting compliance with the proposed amended rules. Finally, the proposed amendments would conform annual privacy notice delivery provisions to the terms of an exception provided by a statutory amendment to the Gramm-Leach-Bliley Act ("GLBA").

DATES: Comments should be received on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Comments may be submitted by any of the following methods:

Electronic Comments:

- Use the Commission's internet comment form (http://www.sec.gov/rules/submitcomments.htm); or
- Send an email to rule-comments@sec.gov. Please include File Number S7-05-23 on the subject line.

Paper Comments:

- Send paper comments to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.

All submissions should refer to File Number S7-05-23. The file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method of submission. The Commission will post all comments on the Commission's website (http://www.sec.gov/rules/proposed.shtml). Comments are also available for website viewing and printing in the Commission's Public Reference Room, 100 F Street, NE, Washington, DC, 20549, on official business days between the hours of 10 a.m. and 3 p.m. Operating conditions may limit access to the Commission's public reference room. All comments received will be posted without change; the Commission does not edit personal identifying information from submissions. You should submit only information that you wish to make available publicly.

Studies, memoranda, or other substantive items may be added by the Commission or staff to the comment file during this rulemaking. A notification of the inclusion in the comment file of any such materials will be made available on the Commission's website. To ensure direct electronic receipt of such notifications, sign up through the "Stay Connected" option at www.sec.gov to receive notifications by email.

FOR FURTHER INFORMATION CONTACT: Susan Poklemba, Brice Prince, or James Wintering, Special Counsels; Edward Schellhorn, Branch Chief; Devin Ryan, Assistant Director;

John Fahey, Deputy Chief Counsel; Emily Westerberg Russell, Chief Counsel; Office of Chief Counsel, Division of Trading and Markets, (202) 551-5550; Jessica Leonardo or Taylor Evenson, Senior Counsels; Aaron Ellias, Acting Branch Chief; Marc Mehrespand, Branch Chief; Thoreau Bartmann, Co-Chief Counsel, Chief Counsel's Office, Division of Investment Management, (202) 551-6792, Securities and Exchange Commission, 100 F Street, NE, Washington, DC, 20549.

SUPPLEMENTARY INFORMATION: The Commission is proposing for public comment amendments to 17 CFR 248 ("Regulation S-P")[1] under Title V of the GLBA [15 U.S.C. 6801 - 6827], the Fair Credit Reporting Act ("FCRA") [15 U.S.C. 1681-1681x], the Securities Exchange Act of 1934 ("Exchange Act") [15 U.S.C. 78a *et seq*.], the Investment Company Act of 1940 ("Investment Company Act") [15 U.S.C. 80a-1 *et seq*.], and the Investment Advisers Act of 1940 ("Investment Advisers Act") [15 U.S.C. 80b-1 *et seq*.].

[1] Unless otherwise noted, all references below to rules contained in Regulation S-P are to Part 248 of Chapter 17 of the Code of Federal Regulations ("CFR").

Table of Contents

I. INTRODUCTION
- A. Background
- B. 2008 Proposal
- C. Overview of the Proposal

II. DISCUSSION
- A. Incident Response Program Including Customer Notification
  1. Assessment
  2. Containment and Control
  3. Service Providers
  4. Notice to Affected Individuals
- B. Remote Work Arrangement Considerations
- C. Scope of Information Protected under the Safeguards Rule and Disposal Rule
  1. Definition of Customer Information
  2. Safeguards Rule and Disposal Rule Coverage of Customer Information
  3. Extending the Scope of the Safeguards Rule and the Disposal Rule to Cover All Transfer Agents
  4. Maintaining the Current Regulatory Framework for Notice-Registered Broker-Dealers
- D. Recordkeeping
- E. Exception from the Annual Notice Delivery Requirement
  1. Current Regulation S-P requirements for privacy notices
  2. Proposed amendment
- F. Request for Comment on Limited Information Disclosure When Personnel Leave Their Firms
- G. Other Current Commission Rule Proposals
  1. Covered Institutions Subject to the Regulation SCI Proposal and the Exchange Act Cybersecurity Proposal
  2. Investment Management Cybersecurity
- H. Existing Staff No-Action Letters and Other Staff Statements
- I. Proposed Compliance Date

III. ECONOMIC ANALYSIS
- A. Introduction
- B. Broad Economic Considerations
- C. Baseline
  1. Safeguarding Customer Information -- Risks and Practices
  2. Regulation
  3. Market Structure
- D. Benefits and Costs of the Proposed Rule Amendments
  1. Response Program
  2. Extend Scope of Customer Safeguards to Transfer Agents
  3. Recordkeeping
  4. Exception from Annual Notice Delivery Requirement
- E. Effects on Efficiency, Competition, and Capital Formation
- F. Reasonable Alternatives Considered
  1. Reasonable Assurances from Service Providers
  2. Lower Threshold for Customer Notice
  3. Encryption Safe Harbor
  4. Longer Customer Notification Deadlines
  5. Broader Law Enforcement Exception from Notification Requirements
- G. Request for Comment on Economic Analysis

IV. PAPERWORK REDUCTION ACT
- A. Introduction
- B. Amendments to the Safeguards Rule and Disposal Rule
- C. Request for Comment

V. INITIAL REGULATORY FLEXIBILITY ACT ANALYSIS
- A. Reason For and Objectives of the Proposed Action
- B. Legal Basis
- C. Small Entities Subject to Proposed Rule Amendments
- D. Projected Reporting, Recordkeeping, and Other Compliance Requirements
- E. Duplicative, Overlapping, or Conflicting Federal Rules
- F. Significant Alternatives
- G. Request for Comment

VI. CONSIDERATION OF IMPACT ON THE ECONOMY

STATUTORY AUTHORITY

I. INTRODUCTION

The Commission adopted Regulation S-P in 2000.[2] Regulation S-P's provisions include, among other requirements, rule 248.30(a) ("safeguards rule"), which requires brokers, dealers, investment companies,[3] and registered investment advisers to adopt written policies and procedures for administrative, technical, and physical safeguards to protect customer records and information.[4] Another provision of Regulation S-P, rule 248.30(b) ("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.[5] Since Regulation S-P was adopted, evolving digital communications and information storage tools and other technologies have made it easier for firms to obtain, share, and maintain individuals' personal information. This evolution also has changed or exacerbated the risks of unauthorized access to or use of personal information,[6] thus increasing the risk of potential harm to individuals whose information is not protected against unauthorized access or use.[7]

---

[2] *See* Privacy of Consumer Financial Information (Regulation S-P), Exchange Act Release No. 42974 (June 22, 2000) [65 FR 40334 (June 29, 2000)] ("Reg. S-P Release"). Regulation S-P is codified at 17 CFR Part 248, Subpart A.

[3] Regulation S-P applies to investment companies as the term is defined in section 3 of the Investment Company Act (15 U.S.C. 80a-3), whether or not the investment company is registered with the Commission. *See* 17 CFR 248.3(r). Thus, a business development company, which is an investment company but is not required to register as such with the Commission, is subject to Regulation S-P. Similarly, employees' securities companies – including those that are not required to register under the Investment Company Act – are investment companies and are, therefore, subject to Regulation S-P. By contrast, issuers that are excluded from the definition of investment company – such as private funds that are able to rely on section 3(c)(1) or 3(c)(7) of the Investment Company Act – would not be subject to Regulation S-P.

[4] *See* 17 CFR 248.30(a).

[5] *See* 17 CFR 248.30(b). In this release, institutions to which Regulation S-P currently applies, or to which the proposed amendments would apply, are sometimes referred to as "covered institutions." The term "covered institution" is sometimes used in this release to refer to institutions referred to as "you" in Regulation S-P.

[6] Unauthorized use differs from unauthorized access in that a person making unauthorized use of customer information may or may not be authorized to access it. Cf. *Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021) (discussing how a person can access a computer without authorization or exceed authorized access). As described in more detail below, covered institutions would have to provide notice to affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.

[7] *See, e.g.*, Federal Bureau of Investigation, 2021 Internet Crime Report (Mar. 22, 2022), at 7-8,

This environment of expanded risks supports our proposing updates to the requirements of Regulation S-P. Currently, the safeguards rule addresses protecting customer information against unauthorized access or use, but it does not include a requirement to notify affected individuals in the event of a data breach. In assessing firm and industry compliance with these requirements, Commission staff typically focus on information security controls, including whether firms have taken appropriate measures to safeguard customer accounts and to respond to data breaches.[8] Commission staff have observed a number of practices with respect to the information safeguards requirements of Regulation S-P and have provided observations on several occasions to assist firms in improving their practices.[9] Although many firms have improved their programs for safeguarding customer records and information in light of these observations, nonetheless we are concerned that some firms may not maintain plans for

---

available at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (stating that the FBI's Internet Crime Complaint Center received 847,376 complaints in 2021 (an increase of approximately 181% from 2017). The complaints included 51,629 related to identity theft and 51,829 related to personal data breaches (increases of approximately 193% and 68% from 2017, respectively)); the Financial Industry Regulatory Authority ("FINRA"), *2021 Report on FINRA's Examination and Risk Monitoring Program: Cybersecurity and Technology Governance* (Feb. 2021), *available at* https://www.finra.org/sites/default/files/2021-02/2021-report-finras-examination-risk-monitoring-program.pdf (noting increased cybersecurity or technology-related incidents at firms); Office of Compliance Inspections and Examinations (now the Division of Examinations) ("EXAMS"), Risk Alert, *Cybersecurity: Safeguarding Client Accounts against Credential Compromise* (Sept. 15, 2020), *available at* https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf (describing increasingly sophisticated methods used by attackers to gain access to customer accounts and firm systems). This Risk Alert, and any other Commission staff statements represent the views of the staff. They are not a rule, regulation, or statement of the Commission. Furthermore, the Commission has neither approved nor disapproved their content. These staff statements, like all staff statements, have no legal force or effect: they do not alter or amend applicable law; and they create no new or additional obligations for any person.

8 *See* EXAMS, *2022 Examination Priorities*, *available at* https://www.sec.gov/files/2022-exam-priorities.pdf; EXAMS, *Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies* (Apr. 16, 2019) ("Reg. S-P Risk Alert"), *available at* https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf.

9 *See* Reg. S-P Risk Alert, *supra* note 8 (noting that examples of the most common deficiencies or weaknesses observed by EXAMS staff included that broker-dealer and investment adviser written incident response plans did not address, among other things, actions required to address a cybersecurity incident and assessments of system vulnerabilities); EXAMS, *Observations from Cybersecurity Examinations* (Aug. 7, 2017) ("Observations Risk Alert"), *available at* https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

addressing incidents of unauthorized access to or use of data[10] We also are concerned the incident response programs that firms have implemented may be insufficient to respond to evolving threats or may not include well-designed plans for customer notification.[11]

We therefore preliminarily believe specifically requiring a reasonably designed incident response program, including policies and procedures for assessment, control and containment, and customer notification, could help reduce or mitigate the potential for harm to individuals whose sensitive information is exposed or compromised in a data breach. Requiring firms to adopt incident response programs to address unauthorized access to or use of customer information, including customer notification and recordkeeping requirements, would enhance protections for customer information. The advance planning required under an incident response program should improve an institution's preparedness and the effectiveness of its response to data breaches while still being consistent with the requirements for safeguarding standards articulated in the GLBA.[12]

In certain instances, some types of customer notification plans may already be required by existing state laws mandating customer notifications. While all 50 states have enacted laws in recent years requiring firms to notify individuals of data breaches, standards differ by state, with some states imposing heightened notification requirements relative to other states.[13] Currently,

---

10 *See* Reg. S-P Risk Alert, *supra* note 8; Observations Risk Alert, *supra* note 9 (noting that some firms lacked plans for addressing access incidents).

11 *See* Reg. S-P Risk Alert, *supra* note 8. Although broker-dealers are subject to self-regulatory organization ("SRO") rules requiring written supervisory procedures and written business continuity plans addressing subjects including data back-up and recovery, SRO rules do not require notification to customers whose information is compromised. *See, e.g.*, FINRA Rule 3110 (Supervision) (requiring members to establish, maintain, and enforce written procedures to supervise the types of business in which they engage and the activities of their associated persons that are reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules), and FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) (requiring members to create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption that must address specified topics including data back-up and recovery).

12 The GLBA's requirements for standards for safeguarding customer records and information are described in the Background section below. *See infra* section I.A.

13 Upon its adoption, rule 248.17 essentially restated the then-current text of section 507 of the

broker-dealers, investment companies, and registered investment advisers respond to data breaches according to applicable state laws. For example, states differ in the types of information that, if accessed or used without authorization, may trigger a notification requirement.[14] States also differ regarding a firm's duty to investigate a data breach when determining whether notice is required, deadlines to deliver notice, and the information required to be included in a notice, among other matters.[15] As a result, a firm's notification obligations arising from a single data breach may vary such that customers in one state may receive notice while customers of the same institution in another state may not receive notice or may receive less information. In reviewing these state laws, we determined that certain aspects of these provisions would be appropriately adopted as components of a Federal minimum standard for customer notification, which would help affected customers understand how to respond to a data breach to protect themselves from potential harm that could result.

Our proposal would afford certain individuals greater protections by, for example, defining "sensitive customer information" more broadly than the current definitions used by at least 12 states, thereby requiring customers in those states to receive notice for a broader range of

---

GLBA, and as such, referenced determinations made by the Federal Trade Commission. *See* Reg. S-P Release, *supra* note 2. The proposal would, however, update rule 248.17 to instead reference determinations made by the Consumer Financial Protection Bureau, consistent with changes made to section 507 of the GLBA by the Dodd-Frank Wall Street Reform and Consumer Protection Act. *See* Pub. L. 111-203, sec. 1041, 124 Stat. 1376 (2010).

[14] For example, some states may require a firm to notify individuals when a data breach includes biometric information, while others do not. *Compare* Cal. Civil Code sec. 1798.29 (notice to California residents of a data breach generally required when a resident's personal information was or is reasonably believed to have been acquired by an unauthorized person; "personal information" is defined to mean an individual's first or last name in combination with one of a list of specified elements, which includes certain unique biometric data) *with* Ala. Stat. secs. 8-38-2, 8-38-4, 8-38-5 (notice of a data breach to Alabama residents is generally required when sensitive personally identifying information has been acquired by an unauthorized person and is reasonably likely to cause substantial harm to the resident to whom the information relates; "sensitive personally identifying information" is defined as the resident's first or last name in combination with one of a list of specified elements, which does not include biometric information).

[15] *See infra* sections II.A.4 and III.C.2.a.

personal information included in a breach.[16] Additionally, the 30-day notification deadline proposed in this release is shorter than the timing currently mandated by 15 states, and would also offer enhanced protections to individuals in 32 states with laws that do not include a notification deadline as well as those in states that mandate or permit delayed notifications for law enforcement purposes.[17] A standardized notification deadline ensures timely notice to affected customers and would enhance their ability to take action quickly to protect themselves against the consequences of a breach. Further, consistent with 22 state laws, this proposal would require customer notification unless, after investigation, the covered institution finds no risk of harm.[18] Twenty-one states currently have a presumption against notifying customers of a breach, and only require notice if, after investigation, the covered institution finds risk of harm.[19] In addition, in the 11 states where state customer notification laws do not apply to entities subject to or in compliance with the GLBA, the proposal would help ensure customers of such institutions receive notice of a breach.[20] As discussed more fully below, establishing a federal minimum standard would protect individuals in an environment of enhanced risk.[21]

There are compelling reasons to revisit other aspects of the current safeguards regime as well. As noted above, the safeguards rule currently applies to broker-dealers, investment companies, and registered investment advisers. The safeguards rule does not currently apply to

---

16 *See infra* section II.C.1.

17 *See infra* section II.A.4.e.

18 *See infra* section II.A.4.a.

19 *See id.*

20 *See id.*

21 The effect of any inconsistency between the proposed customer notification and state law requirements may, however, be mitigated because many states offer safe harbors from their notification laws for entities that are subject to or in compliance with requirements under Federal regulations. In particular, as noted, 11 states offer safe harbors for entities subject to or in compliance with the GLBA, while others offer safe harbors for compliance with the notification requirements of the entity's "primary federal regulator." *See, e.g.*, Del. Code Ann. tit. 6 section 12B-103 (providing that a person regulated by the GLBA and maintaining procedures for security breaches pursuant to the law established by its Federal regulator is deemed to be in compliance with the Delaware notification requirements if the person notifies affected Delaware residents in accordance with those procedures). *See infra* note 106 and accompanying text.

transfer agents, even though they also obtain, share, and maintain personal information on behalf of securityholders who hold securities in registered form (*i.e.*, in their own name rather than indirectly through a broker). Securityholders whose personal information is maintained by transfer agents could be harmed by the unauthorized access or use of such information in the same manner as customers of broker-dealers, investment companies, and registered investment advisers, yet such securityholders are not currently protected by the safeguards rule. The Commission preliminarily believes that extending the safeguards rule to cover transfer agents is necessary to ensure that there is a Federal minimum standard for the notification of securityholders who are affected by a data breach that leads to the unauthorized access or use of their information, regardless of whether that data breach occurs at a broker-dealer, investment company, registered investment adviser, or transfer agent.[22]

In addition, the safeguards rule currently requires only that institutions protect their own customers' information. This potentially overlooks information a broker-dealer, investment company, or registered investment adviser may have received from another financial institution about that financial institution's customers,[23] such as nonpublic personal information from an introducing broker or dealer that clears transactions for its customers through a clearing broker

---

22 *See infra* section II.C.3.

23 Under section 501(b) of the GLBA, the standards to be established by the Commission must, among other things, "protect against unauthorized access to or use of" customer records or information "which could result in substantial harm or inconvenience to *any* customer." *See* 15 U.S.C. 6801(b)(3) (emphasis added). We agree with the Federal Trade Commission ("FTC") that applying the safeguards rule to cover customer information that a financial institution receives pertaining to another institution's customers is consistent with the purpose and language of the GLBA. Further, the Commission agrees with the FTC that this approach is the most reasonable reading of the statutory language and clearly furthers the express congressional policy to respect the privacy of these customers and to protect the security and confidentiality of their nonpublic personal information. *See* FTC, *Standards for Safeguarding Customer Information*, 67 FR 36484, 36485-86 (May 23, 2002); *see also infra* section II.C.2 (describing proposed new definition of "customer information" that would include both nonpublic personal information that a covered institution collects about its own customers and nonpublic personal information about customers of a third-party financial institution that the covered institution receives from the third-party financial institution).

on a fully disclosed basis.[24] Applying the safeguards rule and the disposal rule to customer information that a covered institution receives from other financial institutions would better protect individuals by ensuring customer information safeguards are not lost when a third-party financial institution shares that information with a covered institution.[25] Finally, applying the safeguards rule and the disposal rule to a broader set of information should enhance the security and confidentiality of customers' personal information.

Therefore, the Commission is proposing amendments to Regulation S-P to enhance the protection of this information by: (1) requiring covered institutions to include incident response programs in their safeguards policies and procedures to address unauthorized access to or use of customer information, including procedures for providing timely notification to affected individuals; (2) extending the safeguards rule to all transfer agents registered with the Commission or another appropriate regulatory agency as defined in section 3(a)(34)(B) of the Exchange Act (unless otherwise noted, we refer to them collectively as "transfer agents" for purposes of this release); (3) more closely aligning the information protected by the safeguards rule and the disposal rule; and (4) broadening the set of customers covered by those rules.

A. Background

Title V of the GLBA,[26] among other things, directed the Commission and other Federal financial regulators to establish and implement standards requiring financial institutions subject to their jurisdiction to adopt administrative, technical, and physical safeguards for the protection of customer records and information.[27] The GLBA specified that these standards were "(1) to

---

[24] *See* 17 CFR 248.3(g)(2)(iii) ("An individual is not your consumer if he or she has an account with another broker or dealer (the introducing broker-dealer) that carries securities for the individual in a special omnibus account with you (the clearing broker-dealer) in the name of the introducing broker-dealer, and when you receive only the account numbers and transaction information of the introducing broker-dealer's consumers in order to clear transactions.").

[25] *See infra* section II.C.2.

[26] 15 U.S.C. 6801-6827.

[27] *See* 15 U.S.C. 6801(b) and 6804(a)(1).

insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[28]

As noted above, the safeguards rule sets forth standards for safeguarding customer records and information and currently requires covered institutions to adopt written policies and procedures for administrative, technical, and physical safeguards to protect customer records and information.[29] While the term "customer records and information" is not defined in the GLBA or in Regulation S-P,[30] the safeguards must be reasonably designed to meet the GLBA's standards.[31] This approach is designed to provide flexibility for covered institutions to safeguard customer records and information in accordance with their own privacy policies and practices and business models.

Pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), the Commission amended Regulation S-P in 2004 by adopting the disposal rule to protect against the improper disposal of "consumer report information."[32] "Consumer report information" is

---

[28] 15 U.S.C. 6801(b).

[29] 17 CFR 248.30(a). Other sections of Regulation S-P implement the notice and opt out provisions of the GLBA. *See* 17 CFR 248.1-248.18. In addition to the safeguards rule and the disposal rule (17 CFR 248.30(b)), the GLBA and Regulation S-P require brokers, dealers, investment companies and registered investment advisers to provide an annual notice of their privacy policies and practices to their customers (and notice to consumers before sharing their nonpublic customer information with nonaffiliated third parties outside certain exceptions). *See* 15 U.S.C. 6803(a); 17 CFR 248.4; 17 CFR 248.5. We are also proposing an exception to the annual notice delivery requirement. *See infra* section II.E.

[30] *See* 17 CFR 248.30(a); 15 U.S.C. 6801(b)(1) (discussing but not defining "customer records or information").

[31] Specifically, the safeguards must be reasonably designed to insure the security and confidentiality of customer records and information, protect against anticipated threats to the security or integrity of those records and information, and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. *See* 17 CFR 248.30(a). *See also* 15 U.S.C. 6801(b).

[32] 17 CFR 248.30(b). *See* Disposal of Consumer Report Information, Exchange Act Release No. 50781 (Dec. 2, 2004) [69 FR 71322 (Dec. 8, 2004)] ("Disposal Rule Adopting Release"). Section 216 of the FACT Act amended the FCRA by adding section 628 (codified at 15 U.S.C. 1681w), which directed the Commission and other Federal financial regulators to adopt regulations

defined as "any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report" and also means "a compilation of such records," but does not include "information that does not identify individuals, such as aggregate information or blind data."[33] The disposal rule currently applies to the financial institutions subject to the safeguards rule, except that it excludes "notice-registered broker-dealers,"[34] and it applies to transfer agents registered with the Commission.[35] The disposal rule requires these entities that maintain or possess "consumer report information" for a business purpose, to take "reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[36]

The GLBA and FACT Act oblige us to adopt regulations, to the extent possible, that are consistent and comparable with those adopted by the Banking Agencies and the FTC.[37] Accordingly, in determining the scope of the proposed amendments contemplated in this proposal, including for example, the definitions of "customer information" and "sensitive customer information" described below, we are mindful of the need to set standards for

---

"requiring any person who maintains or possesses consumer information or any compilation of consumer information derived from a consumer report for a business purpose must properly dispose of the information."

33 *See* 17 CFR 248.30(b)(1)(ii).

34 *See* 17 CFR 248.30(b)(1)(iv) (defining "notice-registered broker-dealers" as "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. 78***o***(b)(11))"). *See also infra* section II.C.4 further detailing the current regulatory framework for notice-registered broker-dealers under the safeguards rule and the disposal rule.

35 *See* 17 CFR 248.30(b)(2)(i).

36 *See* 17 CFR 248.30(b).

37 *See generally* 15 U.S.C. 6804(a) (directing the agencies authorized to prescribe regulations under title V of the GLBA to assure to the extent possible that their regulations are consistent and comparable); 15 U.S.C. 1681w(a)(2)(A) (directing the agencies with enforcement authority set forth in 15 U.S.C. 1681s to consult and coordinate so that, to the extent possible, their regulations are consistent and comparable). The "Banking Agencies" include the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), and the former Office of Thrift Supervision.

safeguarding customer records and information that are consistent and comparable with the corresponding standards set by the Banking Agencies and the FTC.

B. 2008 Proposal

In 2008, the Commission proposed amendments to Regulation S-P primarily to help prevent information security breaches in the securities industry and to improve responsiveness when such breaches occur, with the goal of better protecting investors from identity theft and other misuse of what the proposal would have defined as "personal information."[38] The 2008 Proposal would have set out specific standards for safeguarding customer records and information, including requirements for procedures to respond to incidents of unauthorized access to or use of personal information. Those requirements would have included procedures for notifying the Commission (or a broker-dealer's designated examining authority[39]) of data breach incidents, and procedures for notifying individuals of incidents of unauthorized access to or misuse of sensitive personal information, if the misuse had occurred or was reasonably possible. The 2008 Proposal also would have amended the safeguards rule and the disposal rule so that both would have protected "personal information," which would have included any record containing either "nonpublic personal information" or "consumer report information."[40] In addition, the 2008 Proposal would have extended the safeguards rule to apply to transfer

---

[38] *See* Part 248 – Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer information, Exchange Act Release No. 57427 (Mar. 4, 2008) [73 FR 13692, 13693-94 (Mar. 13, 2008)] ("2008 Proposal"). The amendments to Regulation S-P referenced in the 2008 Proposal have not been adopted.

[39] A broker-dealer's designated examining authority is the SRO of which the broker-dealer is a member, or, if the broker-dealer is a member of more than one SRO, the SRO designated by the Commission pursuant to 17 CFR 240.17d-1 as responsible for examination of the member for compliance with applicable financial responsibility rules (including the Commission's customer account protection rules at 17 CFR 240.15c3-3). *See* 2008 Proposal, *supra* note 38, at n.44.

[40] The 2008 Proposal would have made both the safeguards rule and the disposal rule, as amended, applicable to "personal information," which would have been defined to include any record containing either "nonpublic personal information" or "consumer report information" that is identified with any consumer, or with any employee, investor, or securityholder who is a natural person, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of a covered institution. *See* 2008 Proposal, *supra* note 38, at 73 FR 13700.

agents registered with the Commission, and would have extended the disposal rule to apply to natural persons who are associated persons of a broker or dealer, supervised persons of a registered investment adviser, and associated persons of any transfer agent registered with the Commission. The 2008 Proposal would have further required brokers, dealers, investment companies, registered investment advisers, and transfer agents registered with the Commission to maintain and preserve written records of their policies and procedures required under the disposal and safeguards rules and compliance with those policies and procedures.

The Commission received over 400 comment letters in response to the 2008 Proposal.[41] The current proposal to amend Regulation S-P has been informed by comments received on the 2008 Proposal. Most commenters supported requirements for comprehensive information security programs that are consistent and comparable to the rules and guidance of other Federal financial regulators.[42] Many commenters, however, objected to changes in the scope of information and entities covered by the proposed amendments.[43] Many commenters opposed or suggested modifying the proposed amendments' information security breach response provisions.[44] Comments were mixed on the proposed exception for disclosures relating to transfers of representatives from one broker-dealer or registered investment adviser to another.[45]

---

41 Comments on the proposal, including comments referenced in this Release are available on the Commission website at http://www.sec.gov/comments/s7-06-08/s70608.shtml. Approximately 328 of the comments received contained substantially the same content. *See* example of Letter Type A available at https://www.sec.gov/comments/s7-06-08/s70608typea.htm.

42 *See, e.g.*, Letter from Alan E. Sorcher, Managing Director and Associate General Counsel, Securities Industry and Financial Markets Association (May 12, 2008) ("SIFMA Letter"); Letter from Tamara K. Salmon, Senior Associate Counsel, Investment Company Institute (May 2, 2008) ("ICI Letter"); Letter from Marcia E. Asquith, Senior Vice President and Corporate Secretary, Financial Industry Regulatory Authority (May 12, 2008) ("FINRA Letter").

43 *See, e.g.*, SIFMA Letter; Letter from Charles V. Rossi, President, The Securities Transfer Association, Inc. (May 9, 2008) ("STA Letter").

44 *See, e.g.*, SIFMA Letter; ICI Letter; Letter from Karen L. Barr, General Counsel, Investment Adviser Association (May 12, 2008) ("IAA Letter"); Letter from Sarah Miller, General Counsel, ABA Securities Association (May 22, 2008) ("ABASA Letter").

45 *See, e.g.*, SIFMA Letter; IAA Letter (both in support); Letter from Julius L. Loeser, Chief Regulatory and Compliance Counsel, Comerica Securities, Inc. (May 9, 2008) ("Comerica Letter"); Letter from Steven French, President, MemberMap LLC (May 11, 2008) ("MemberMap

C. Overview of the Proposal

There are no Commission rules at this time expressly requiring broker-dealers, investment companies, or registered investment advisers to have policies and procedures for responding to data breach incidents or to notify customers of those breaches.[46] As noted above, advance planning would be part of creating a reasonably designed incident response program, and its prompt implementation following a breach (including notification to affected individuals), is important in limiting potential harmful impacts to individuals. While we recognize that state laws require covered institutions to notify state residents of data breaches, those laws are not consistent and exclude some entities from certain requirements. Accordingly, a Federal minimum standard would provide notification to all customers of a covered institution affected by a data breach (regardless of state residency) and provide consistent disclosure of important information to help affected customers respond to a data breach. Other Federal regulators' GLBA safeguarding standards also include a requirement for a data breach response plan or program.[47]

Letter") (both opposed).

46 As noted above, there are no SRO rules requiring notification to customers whose information has been compromised. *See supra* note 11. The Commission has pending proposals to address cybersecurity risk with respect to investment advisers, investment companies, and public companies. The Commission encourages commenters to review those proposals to determine whether it might affect their comments on this proposing release. *See infra* note 55.

47 The FTC recently amended its Safeguards Rule by, among other things, adding a requirement for financial institutions under the FTC's GLBA jurisdiction to establish a written incident response plan designed to respond to information security events. *See* FTC, Standards for Safeguarding Customer Information, 86 FR 70272 (Dec. 9, 2021) ("FTC Safeguards Release"). As amended, the FTC's rule requires that a response plan address security events materially affecting the confidentiality, integrity, or availability of customer information in the financial institution's control, and that the plan include specified elements that would include procedures for satisfying an institution's independent obligation to perform notification as required by state law. *See* FTC Safeguards Release, at 70297-98, n.295. Earlier, the Banking Agencies and the National Credit Union Administration ("NCUA") jointly issued guidance on responding to incidents of unauthorized access to or use of customer information. *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 FR 15736, 15743 (Mar. 29, 2005) ("Banking Agencies' Incident Response Guidance"). The Banking Agencies' Incident Response Guidance provides, among other things, that when an institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to determine promptly the likelihood that the information has been or will be misused. If the institution determines that misuse of the

The Commission is proposing amendments to Regulation S-P's safeguards rule. The proposed amendments would 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.[48] The amendments would 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.[49]

The proposed response program procedures also would have to include notification to individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.[50] Notice would 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.[51] Under the proposed amendments, a customer notice must be clear and conspicuous and provided by a means designed to ensure that each affected individual can reasonably be expected to receive it.[52] A covered institution would be required to provide notice as soon as practicable, but not later than 30 days, that the incident occurred or is reasonably likely to have occurred.[53] To the extent a covered institution would have a

---

information has occurred or is reasonably possible, it should notify affected customers as soon as possible.

48 *See* proposed rule 248.30(b).

49 *See* proposed rule 248.30(b)(3).

50 *See* proposed rule 248.30(b)(4). *See* proposed rule 248.30(e)(9) for the definition of "sensitive customer information." *See also infra* section II.A.4, which includes a discussion of "sensitive customer information."

51 *See id.*

52 *See* proposed rule 248.30(b)(4)(i).

53 *See* proposed rule 248.30(b)(4)(iii).

notification obligation under both the proposed rules and a similar state law, a covered institution should be able to provide one notice to satisfy notification obligations under both the proposed rules and the state law, provided it included all information required under both the proposed rules and the state law.[54]

The Commission also is proposing amendments to Regulation S-P to enhance the protection of customers' nonpublic personal information. These proposed amendments would 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. We also propose to broaden the group of customers whose information is protected under both rules. Additionally, we propose to bring all transfer agents within the scope of the safeguards rule.

The proposal is not inconsistent with other recent cybersecurity-related rulemaking proposals.[55] Additionally, as described in greater detail below,[56] the Commission is also proposing rules and rule amendments related to cybersecurity risk and related disclosures as well as Regulation SCI.[57] We encourage commenters to review those other cybersecurity-related

---

54 We are not aware of any laws that would require the sending of multiple customer notices.

55 *See* Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Securities Act Release No. 11028 (Feb. 9, 2022) [87 FR 13524 (Mar. 9, 2022)] ("Investment Management Cybersecurity Proposal"); *see also* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Securities Act Release No. 11038 (Mar. 9, 2022) [87 FR 16590 (Mar. 23, 2022) ("Corporation Finance Cybersecurity Proposal").

56 *See infra* section II.G.

57 Regulation SCI is codified at 17 CFR 242.1000 through 1007. As described further below, while the overall nature of each cybersecurity-related proposal is similar given the topic, the scope of each proposal addresses different cybersecurity-related issues as they relate in different ways to different entities, types of covered information or systems, and products. *See* Cybersecurity Risk Management Proposed Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, Exchange Act Release No. 97142 (Mar. 15, 2023), ("Exchange Act Cybersecurity Proposal") and Regulation Systems Compliance and Integrity, Exchange Act Release No. 97143 (Mar. 15, 2023), ("Regulation SCI Proposal").

rulemaking proposals to determine whether those proposals might affect comments on this proposing release.

II. DISCUSSION

A. Incident Response Program Including Customer Notification

Security incidents can occur in different ways, such as through takeovers of online accounts by bad actors, improper disposal of customer information in areas that may be accessed by unauthorized persons, or the loss or theft of data that includes customer information. Whatever the means, unauthorized access to, or use of, customer information may result in misuse, exposure or theft of a customer's nonpublic personal information, which could result in substantial harm or inconvenience to individuals affected by a security incident. Exposure of customer information in a security incident, whether it results from unauthorized access to or use of customer information by an employee[58] or external actor,[59] could leave affected individuals

---

[58] For example, an employee might access and download confidential customer data to a personal server that is subsequently hacked by a third party. Once the customer data has been stolen, portions of the customer data could be posted on the Internet along with an offer to sell a larger quantity of stolen data in exchange for payment. *See, e.g.*, Commission Order, *In the Matter of Morgan Stanley Smith Barney LLC,* Release No. 34-78021 (June 8, 2016), *available at* https://www.sec.gov/litigation/admin/2016/34-78021.pdf (settled order) (finding that an employee misappropriated data regarding approximately 730,000 customer accounts, associated with approximately 330,000 different households, by accessing two of the firm's portals. The misappropriated data included personally identifiable information ("PII") such as customers' full names, phone numbers, street addresses, account numbers, account balances, and securities holdings).

[59] For example, unauthorized third parties could take over email accounts, resulting in exposure of customer information. An email account takeover occurs when an unauthorized third party gains access to the email account and, in addition to being able to view its contents, is also able to take actions of a legitimate user, such as sending and deleting emails or setting up forwarding rules. *See, e.g.*, Commission Order, *In the Matter of Cambridge Investment Research, Inc., et al.*, Release No. 34-92806 (Aug. 30, 2021) ("Cambridge Order"), *available at* https://www.sec.gov/litigation/admin/2021/34-92806.pdf (settled order) (finding that cloud-based email accounts of over 121 Cambridge independent contractor representatives were taken over by third parties resulting in the exposure of at least 2,177 customers' PII stored in the compromised email accounts and potential exposure of another 3,800 customers' PII); Commission Order*, In the Matter of Cetera Advisor Networks LLC, et al.*, Release No. 34-92800 (Aug. 30, 2021), *available at* https://www.sec.gov/litigation/admin/2021/34-92800.pdf (settled order) (finding that email accounts of over 60 Cetera personnel were taken over by unauthorized third parties resulting in the exposure of over 4,388 of Cetera customers' PII stored in the compromised email accounts); Commission Order, *In the Matter of KMS Financial Services, Inc.*, Release No. 34-92807 (Aug. 30, 2021) ("KMS Order"), *available at* https://www.sec.gov/litigation/admin/2021/34-92807.pdf (settled order) (finding that fifteen KMS

vulnerable to having their information further compromised.[60] Bad actors can use customer information to cause harm in a number of ways, such as by stealing customer identities to sell to other bad actors on the dark web,[61] publishing customer information on the dark web, using customer identities to carry out fraud themselves, or taking over a customer's account for malevolent purposes. For example, a bad actor could use compromised customer information such as login credentials (*e.g.*, a username and password), as part of an account takeover scheme to obtain unauthorized entry to a customer's online brokerage account, putting customer assets at risk for unauthorized fund transfers or trades.[62] Similarly, a bad actor could engage in new account fraud by using compromised customer information to establish a brokerage account

---

financial adviser email accounts were accessed by unauthorized third parties resulting in the exposure of customer records and information, including PII, of approximately 4,900 KMS customers).

60 Modes of compromise could include, for example, phishing or credential stuffing. "Phishing" is a means of gaining unauthorized access to a computer system or service by using a fraudulent or "spoofed" email to trick a victim into taking action, such as downloading malicious software or entering his or her log-in credentials on a fake website purporting to be the legitimate log-in website for the system or service, while "credential stuffing" is a means of gaining unauthorized access to accounts by automatically entering large numbers of pairs of log-in credentials that were obtained elsewhere. *See* Cambridge Order, *supra* note 59, at 3, n.5 and n.6.

For example, individuals affected by a security incident might receive phishing emails requesting them to wire funds to a bank account or enter PII to access a document, among other things. *See, e.g.*, KMS Order, *supra* note 59, at 4.

61 The "dark web" is a part of the internet that requires specialized software to access and is specifically designed to facilitate anonymity by obscuring users' identities, including by hiding users' internet protocol addresses. The anonymity provided by the dark web has allowed users to sell and purchase illegal products and services. *See, e.g., SEC v. Apostolos Trovias*, Case 1:21-cv-05925 (S.D.N.Y. filed July 9, 2021) Dkt. No. 1 (complaint) at 1-2, *available at* https://www.sec.gov/litigation/complaints/2021/comp-pr2021-122.pdf. The SEC obtained a final judgment against the defendant on July 19, 2022. *See* Litigation Release No. 25447 (July 21, 2022), *available at* https://www.sec.gov/litigation/litreleases/2022/judg25447.pdf.

62 *See, e.g.,* FINRA Regulatory Notice 20-32, *FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud* (Sept. 17, 2020), *available at* https://www.finra.org/rules-guidance/notices/20-32 (stating that FINRA recently observed an increase in fraudulent options trading being facilitated by account takeover schemes and the use of new account fraud); *see also* FINRA Regulatory Notice 20-13, *FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic* (May 5, 2020), *available at* https://www.finra.org/rules-guidance/notices/20-13 (stating that some firms have reported an increase in newly opened fraudulent accounts, and urging firms to be cognizant of the heightened threat of frauds and scams to which firms and their customers may be exposed during the COVID-19 pandemic).

without the customer's knowledge through identity theft. Once the bad actor has taken over the customer's account, or has opened a fraudulent new account, it could potentially use a separate account at another broker-dealer to trade against these accounts for profit, which could result in harm to the affected customer.[63]

To help protect against harms that may result from a security incident involving customer information, the Commission is proposing to amend the safeguards rule to require that covered institutions' safeguards policies and procedures include a response program for unauthorized access to or use of customer information, which would include customer notification procedures.[64] The proposed amendments would require the response program to be reasonably designed to detect, respond to, and recover from both unauthorized access to and unauthorized use of customer information (for the purposes of this release, an "incident").[65] As noted above, any instance of unauthorized access to or use of customer information would trigger a covered institution's incident response protocol. The amendments would also require that the response

---

[63] In 2017, the SEC charged an individual with engaging in an illegal brokerage account takeover and unauthorized trading scheme with at least one other person. The SEC's complaint alleged that, in furtherance of the scheme, the other person(s) accessed at least 110 brokerage accounts of unwitting accountholders, secretly and without authorization, and used those accounts to place securities trades that artificially affected the stock prices of various publicly traded companies. At or about the same time, the charged individual used his brokerage accounts to trade the same securities, generating profits by taking advantage of the artificial stock prices that resulted from the unauthorized trades placed in the victims' accounts. The complaint alleged that the individual generated at least $700,000 in illicit profits through his participation in the scheme by buying or selling stock in his brokerage accounts in his name at artificially low or high prices generated by the unauthorized trading of stock in the victims' accounts. *See SEC v. Joseph P. Willner*, Case 1:17-cv-06305 (E.D.N.Y. filed Oct. 30, 2017) (complaint), *available at* https://www.sec.gov/litigation/complaints/2017/comp-pr2017-202.pdf. In Oct. 2020, the U.S. District Court for the Eastern District of New York entered a final consent judgment against this individual for his role in the scheme. *See* Litigation Release No. 24947 (Oct. 19, 2020), *available at* https://www.sec.gov/litigation/litreleases/2020/lr24947.htm.

[64] *See* proposed rule 248.30(b)(3). For clarity, when the proposed amendments to the safeguards rule refer to "unauthorized access to or use", the word "unauthorized" modifies both "access" and "use."

[65] *See* proposed rule 248.30(b)(3). *See also infra* section II.C.1 for a discussion of "customer information."

program include procedures for notifying affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.[66]

In this regard, requiring covered institutions to have this type of incident response program could help mitigate the risk of harm to affected individuals stemming from such incidents. For example, having a response program should help covered institutions to be better prepared to respond to incidents, and providing notice to affected individuals should aid those individuals in taking protective measures that could mitigate harm that might otherwise result from unauthorized access to or use of their information. Further, a reasonably designed response program will help facilitate more consistent and systematic responses to customer information security incidents, and help avoid inadequate responses based on a covered institution's initial impressions of the scope of the information involved in the compromise. In addition, requiring the response program to address any incident involving customer information can help a covered institution better contain and control these incidents and facilitate a prompt recovery.

The amendments would require that a covered institution's response program include policies and procedures containing certain general elements, but would not prescribe specific steps a covered institution must take when carrying out incident response activities. Instead, covered institutions may tailor their policies and procedures to their individual facts and circumstances. We recognize that given the number and varying characteristics (*e.g.*, size, business, and complexity) of covered institutions, each such institution needs to be able to tailor its incident response program procedures based on its individual facts and circumstances. The proposed amendments therefore are intended to give covered institutions the flexibility to

---

[66] *See* proposed rule 248.30(e)(9) for the definition of "sensitive customer information." *See also infra* section II.A.4, which includes a discussion of "sensitive customer information." Notice would have to be provided unless 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 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.

address the general elements in the response program based on the size and complexity of the institution and the nature and scope of its activities.

Specifically, a covered institution's incident response program would be required to have written policies and procedures 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;[67]

(ii) take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information;[68] 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 the notification obligations 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, 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.[69]

The proposed response program is designed to further the objectives of the safeguards rule, particularly protecting against unauthorized access to or use of customer information. We have also proposed rules that would more broadly address general cybersecurity risks, with which the response program proposed in Regulation S-P is not inconsistent, as discussed in more

---

[67] *See* proposed rule 248.30(b)(3)(i). The term "customer information systems" would 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. *See* proposed rule 248.30(e)(6).

[68] *See* proposed rule 248.30(b)(3)(ii).

[69] *See* proposed rule 248.30(b)(3)(iii).

detail below.[70] Our recent proposals would require investment advisers, investment companies, and certain market entities[71] to adopt and implement written policies and procedures that require measures to detect, respond to, and recover from a cybersecurity incident.[72] The Investment Management Cybersecurity Proposal, including the cybersecurity response measures, is more broadly focused on investment advisers and investment companies and their operations. Among other objectives, the proposed measures would include policies and procedures reasonably designed to ensure the protection of adviser (or fund) information systems and adviser (or fund) information residing therein.[73] Similarly, the Exchange Act Cybersecurity Proposal, which includes cybersecurity response measures, is more broadly focused on Market Entities and their operations, and would include policies and procedures reasonably designed to ensure the protection of the Market Entities' information systems and the information residing on those systems.

The response program proposed in Regulation S-P, however, is narrowly focused and the required incident response policies and procedures should be specifically tailored to address unauthorized access to or use of customer information, including procedures for assessing the nature and scope of such incidents and identifying the customer information and customer information systems that may have been accessed or used without authorization, as well as taking steps to contain and control the incident to prevent further unauthorized access to or use of

---

70 *See infra* section II.G.1 - II.G.2, which addresses areas that are related between the Regulation SCI Proposal and the Exchange Act Cybersecurity Proposal, as well as with the Investment Management Cybersecurity Proposal, respectively.

71 The Exchange Act Cybersecurity Proposal rules would be applicable to "Market Entities" including: broker-dealers; clearing agencies; major security-based swap participants; the Municipal Securities Rulemaking Board; national securities exchanges; national securities associations (*i.e.*, FINRA); security-based swap data repositories; security-based swap dealers; and transfer agents (collectively, "Covered Entities") as well as broker-dealers that are non-Covered Entities. *See* Exchange Act Cybersecurity Proposal, *supra* note 57.

72 *See* Investment Management Cybersecurity Proposal, *supra* note 55; Exchange Act Cybersecurity Proposal, *supra* note 57.

73 *See* Investment Management Cybersecurity Proposal, *supra* note 55, at 13589 for definitions of "fund information system" and "fund information."

customer information. Given the risk of harm posed to customers and other affected individuals by incidents involving customer information, it is important that covered institutions' policies and procedures be reasonably designed to implement an incident response under these circumstances.

We request comment on the proposed rule's requirement that covered institutions' policies and procedures include an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including the following:

1. What best practices have commenters developed or become aware of with respect to the types of measures that can be implemented as part of an incident response program? Are there any measures commenters have found to be ineffective or relatively less effective? To the contrary, are there any measures that commenters have found to be effective, or relatively more effective?
2. Should we require the response program procedures to set forth a specific timeframe for implementing incident response activities under Regulation S-P? For example, should the procedures state that incident response activities, such as assessment and containment, should commence promptly, or immediately, once an incident has been discovered?
3. Are the proposed elements for the incident response program appropriate? Should we modify the proposed elements? For instance, should the rule prescribe more specific steps for incident response within the framework of the procedures, such as detailing the steps that an institution should take to assess the nature and scope of an incident, or to contain and control an incident? If so, please describe the steps and explain why they should be included. Alternatively, should the requirements for the incident response program be less prescriptive and more principles-based? If so, please describe how and why the requirements should be modified.

4. Are there additional or different elements that should be included in an incident response program? For example, should the rule require procedures for taking corrective measures in response to an incident, such as securing accounts associated with the customer information at issue? Should the rule require procedures for monitoring customer information and customer information systems for unauthorized access to or use of those systems, and data loss as it relates to those systems? Should the rule require procedures for identifying the titles and roles of individuals or departments (e.g., managers, directors, and officers) who should be responsible for overseeing, implementing, and executing the incident response program, as well as procedures to determine compliance? If additional or different elements should be added, please describe the element, and explain why it should be included in the response program.

5. Is the scope of the incident response program appropriate? For example, is the scope of the incident response program reasonably aligned with the vulnerability of the customer information at issue?

    - Should the incident response program be more limited in scope, so that it would only address incidents that involve unauthorized access to or use of a subset of customer information (*e.g.*, sensitive customer information)? If so, please explain the subset of customer information that should require an incident response program.
    - Alternatively, should the incident response program be more expansive in scope, so that it would cover additional activity beyond unauthorized access to or use of customer information? For example, should the incident response program address cybersecurity incident response and recovery at large (*i.e.*,

should the rule require covered institutions to have a response program reasonably designed to detect, respond to, and recover from a cybersecurity incident)?

1. Assessment

The Commission is proposing to require that the incident response program include procedures for: (1) assessing the nature and scope of any incident involving unauthorized access to or use of customer information, and (2) identifying the customer information systems and types of customer information that may have been accessed or used without authorization.[74] For example, a covered institution's assessment may include gathering information about the type of access, the extent to which systems or other assets have been affected, the level of privilege attained by any unauthorized persons, the operational or informational impact of the breach, and whether any data has been lost or exfiltrated.[75] Examining a range of data sources could shed light on the incident timeline, and assessing affected systems and networks could help to identify additional anomalous activity that might be adversarial behavior.[76]

---

[74] *See* proposed rule 248.30(b)(3)(i). The proposed requirements related to assessing the nature and scope of a security incident are consistent with the components of a response program as set forth in the Banking Agencies' Incident Response Guidance. *See* Banking Agencies' Incident Response Guidance, *supra* note 47, at 15752.

[75] *See* Cybersecurity and Infrastructure Security Agency ("CISA"), Cybersecurity Incident & Vulnerability Response Playbooks (Nov. 2021), at 10-13 ("CISA Incident Response Playbook"), *available at* https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf. While the CISA Incident Response Playbook specifically provides Federal agencies with a standard set of procedures to respond to incidents impacting "Federal Civilian Executive Branch" networks, it may also be useful for the purpose of strengthening cybersecurity response practices and operational procedures for public and private sector entities in addition to the Federal government. *See* CISA, Press Release, *CISA Releases Incident and Vulnerability Response Playbooks to Strengthen Cybersecurity for Federal Civilian Agencies* (Nov. 16, 2021), *available at* https://www.cisa.gov/news/2021/11/16/cisa-releases-incident-and-vulnerability-response-playbooks-strengthen. A list of the Federal Civilian Executive Branch agencies identified by CISA is available at https://www.cisa.gov/agencies. The National Institute for Standards and Technology ("NIST") defines "exfiltration" as "the unauthorized transfer of information from a system." *See* NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, Appendix A at 402 (Sept. 2020) *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[76] *See* CISA Incident Response Playbook, *supra* note 75, at 10-13. NIST defines "adversary" as

The assessment requirement is designed to require a covered institution to identify both the customer information systems and types of customer information that may have been accessed or used without authorization during the incident, as well as the specific customers affected, which would be necessary to fulfill the obligation to notify affected individuals. Covered institutions generally should evaluate and adjust their assessment procedures periodically, regardless of any specific regulatory requirement, to ensure they remain reasonably designed to accomplish their goals. In addition, assessment should help facilitate the evaluation of whether sensitive customer information has been accessed or used without authorization, which informs whether notice would have to be provided, as discussed below. A covered institution's assessment may also be useful for collecting other information that is required to populate the notice, such as identifying the date or estimated date of the incident, among other details. 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.

We request comment on the proposed rule's requirements related to assessing the nature and scope of any incident involving unauthorized access to or use of customer information, including the following:

6. Should we provide additional examples for consideration in assessing the nature and scope of an incident, beyond the examples provided above (*e.g.*, type of access, the extent to which systems or other assets have been affected, the level of privilege

---

"[a]n entity that is not authorized to access or modify information, or who works to defeat any protections afforded the information." *See* NIST Special Publication 800-107, *Recommendation for Applications Using Approved Hash Algorithms*, Section 3.1 Terms and Definitions, at 3 (Aug. 2012), *available at* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf.

attained by any unauthorized persons, the operational or informational impact of the breach, and whether any data has been lost or exfiltrated)?

7. Should we require that the assessment include the specific components referenced in the above question?

8. Should we require any specific training for personnel performing assessments of security incidents? Should the training have to encompass security updates and training sufficient to address relevant security risks?

9. Various rules applicable to certain entities require, among other things, the review, testing, verification, and/or amendment of policies and procedures at regular intervals.[77] Should we specifically require covered institutions to evaluate and adjust, as appropriate, the assessment procedures periodically in this rule? If so, how frequently should the evaluation occur? Should we require any testing (such as a practice exercise) of a covered institution's assessment process?

10. Would covered institutions expect to use third parties to conduct these assessments? If so, to what extent and in what manner? Should there be any additional or specific requirements for third parties that conduct assessments? Why or why not?

2. Containment and Control

The Commission is proposing to require that the response program have procedures for taking appropriate steps to contain and control a security incident, to prevent further unauthorized access to or use of customer information.[78] The objective of containment and control is to prevent additional damage from unauthorized activity and to reduce the immediate

---

[77] *See e.g.,* Rule 38a-1(a)(3) under the Investment Company Act; FINRA Rule 3120 (Supervisory Control System) and FINRA Rule 3130 (Annual Certification of Compliance and Supervisory Processes).

[78] *See* proposed rule 248.30(b)(3)(ii). These proposed requirements are consistent with the components of a response program as set forth in the Banking Agencies' Incident Response Guidance. *See* Banking Agencies' Incident Response Guidance, *supra* note 47, at 15752.

impact of an incident by removing the source of the unauthorized activity.[79] Covered institutions generally should evaluate and revise their containment and control procedures periodically, regardless of any specific regulatory requirement, to ensure they remain reasonably designed to accomplish their goals. 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. Some standards advise that after ensuring that all means of persistent access into the network have been accounted for, and any intrusive activity has been sufficiently contained, the artifacts of the incident should also be eliminated (*e.g.*, by removing malicious code or re-imaging infected systems) and vulnerabilities or other conditions that were exploited to gain unauthorized access should be mitigated.[80]

Additional eradication activities may include, for example, remediating all infected IT environments (*e.g.*, cloud, operational technology, hybrid, host, and network systems), resetting passwords on compromised accounts, and monitoring for any signs of adversary response to containment activities. 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.

---

[79] For a further discussion of the purposes and practices of such containment measures, *see generally* CISA Incident Response Playbook, *supra* note 76, at 14; *see also* Federal Financial Institutions Examination Council ("FFIEC"), Information Technology Examination Handbook - Information Security (Sept. 2016), at 52, *available at* https://ithandbook.ffiec.gov/media/274793/ffiec_itbooklet_informationsecurity.pdf.

[80] *See, e.g.*, CISA Incident Response Playbook, *supra* note 75, at 15.

We request comment on the proposed rule's requirement that the incident response program have procedures for taking appropriate steps to contain and control a security incident, including the following:

11. Should there be additional or more specific requirements for containing and controlling a breach of a customer information system? Should the rule prescribe specific minimum steps that need to be taken to remediate any identified weaknesses in customer information systems and associated controls? For example, should we require that a covered institution's containment or control activities be consistent with any current governmental or industry standards or guidance, such as standards disseminated by NIST, guidance disseminated by CISA, or others?[81]
12. Are the examples of steps that may be taken to contain and control an incident (*e.g.*, 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) appropriate? Are there any additional examples of steps that could be taken to contain and control an incident that should be provided?
13. Are the examples of remediation and eradication activities provided (*e.g.*, remediating all infected IT environments (such as cloud, operational technology, hybrid, host, and network systems, resetting passwords on compromised accounts, and monitoring for any signs of adversary response to containment activities) appropriate? Are there any additional examples of remediation or eradication activities that should be provided?

---

[81] Examples of such standards and guidance include the NIST Computer Security Incident Handling Guide (NIST Special Publication 800-61, Revision 2, *available at* https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final) and the CISA Incident Response Playbook, *supra* note 75, among others.

14. Should the rule require that a covered institution evaluate and revise its incident response plan following a customer information incident?

15. Various rules applicable to certain entities require, among other things, the review, testing, verification, and/or amendment of policies and procedures at regular intervals.[82] Should we specifically require covered institutions to evaluate and revise containment and control procedures related to preventing unauthorized access to or use of customer information periodically? If so, how frequently should the evaluation occur? For example, should a covered institution be required to evaluate and revise these containment and control procedures at least annually?

16. Who should be responsible for making decisions related to containment and control? Should the rule require covered institutions to designate specific personnel to be responsible for making decisions related to containment and control? For example, should a covered institution have to identify specific personnel with sufficient cybersecurity qualifications and experience to either determine if an incident has been contained or controlled themselves, or hire a third party who has the requisite cybersecurity and recovery expertise to perform containment and control functions? If so, what type of qualifications or experience are useful for informing decisions related to containment and control? Or should it be the same individuals who are designated to perform incident response and recovery related functions for cybersecurity incidents under the Investment Management Cybersecurity Proposal and the Exchange Act Cybersecurity Proposal?

3. Service Providers

---

[82] *See e.g.,* Rule 38a-1(a)(3) under the Investment Company Act; FINRA Rule 3120 (Supervisory Control System) and FINRA Rule 3130 (Annual Certification of Compliance and Supervisory Processes).

We understand that a covered institution may contract with third-party service providers to perform certain business activities and functions, for example, trading and order management, information technology functions, and cloud computing services, among others, in a practice commonly referred to as outsourcing.[83] As a result of this outsourcing, service providers may receive, maintain, or process customer information, or be permitted to access a covered institution's customer information systems. These outsourcing relationships or activities may expose covered institutions and their customers to risk through the covered institutions' service providers, including risks related to system resiliency and the ability of a service provider to protect customer information and systems (including service provider incident response programs). Moreover, a security incident at a service provider could lead to the unauthorized access to or use of customer information or customer information systems, which could potentially result in harm to customers. For example, a bad actor could use a service provider's access to a covered institution's systems to infiltrate the covered institution's network through a cybersecurity compromise in the supply chain,[84] which is a vector that can be used to conduct a data breach, and thereby gain unauthorized access to the covered institution's customer

---

[83] *See, e.g.*, Outsourcing by Investment Advisers, Investment Advisers Act Release No. 6176 (Oct. 26, 2022) [87 FR 68816 (Nov. 16, 2022)] ("Adviser Outsourcing Proposal"); FINRA Notice to Members 05-48, *Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers* (July 28, 2005), *available at* https://www.finra.org/rules-guidance/notices/05-48.

[84] NIST defines a "cybersecurity compromise in the supply chain" as "an occurrence within the supply chain whereby the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits is jeopardized. A supply chain incident can occur anywhere during the life cycle of the system, product or service." *See* NIST, Special Publication NIST SP 800-161r1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, Glossary at 299, *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf. According to NIST, key cybersecurity supply chain risks include risks from third-party service providers with physical or virtual access to information systems, software code, or intellectual property. *See* NIST, *Best Practices in Cyber Supply Chain Risk Management*, Conference Materials ("NIST Best Practices in Cyber Supply Chain Risk Management"), *available at* https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.

information and customer information systems through an initial compromise at the service provider.[85]

Under the proposed amendments, we propose to define the term "service provider" to mean any person or entity that is a third party and receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution.[86] This definition would include affiliates of covered institutions if they are permitted access to this information through their provision of services. The proposed scope is intended to help protect against the risk of harm that may arise from third-party access to a covered institution's customer information and customer information systems. For example, in 2015, Division of Examinations staff released observations following the examinations of some institutions' cybersecurity policies and procedures relating to vendors and other business partners, which revealed mixed results with respect to whether the firms incorporated requirements related to cybersecurity risk into their contracts with vendors and business partners.[87]

Given the potential for bad actors to target third parties with access to a covered institution's systems, it is important to help mitigate the risk of harm posed by security compromises that may occur at service providers. For example, a covered institution could retain a cloud service provider to maintain its books and records.[88] A security incident at this

---

85 For example, in a 2013 cyber supply chain attack, a bad actor breached the Target Corporation's network and was able to steal personal information for up to 70 million customers. The bad actor was able to gain a foothold in Target's network through a third-party vendor. *See* U.S. Senate, Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach*, Majority Staff Report (Mar. 26, 2014), *available at* https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883.

86 *See* proposed rule 248.30(e)(10).

87 *See* EXAMS, Cybersecurity Examination Sweep Summary, National Exam Program Risk Alert, Volume IV, Issue 4 (Feb. 3, 2015), at 4, *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

88 According to NIST, key cybersecurity supply chain risks include risks from third-party data storage or data aggregators. *See* NIST Best Practices in Cyber Supply Chain Risk Management, *supra* note 84.

cloud service provider that resulted in unauthorized access to or use of these books and records could create a risk of substantial harm to the covered institution's customers and trigger a need for notification to allow the affected customers to address this risk. Because service providers would be obligated to notify a covered institution in the event of security breaches involving customer information systems, as discussed below, this could potentially help covered institutions implement their own incident response protocol more quickly and efficiently after such breaches, which would include notifying affected individuals as needed.

The proposed amendments would require that a covered institution's incident response program include written policies and procedures that address the risk of harm posed by security compromises at service providers.[89] Specifically, these policies and procedures would require covered institutions, pursuant to a written contract between the covered institution and its service providers, to require service providers to take appropriate measures that are designed to protect against unauthorized access to or use of customer information.[90] Appropriate measures would include the obligation for a service provider to notify a covered institution as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security that results in unauthorized access to a customer information system maintained by the service provider, in order to enable the covered institution to implement its incident response program expeditiously.[91] In addition, we are not limiting entities that can provide customer notification for or on behalf of covered institutions. A covered institution may, as part of its incident response program, enter into a written agreement with its service provider to have the service provider notify affected individuals on its behalf in accordance with the notification obligations discussed below.[92] In that circumstance, the covered institution could delegate

---

89 *See* proposed rule 248.30(b)(5)(i).

90 *Id.*

91 *Id.*

92 *See* proposed rule 248.30(b)(5)(ii).

performance of its notice obligation to a service provider through written agreement, but the covered institution would remain responsible for any failure to provide a notice as required by the proposed rules, if adopted.[93]

We request comment on the proposed requirements related to service providers, including the following:

17. Should we modify the proposed definition of "service provider"? For example, should we exclude a covered institution's affiliates from the definition? Alternatively, should we define "service provider" in this rule in a manner similar to proposed rule 206(4)-11 under the Investment Advisers Act? Are there any other alternative definitions of "service provider" that should be used[94]?
18. Should there be additional or more specific requirements for entities that are included in the definition of "service providers?"
19. The proposed definition of service providers applies to entities that receive, maintain or process customer information, or are permitted access to a covered institution's customer information. Is this scope of activities appropriate? Should we exclude any of these activities? Should we include any other activities?
20. To what extent do covered institutions already have written policies and procedures that include contractually requiring service providers to take appropriate measures

---

[93] Covered institutions may delegate other functions to service providers, such as reasonable investigation to determine whether 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. Covered institutions would remain responsible for these functions even if they are delegated to service providers.

[94] *See* Adviser Outsourcing Proposal *supra* note 83. In proposed rule 206(4)-11, "service provider" would mean a person or entity that performs one or more covered functions, and is not a supervised person as defined in 15 U.S.C. 80b-2(a)(25) of the Investment Advisers Act, of the investment adviser. In the proposal, a "covered function" would mean a function or service that is necessary for the investment adviser to provide its investment advisory services in compliance with the Federal securities laws, and that, if not performed or performed negligently, would be reasonably likely to cause a material negative impact on the adviser's clients or on the adviser's ability to provide investment advisory services. In the proposal, a covered function would not include clerical, ministerial, utility, or general office functions or services.

designed to protect against unauthorized access to or use of customer information? For example, to what extent have contractual requirements been incorporated pursuant to an exception from Regulation S-P's opt-out requirements for service providers and joint marketing provided by 17 CFR 248.13, which is conditioned on having a contractual agreement prohibiting the service provider from disclosing or using customer information other than to carry out the purposes for which it is disclosed, or pursuant to Regulation S-ID's requirements[95] at 17 CFR 248.201(d)(2)(iii) to respond appropriately to any detected identity theft red flags to prevent and mitigate identity theft, and under 17 CFR 248.201(e)(4) to exercise appropriate and effective oversight of service provider arrangements?

21. The proposed rule would require policies and procedures requiring a covered institution, by contract, to require that its service providers take appropriate measures designed to protect against unauthorized access to or use of customer information, including notification to a covered institution in the event of certain types of breaches in security. Are there any contexts in which a written contract may be more feasible than others? Rather than using a contractual approach to implement this requirement that a covered institution take the required appropriate measures, should the rule require policies and procedures that require due diligence of or some type of reasonable assurances from its service providers? What should reasonable assurances include? For example, should they cover notification to the covered institution as soon as possible in the event of any breach in security resulting in unauthorized access to a customer information system maintained by

---

[95] *See* 17 CFR 248.201(d)(2)(iii) and (e)(4). As discussed further below, Regulation S-ID, among other things, requires financial institutions subject to the Commission's jurisdiction with covered accounts to develop and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with covered accounts, which must include, among other things, policies and procedures to respond appropriately to any red flags that are detected pursuant to the program. *See also infra* note 547.

the service provider to enable the covered institution to implement its response program? Are there other reasonable assurances we should require? Alternatively, should we only require disclosure of whether a covered institution has or does not have a written contract with service providers?

22. Should there be a written contract requirement for certain service providers and not others? For example, should the rule identify a sub-set of service providers as critical service providers and require a written agreement in those circumstances only, and if so, what service providers should be included?

23. Are there other methods that we should permit or require covered institutions to use to help ensure that service providers take appropriate measures that are designed to protect against unauthorized access to or use of customer information (for example, a security certification or representation)? Should we have different requirements for smaller covered institutions?

24. The proposed rule would require policies and procedures requiring a covered institution, by contract, to require its service providers to provide notification to a covered institution as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security resulting in unauthorized access to a customer information system maintained by the service provider. Is "as soon as possible, but no later than 48 hours after becoming aware of a breach" an appropriate timeframe for service providers to provide notification to a covered institution after such a breach occurs? Why or why not? Should we use a different timeframe such as "as soon as practicable"?

25. Is it appropriate to permit covered institutions to delegate providing notice to service providers? If service providers are permitted to provide notice on behalf of covered institutions, should there be additional or specific requirements for a

service provider that provides notification on behalf of a covered institution? If so, please describe those requirements and why they should be included.

26. The proposed rule would set forth that as part of its incident response program, a covered institution may enter into a written agreement with its service provider for the service provider to notify affected individuals on its behalf (*i.e.*, to delegate the notice functions required under the rule to service providers while remaining responsible for the notice obligation). Should we set forth that a covered institution may enter into a written agreement with its service provider for other potentially delegated functions as discussed in this proposal? For example, should we set forth that a covered institution may enter into a written agreement for delegating the performance of a reasonable investigation (*e.g.*, to determine whether 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 a service provider? Should we set forth that a covered institution may enter into a written agreement for delegating the performance of assessment activities, or containment and control activities, to a service provider? Additionally, is it appropriate for a service provider to assist with these functions, with the responsibility remaining with the covered institution? Why or why not?

27. To what extent do service providers sub-delegate functions provided in this proposal to third parties? If so, how should the rule address sub-delegations between service providers and third parties?

4. Notice to Affected Individuals

Under the proposed amendments, a covered institution must notify each affected individual whose sensitive customer information was, or was reasonably likely to have been, accessed or used without authorization, unless the covered institution has determined, after a reasonable investigation of the incident, 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 to each affected individual by a means designed to ensure that the individual can reasonably be expected to receive actual notice in writing. The notice must be provided as soon as practicable, but not later than 30 days, after the covered institution becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred.

a. Standard for Providing Notice

The proposed amendments would create an affirmative requirement for a covered institution to provide notice to individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.[96] These notices would be designed to give affected individuals an opportunity to respond to and remediate issues arising from an information security incident, such as monitoring credit reports for unauthorized activity, placing fraud alerts on relevant accounts, or changing passwords used to access accounts.[97] Such measures, when taken in a timely fashion, may help affected individuals avoid or mitigate the risk of substantial harm or inconvenience ("harm risk"),[98] and in an environment of expanded risk of cyber incidents,[99] taking such actions may be particularly important to protect individuals. Conversely, giving covered institutions greater discretion to determine whether and when to provide notices could jeopardize affected individuals' ability to evaluate the risk of harm posed by an incident and choose how to respond to and remediate it.

---

96 *See* proposed rule 248.30(b)(3)(iii). As noted above, a covered institution could delegate its responsibility for providing notice to an affected individual to a service provider, by contract, but the covered institution would remain responsible for any failure to provide a notice as required by the proposed rules. *See infra* section II.A.

97 Affected individuals include individuals with whom the covered institution has a customer relationship, or are individuals that are customers of other financial institutions whose information has been provided to the covered institution, and whose sensitive information was, or is reasonably likely to have been, accessed or used without authorization. *See infra* note 127.

98 *See infra* section II.A.4.e (Timing Requirements); *see also supra* note 7 and accompanying text (addressing environment of expanded risks).

99 *See supra* note 7 and accompanying text.

A covered institution would not have to provide notice if, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, it 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.[100] To be clear, although the incident response program would be required to address information security incidents involving any form of customer information, the notice requirement would only be triggered by unauthorized access to or use of sensitive customer information.[101] Unauthorized access to or use of sensitive customer information presents an increased risk of harm to the affected individual and accordingly is the appropriate trigger for customer notification.[102]

The proposed amendment is designed to permit covered institutions to rebut the affirmative presumption of notification based on a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information. Such an investigation would have to provide a sufficient basis for the determination that sensitive

---

100 *See* proposed rule 248.30(b)(3)(iii). In 2003, the Banking Agencies also proposed a similar standard for customer notification, though it was not ultimately adopted. *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 68 FR 47954 (Aug. 12, 2003) ("Banking Agencies' Proposing Release"). The proposed guidance stated that an institution should notify affected customers whenever it becomes aware of unauthorized access to sensitive customer information, unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur. *See id.* at 47960. In adopting the Banking Agencies' Incident Response Guidance, the Banking Agencies indicated that they wanted to give institutions greater discretion in determining whether to send notices, to avoid alarming customers with too many notices and not to require institutions to prove a negative. *See* the Banking Agencies' Incident Response Guidance, *supra* note 47, at 15743. We preliminarily believe, however, that a presumption that individuals would be timely provided with the information in the notifications would enable them to make their own determinations regarding the incident.

101 *See infra* section II.A.4.a and section II.A.4.b.

102 Customer information that is not disposed of properly could trigger the requirement to notify affected individuals under proposed rule 248.30(b)(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.

customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. In these limited circumstances, the proposed amendments would not require the covered institution to provide a notice.

In contrast, if a malicious actor has gained access to a customer information system and the covered institution simply lacked information indicating that any particular individual's data stored in that customer information system was or was not used in a manner that would result in substantial harm or inconvenience, a covered institution would not have a sufficient basis to make this determination.[103] In order to have a sufficient basis to determine that notice is not required, a covered institution's investigation would need to have revealed information sufficient for the institution to conclude 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.

For any determination that a covered institution makes that notice is not required, the covered institution generally should maintain a record of the investigation and basis for its determination.[104] Whether an investigation qualifies as reasonable would depend on the particular facts and circumstances of the unauthorized access or use. For example, unauthorized access that is the result of intentional intrusion by a bad actor may warrant more extensive investigation than inadvertent unauthorized access by an employee. The investigation may occur in parallel with an initial assessment and scoping of the incident and may build upon information generated from those activities, and the scope of the investigation may be refined by using

---

[103] *See also infra* section II.A.4.d (discussing the identification of affected individuals in such circumstances).

[104] Proposed rules 248.30(d), 240.17a-4, 240.17ad-7, 270.31a-1, 270.31a-2, and 275.204-2; *see infra* section II.C. The Commission's proposal includes an amendment to a CFR designation in order to ensure regulatory text conforms more consistently with section 2.13 of the Document Drafting Handbook. *See* Office of the Federal Register, Document Drafting Handbook (Aug. 2018 Edition, Revision 1.4, dated January 7, 2022), *available at* https://www.archives.gov/files/federal-register/write/handbook/ddh.pdf. In particular, the proposal is to amend the CFR section designation for Rule 17Ad-7 (17 CFR 240.17Ad-7) to replace the uppercase letter with the corresponding lowercase letter, such that the rule would be redesignated as Rule 17ad-7 (17 CFR 240.17ad-7).

available data and the results of ongoing incident response activities. Information related to the nature and scope of the incident may be relevant to determining the extent of the investigation, such as whether the incident is the result of internal unauthorized access or an external intrusion, the duration of the incident, what accounts have been compromised and at what privilege level, and whether and what type of customer information may have been copied, transferred, or retrieved without authorization.[105]

As discussed above, while some state laws currently include similar standards for providing notifications, the proposed rules would impose a minimum standard to help ensure all individuals would presumptively receive notifications.[106] Twenty-one states only require notice if, after an investigation, the institution finds that a risk of harm exists, and in eleven states, customer notification laws do not apply to entities subject to or in compliance with the GLBA.[107] We preliminarily believe that setting a minimum standard based on an affirmative presumption of notification appropriately balances the need for transparency (*i.e.*, the need for affected individuals to be informed so that they can take steps to protect themselves, including for example, by placing fraud alerts in credit reports) with concerns that the volume of notices that individuals would receive could erode their efficacy or lead to complacency by affected individuals. Notice of every incident could diminish the impact and effectiveness of the notice in a situation where enhanced vigilance is necessary.[108] Covered institutions likely would be able to

---

105 For example, depending on the nature of the incident, it may be necessary to consider how a malicious intruder might use the underlying information in light of current trends in identity theft.

106 A risk of harm provision under a particular state's rules may either (i) require a notice only after an entity performs a required analysis to determine that there is a reasonable likelihood of harm, or (ii) require notice unless a permitted analysis determines that there is no reasonable likelihood of harm. This latter approach is a stricter standard imposed by 22 states and is consistent with the standard we are proposing. *See* National Conference of State Legislatures, Security Breach Notification Laws, ("NCSL Security Breach Notification Law Resource"), *available at* https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

107 *See* NCSL Security Breach Notification Law Resource, *supra* note 106.

108 Eight states do not have risk of harm provisions, including California and Texas. *See* NCSL Security Breach Notification Law Resource, *supra* note 106. In these states, notices must generally be provided in all cases of a breach.

send a single notice that complies with multiple regulatory requirements, which may reduce the number of notices an individual receives. In addition, the proposed standard would help to improve security outcomes in general by incentivizing covered institutions to conduct more thorough investigations after an incident occurs, because a reasonable investigation provides the only means to rebut the presumption of notification. Reasonably designed policies and procedures generally should include that a covered institution would revisit a determination whether a notification is required based on its investigation if new facts come to light. For example, if a covered institution determines that risk of use in a manner that would result in substantial harm or inconvenience is not reasonably likely based on the use of encryption in accordance with industry standards at the time of the incident, but subsequently the encryption is compromised or it is discovered that the decryption key was also obtained by the threat actor, the covered institution generally should consider revisiting its determination.

We request comment on the proposed standard for notification to affected individuals, including the following:

28. The proposed standard requires providing notice to affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. Is the proposed standard for providing notification sufficiently clear? Is a standard of "reasonably likely" appropriate? Should the trigger for notification be a determination by a covered institution that the risk of unauthorized access or use of sensitive customer information has occurred or is "reasonably possible" which would suggest a more expansive standard than "likely"?

29. A covered institution can rebut the presumption of notification if it determines that, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, 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. Is this standard "not reasonably likely to be" for rebutting the presumption to notify the appropriate standard? Should the standard be "not reasonably possible"?

30. Should customer notification be required for any incident of unauthorized access to or use of sensitive customer information regardless of the risk of use in a manner that would result in substantial harm or inconvenience? Is there a risk that the volume of notices received under such a standard would inure affected individuals to notices of potentially harmful incidents and result in their not taking protective actions?

31. Do covered institutions expect to be able to perform reasonable investigations in order to rebut the notification presumption? Why or why not? Would it be helpful to include specific requirements for a reasonable investigation? Are there other factors that would influence whether a covered institution decides to conduct a reasonable investigation or notify individuals? If additional clarity would assist covered institutions in making these determinations, please explain.

32. Should we require a covered institution to revisit a determination that notification is not required based on its investigation if new facts come to light? If yes, should the rule provide specific requirements for a covered institution to revisit its determination?

33. Should we incorporate any additional aspects of the protections offered to individuals under state laws into the proposed rules? Alternatively, should any components of the proposal that offer additional protections to individuals beyond some states' laws be omitted? Please explain.

34. Under what scenarios would a covered institution be unable to comply with both the proposed rules and applicable state laws? Please explain.

35. Should the proposed rules be modified in order to help ensure covered institutions would not need to provide multiple notices in order to satisfy obligations under the proposed rules and similar state laws?

b. Definition of "Sensitive Customer Information"

We propose to define the term "sensitive customer information" to mean "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."[109] This definition is intended to cover the types of information that could most likely be used in a manner that would result in substantial harm or inconvenience, such as to commit fraud, including identify theft.[110] We do not believe that notification would be appropriate if unauthorized access to customer information is not reasonably likely to cause a harm risk because a customer is unlikely to need to take protective measures. Moreover, the large volume of notices that individuals might receive in the event of unauthorized access to such customer information could erode their efficacy. Accordingly, the proposed definition is limited to information that, if compromised, could create a "reasonably likely risk of substantial harm or inconvenience."[111]

The definition also provides examples of the types of information included within the definition of "sensitive customer information."[112] These examples include certain customer

---

[109] *See* proposed rule 248.30(e)(9)(i). Our proposed definition is limited to information identified with customers of financial institutions. *See* proposed rule 248.30(e)(5)(i); *infra* section II.C.1. Information subject to the safeguards rule, including the incident response program and customer notice requirements would be information pertaining to a covered institution's customers and to customers of other financial institutions that the other institutions have provided to the covered institution. *See* proposed rule 248.30(a); *infra* section II.C.1.

[110] *See supra* note 6 and accompanying text (noting increased risks of unauthorized access and use of personal information).

[111] *See* proposed rule 248.30(e)(9)(i).

[112] *See* proposed rule 248.30(e)(9)(ii). While the information cited in these examples is sensitive customer information, when that information is encrypted, it would not necessarily be sensitive customer information. That cipher text (*i.e.*, the data rendered in a format not understood by people or machines without an encryption key) may be analyzed as such (rather than as the decrypted sensitive customer information, *e.g.*, a Social Security number referenced in the

information identified with an individual that, without any other identifying information, could create a substantial risk of harm or inconvenience to an individual identified with the information.[113] For example, Social Security numbers alone, without any other information linked to the individual, would be sensitive because they have been used in "Social Security number-only" or "synthetic" identity theft. In this type of identity theft, a Social Security number, combined with identifying information of another real or fictional person, is used to create a new (or "synthetic") identity, which then may allow the malicious actor to, among other things, open new financial accounts.[114] A similar sensitivity exists with other types of identifying information that can be used alone to authenticate an individual's identity. A biometric record of a fingerprint or iris image would present a significant threat of account fraud, identity theft, or other substantial harm or inconvenience if the image is used to authenticate a customer of a financial institution.

The proposed definition also provides examples of combinations of identifying information and authenticating information that could create a harm risk to an individual identified with the information. These examples include information identifying a customer, such as a name or online user name, in combination with authenticating information such as a

---

examples provided in 248.30(e)(9)(ii)(A)(1)-(4) or in 248.30(e)(9)(ii)(B), and be determined not to be sensitive customer information). And as discussed *infra* note 119, a covered institution could consider the strength of the encryption and the security of the associated decryption key as factors in determining whether information is sensitive customer information. Accordingly, in certain circumstances, information that is an encrypted representation of, for example, a customer's Social Security number may not be sensitive customer information under the proposed definition.

[113] In this respect, our proposed definition is broader than the definition of "sensitive customer information" provided in the Banking Agencies' Incident Response Guidance. That definition includes a customer's name, address, or telephone number, only in conjunction with other pieces of information that would permit access to a customer account. Our proposed definition would also be broader than similar definitions of personal information used in some state statutes to determine the scope of information that, when subject to breaches, requires notification. *See infra* note 103 and accompanying text.

[114] *See, e.g., generally* Michael Kan, *More Crooks Tapping "Synthetic Identity Fraud" to Commit Financial Crimes*, PCMag (June 8, 2022), *available at* https://www.pcmag.com/news/more-crooks-tapping-synthetic-identity-fraud-to-commit-financial-crimes (describing recent increased frequency of synthetic identity fraud).

partial Social Security number, access code, or mother's maiden name. A mother's maiden name, for example, in combination with other identifying information, would present a harm risk because it may be so widely used for authentication purposes, even if the maiden name is not used as a password or security question at the covered institution. For these reasons, we are proposing that covered institutions should notify customers if this sensitive information is compromised.[115]

In determining whether the compromise of customer information could create a reasonably likely harm risk to an individual identified with the information, a covered institution could consider encryption as a factor.[116] Most states except encrypted information in certain circumstances, including, for example, where the covered institution can determine that the encryption offers certain levels of protection or the decryption key has not also been compromised.[117]

Specifically, 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 encryption in accordance with current industry standards 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.

---

115 While some states currently define the scope of personal information incurring a notification obligation in ways that generally align with our proposed definition of "sensitive customer information," at least 12 states generally do not include information we propose to include, such as identifying information that, in combination with authenticating information, would create a substantial risk of harm or inconvenience. *See* NCSL Security Breach Notification Law Resource, *supra* note 106.

116 We also considered a safe harbor from the definition of sensitive customer information for encrypted information. *See infra* section III.F.

117 *See e.g.,* R.I. Gen. Laws sec. 11-49.3-3(a) (defining a security breach as unauthorized access to or acquisition of certain "unencrypted, computerized data information," and defining "encrypted" as data transformed "through the use of a one hundred twenty-eight (128) bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key" unless the data was "acquired in combination with any key, security code, or password that would permit access to the encrypted data."). *See also* NCSL Security Breach Notification Law Resource, *supra* note 106.

Covered institutions may also reference commonly used cryptographic standards to determine whether encryption does, in fact, substantially impede the likelihood that the cipher text's compromise could create such risks.[118] As industry standards continue to develop in the future, covered institutions generally should review and update, as appropriate, their encryption practices.[119]

We request comment on the proposed rule's definition of sensitive customer information, including the following:

36. Should we broaden the proposed definition of "sensitive customer information" to cover additional information? Alternatively, should we remove some information covered under the proposed definition or conform the definition to the Banking Agencies' Incident Response Guidance?[120] Are there operational or compliance challenges to the proposed definition?

37. Should the rule limit the definition to information or data elements that alone or when linked would permit access to an individual's accounts? Should the rule specify the identifying information or data elements (*e.g.*, name, address, Social Security number, driver's license or other government identification number, account number, credit or debit card number)?

38. Is the proposed standard in the definition, which covers any component of customer information the compromise of which could create a "reasonably likely" risk of

---

118 For example, we understand that standards included in Federal Information Processing Standard Publication 140-3 (FIPS 140-3) are widely referenced by industry participants.

119 Encryption alone does not determine whether data is "sensitive customer information." For example, to the extent a covered institution determines that cipher text is itself sensitive customer information, for example because the encryption was compromised, an investigation of the incident would likely indicate that there is a risk that the compromised information could be used in a way to result in substantial harm or inconvenience. A covered institution may, however, still be able to determine that the risk of use in this manner is not reasonably likely for reasons unrelated to the encryption, including for example, because the cipher text was only momentarily compromised. *See generally supra* note 115 and accompanying text.

120 *See supra* note 116.

substantial harm or inconvenience, the appropriate standard? Do commenters believe that a different standard would be more appropriate for the proposed rule? For example, would a "reasonably foreseeable" standard be more appropriate, even if harm is not likely to occur? Instead of covering any component of customer information the compromise of which "could" create a reasonably likely risk of substantial harm or inconvenience, should the standard cover components of customer information that "would" create such risk?

39. Should we provide additional or alternative examples of what constitutes "sensitive customer information" in the rule text? Do covered persons or individuals widely use other pieces of information for authentication purposes, such that our examples should explicitly reference other authenticating or identifying information that, in combination, could create a harm risk?

40. Is encryption a relevant factor to a covered institution's determination of the harm risk? Could encrypted information not present such risks because of the current strength of the relevant encryption algorithm, even if this could change in the future because, for example, of future developments in quantum computing? If a covered institution determines that encrypted information is not sensitive customer information, should the covered institution be required to monitor decryption risk based on, for example, advances in technology or a future compromise of a decryption key? If such risks do arise, should a covered institution be required to deliver a notice for a past incident?

41. Do covered institutions' encryption practices commonly adhere to particular cryptographic standards, such as those included in FIPS 140-3?[121] Should we recognize adherence to particular standards as a requirement when determining that

---

[121] *See supra* note 121.

encryption is relevant to a covered institution's determination that cipher text's compromise would not create a reasonably likely harm risk to an individual identified with the information?

42. Should we except from the definition of "sensitive customer information" encrypted information, as certain states do? Should any such exception only apply in limited circumstances, including, for example, for certain types of information or where the covered institution can determine that the encryption offers certain levels of protection (including where the decryption key has not been compromised)? Would such an exception prevent individuals from receiving beneficial notifications, including where, for example, information could be easily decrypted? Should any other type of information be excepted?

c. Definition of "Substantial Harm or Inconvenience"

We propose to define "substantial harm or inconvenience" to mean "personal injury, or financial loss, expenditure of effort or loss of time that is more than trivial," and provide examples of included harms.[122] As noted above, Regulation S-P requires a covered institution's policies and procedures to be reasonably designed to, among other things, protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.[123] Although GLBA and the safeguards rule use the term "substantial harm or inconvenience," neither defines the term. The proposed definition is intended to include a broad range of financial and non-financial harms and inconveniences that may result from failure to safeguard sensitive customer information.[124] For example, a malicious

---

[122] *See* proposed rule 248.30(e)(11).

[123] *See supra* section I.A.

[124] Data security incidents may result in varied types of harms. *See generally* Alex Scroxton, *Data Breaches Are a Ticking Timebomb for Consumers*, ComputerWeekly.com (Feb. 9, 2021), *available at* https://www.computerweekly.com/news/252496079/Data-breaches-are-a-ticking-timebomb-for-consumers (citing a report in which consumers reported financial loss, stress, and loss of time among other effects, from data breaches); Jessica Guynn, *Anxiety, Depression and PTSD: The Hidden Epidemic of Data Breaches and Cyber Crimes*, USA TODAY (Feb. 24,

actor could use sensitive customer information about an individual to engage in identity theft or as a means of extortion by threatening to make the information public unless the individual agrees to the malicious actor's demands.[125] This could cause a customer to incur financial loss, or experience personal injury, such as physical harm or damaged reputation, or cause the customer to expend effort to remediate the breach or avoid losses. All of these effects would be included under our proposed definition.

The proposed definition would include all personal injuries due to the significance of their impact on customers. However, the proposed definition includes other harms or inconveniences only when they are, in each case, more than trivial. More than trivial financial loss, expenditure of effort, or loss of time would generally include harms that are likely to be of concern to customers and are of the nature such that customers are likely to take further action to protect themselves. By contrast, where a covered institution, its affiliate, or the individual simply changes the individual's account number as the result of an incident, this likely would be a trivial effect since it is not likely to be of concern to the individual or of the nature that the individual would be likely to take further action. Similarly, in the absence of additional effects, accidental access of information by an employee or other agent of the covered institution, its affiliate, or its service provider would also likely be trivial harms. We do not intend for covered institutions to design programs and incur costs to protect customers from harms of such trivial significance that the customer would be unconcerned with remediating. In this regard, our proposal to adopt standards that protect customers against substantial harm or inconvenience

---

2020), *available at* https://www.usatoday.com/story/tech/conferences/2020/02/21/data-breach-tips-mental-health-toll-depression-anxiety/4763823002/ (describing significant psychological effects of data breach incidents); Eleanor Dallaway, *#ISC2Congress: Cybercrime Victims Left Depressed and Traumatized*, INFO. SEC. (Sept. 12, 2016), *available at* https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/ (describing mental health effects of cybercrime).

125 The proposed definition of "sensitive customer information" is discussed *supra* in section II.A.4.b.

from failures to safeguard information is intended to be consistent with the purposes of the GLBA and Congress's goals.[126]

We request comment on the proposed rule's definition of substantial harm or inconvenience, including the following:

43. Should we expand the proposed definition of "substantial harm or inconvenience"? Alternatively, should we exclude some harms covered under the proposed definition? Should we exclude some smaller (but more than trivial) effects? If so, please explain why the rule should not address these potential harms.

44. Do commenters believe that the proposed rule should reference a term or terms other than "substantial" and "more than trivial" in describing the types of harms that meet our definition? Are additional or alternative clarifications needed? Is "more than trivial" the appropriate standard? Should we instead use a term such as "immaterial" or "insignificant"?

45. Would a numerical or other objective standard for "substantial" harm or inconvenience be appropriate, given the definition includes harms that would present substantial difficulty in quantifying, including damaged reputation? If so, please describe how such an objective standard could be designed and provide examples.

46. Should a harm that is a "personal injury," such as physical, emotional, or reputational harm, only be included in the proposed definition if it is more than "trivial," similar to our proposed treatment of financial loss, expenditure of effort or loss of time? Should the standard for a harm that is a "personal injury" be something other than "trivial?"

---

[126] *See* 15 U.S.C. 6801(a) (stating that it is "the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of these customers' nonpublic personal information."). *See also supra* note 26, *infra* note 160, and accompanying text.

47. What kinds of financial loss, expenditure of effort or loss of time would individuals likely be unconcerned with and/or likely not to try to mitigate? Please provide data, such as customer surveys, to support your response.

48. Are the rule's proposed examples of certain effects that would be unlikely to meet the definition of substantial harm or inconvenience appropriate? If so, please provide examples and explain why.

d. Identification of Affected Individuals

Under the proposed rules, covered institutions would be required to provide a clear and conspicuous notice to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.[127] We believe notices should be provided to these affected individuals because they would likely need the information contained in the notices to respond to and remediate the incident.

We understand, however, that notwithstanding a covered institution's determination to provide notices, the identification of affected individuals may be difficult in circumstances where a malicious actor has accessed or used information without authorization in a customer information system. It may, for example, be clear that a malicious actor gained access to the entire customer information system, but the covered institution may not be able to determine which specific individuals' data has been accessed or used. In such cases, we preliminarily believe that all individuals whose sensitive customer information is stored in that system should be notified so that they may have an opportunity to review the information in the required

---

[127] As discussed below, proposed rule 248.30(a) explains that the safeguards rule, including the response program and customer notification, applies to all customer information that pertains to individuals with whom the covered institution has a customer relationship or to customers of other financial institutions and has been provided to the covered institution. *See infra* section II.C.1. Accordingly, proposed rule 248.30(b)(3)(iii) and (b)(4)(i) refers to "affected individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization" rather than "customer." This is because the term "customer" is defined in section 248.3(j) as "a consumer that has a customer relationship with the [covered] institution," and would not include customers of financial institutions that had provided information to the covered institution (within the scope of proposed rule 248.30(a)).

notification, and take remedial action as they deem appropriate. For example, individuals may be more vigilant in reviewing account statements or place fraud alerts in a credit report. They may also be able to place a hold on opening new credit in their name, or take other protective actions. Accordingly, the proposed rule would require a covered institution that is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization to provide notice to all individuals whose sensitive customer information resides in the affected system that was, or was reasonably likely to have been, accessed or used without authorization.[128]

We request comment on the proposed rule's requirements for the identification of affected individuals, including the following:

49. Does the standard "all individuals whose sensitive customer information resides in the customer information system" adequately cover all of the individuals who are potentially at risk as a result of unauthorized access to or use of a customer information system? Should the rule require notice to additional or different individuals?

50. To the extent covered institutions are not able to determine which individuals are affected with certainty, should the rule require notice only to those individuals whose sensitive customer information was "reasonably likely" to have been accessed or used without authorization? Alternatively, should the rule require notice unless it is "unlikely" that the information was not accessed, or would some other standard be appropriate? Please address how any such standard would help ensure that all individuals potentially at risk because of unauthorized access to or use of the customer information system receive notice.

---

[128] *See* proposed rule 248.30(b)(4)(ii).

51. The proposed rule would require covered institutions to provide notice to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization, including customers of other financial institutions where information has been provided to the covered institution. Do covered institutions have the contact information for customers of other financial institutions necessary to send the notices as required? Alternatively, should the rule require only that a covered institution provide notices to their own customers or to the institution that provided the covered institution the sensitive customer information? Are there other operational or compliance challenges to identifying affected individuals? Would this requirement result in the practical effect of requiring covered institutions to send notices to all individuals potentially subject to a breach of their systems (regardless of whether they are a customer or not) due to the difficulty of determining an affected individual's status?

e. Timing Requirements

As proposed, the rule would require covered institutions to provide notices as soon as practicable, but not later than 30 days, after the covered institution becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred except under limited circumstances, discussed below.[129] We propose that covered institutions provide notices "as soon as practicable" to expeditiously notify individuals whose information is compromised, so that these individuals may take timely action to protect themselves from identity theft or other harm. The amount of time that would constitute "as soon as practicable" may vary based on several factors, such as the time required to assess, contain, and control the incident, and if the institution conducts one, the time required to investigate the likelihood the information could be used in a manner that would result in substantial harm or

---

[129] *See* proposed rule 248.30(b)(4)(iii).

inconvenience. For example, "as soon as practicable" may be longer with an incident involving a significant number of customers.

Consistent with the approach taken by many states, we have included an outside date to ensure that all covered institutions meet a minimum standard of timeliness. We preliminarily believe that a 30-day period after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred would permit customers to take actions in response to an incident, including by placing fraud alerts on relevant accounts or changing passwords used to access accounts.[130] The proposal's 30-day period would establish a shorter notification deadline than those currently used in 15 states, and would also offer enhanced protections to individuals in 32 states with laws that do not include an outside date.[131] At the same time, this 30-day period would generally allow sufficient time for covered institutions to perform their assessments, take remedial measures, conclude any investigation, and prepare notices.[132] Accordingly, we preliminarily believe that establishing a minimum requirement to provide notifications as soon as practicable, together with a 30-day outside date, strikes the appropriate balance between promoting timely notice to affected individuals and allowing institutions sufficient time to implement their incident response programs.[133]

---

130 Nineteen states provide an outside date for providing customer notification, which range from 30 to 90 days. *See, e.g.*, Colo. Rev. Stat. sec. 6-1-716(2) (providing that notifications be provided not later than thirty days after the date of determination that a security breach occurred); Conn. Gen. Stat. sec. 36a-701b (b)(1) (providing that notifications be provided not later than ninety days after the date of determination that a security breach occurred).

131 *See* NCSL Security Breach Notification Law Resource, *supra* note 106.

132 *See supra* section II.A.4.a (discussing the standard of notice, including that a covered institution must provide clear and conspicuous notice unless it 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 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* proposed rule 284.30(b)(4)(i).

133 An institution that has completed the required tasks and has undertaken an investigation before the end of the 30-day period would be required to provide notices to affected customers "as soon as practicable." For example, an incident of unauthorized access by a single employee to a limited set of sensitive customer information may take only a few days to assess, remediate, and investigate. In those circumstances we believe a covered institution generally should provide notices to affected individuals at the conclusion of those tasks and as soon as the notices have been prepared.

Further, the proposed requirement that a covered institution have written policies and procedures that provide for a systematic response to each incident also may facilitate the institution's preparation and ability to perform an assessment, remediation, and investigation in a timely manner and within the 30-day period required for providing customer notices. At the same time, a covered institution would be required to provide notice within 30 days after becoming aware that an incident occurred even if the institution had not completed its assessment or control and containment measures.

Similarly, the proposal would effectively impose a uniform 30-day notification time-period and would not generally provide for a notification delay. For example, when there is an ongoing internal or external investigation related to an incident involving sensitive customer information.[134] On-going internal or external investigations – which often can be lengthy – on their own would not provide a basis for delaying notice to customers that their sensitive customer information has been compromised.[135] Additionally, any such delay provision could undermine timely and uniform customer notification that customers' sensitive customer information has been compromised, as investigations and resolutions of incidents may occur over an extended period of time and may vary widely in timing and scope.

At the same time, we recognize that a delay in customer notification may facilitate law enforcement investigations aimed at apprehending the perpetrators of the incident and preventing future incidents. Many states have laws that either mandate or allow entities to delay providing customer notifications regarding an incident if law enforcement determines that notification may impede its investigation.[136] The principal function of such a delay would be to allow a law

---

[134] Internal investigation refers to an investigation conducted by a covered institution or a third party selected by a covered institution. An external investigation refers to any investigation not conducted by, or at the request of, a covered institution.

[135] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018) [83 FR 8166, 8169 (Feb. 26, 2018)].

[136] Of the 40 states that allow entities to delay providing notices to individuals for law enforcement investigations, 11 deem entities to be in compliance with state notification laws if the entity is

enforcement or national security agency to keep a cybercriminal unaware of their detection.

The proposed rule would allow a covered institution to delay providing notice after receiving a written request from the Attorney General of the United States that the notice required under this rule poses a substantial risk to national security.[137] The covered institution may delay such a notice for an initial period specified by the Attorney General of the United States, but not for longer than 15 days. The notice may be delayed an additional 15 days if the Attorney General of the United States determines that the notice continues to pose a substantial risk to national security. This would allow a combined delay period of up to 30 days, upon the expiration of which the covered institution must provide notice immediately.

A covered institution, in certain instances, may be required to notify customers under the proposal even though that covered institution could have separate delay reporting requirements under a particular state law. On balance, it is our current view that timely customer notification would allow the customer to take remedial actions and, thereby, would justify providing only for a limited delay.[138]

We request comment on the proposed rule's notification timing requirements, including the following:

52. Does this proposed requirement provide covered institutions with sufficient time to perform assessments, collect the information necessary to include in customer notices, perform an investigation if appropriate, and provide notices? Alternatively, does the proposed "as soon as practicable" or 30 day outside date provide too much

---

subject to or in compliance with GLBA, and nine states mandate the delay of notices to individuals for law enforcement investigations, with forty states permitting such delays. *See* NCSL Security Breach Notification Law Resource, *supra* note 106. *See supra* note 14 for information regarding the interaction between Regulation S-P and state laws.

137 Any such written request from the Attorney General of the United States would be subject to the recordkeeping requirements for covered institutions discussed in section II.D.

138 For example, after timely notice of a breach, individuals can take important steps to safeguard their information, including changing passwords, freezing their accounts, and putting a hold on their credit.

time? Should the rule require institutions to provide notice "as soon as possible," for example? Should the rule provide parameters to define "as soon as practicable," "as soon as possible," "as soon as reasonably practicable" or an alternate standard? If so, please describe the parameters or other standard. Should the rule require less time for an outside date, such as 10, 15, or 20 days? Should the rule provide more time for an outside date, such as 45, 60, or 90 days? Please be specific on the appropriate outside date and the basis for the shorter or longer time period. Also, please specify the potential costs and benefits to a different outside date.

53. Should the proposed timing requirement begin to run upon an event other than "becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred"? Should the timing requirement begin to run, for example, after the covered institution "reasonably should have been aware" of the incident or, alternatively, after completing its assessment of the incident or containment? If the timing requirement should begin upon "becoming aware that that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred," should we provide covered institutions with examples of what would constitute becoming aware?

54. Should the proposed rules incorporate any exceptions from the timing requirement that would allow for delays under limited circumstances? If so, what restrictions or conditions should apply to any such delay and why?

55. Are there other challenges to meeting the proposed timing requirements, including the requirement to provide notices within 30 days of becoming aware of the incident? If yes, please describe.

56. What operational or compliance challenges arise from the proposed limited delay for notice or its expiration? Should the proposed rule have a different delay for notice, for example, by providing that the Commission shall allow covered

institutions to delay notification to customers where any law enforcement agency requests such a delay from the covered institution? If so, what restrictions or conditions should apply to any such law enforcement delay, for example, a certification, or a different outside time limit on the delay?

f. Notice Contents and Format

We are proposing to require that notices include key information with details about the incident, the breached data, and how affected individuals could respond to the breach to protect themselves. This requirement is designed to help ensure that covered institutions provide basic information to affected individuals that would help them avoid or mitigate substantial harm or inconvenience.

More specifically, some of the information required, including information regarding a description of the incident, type of sensitive customer information accessed or used without authorization, and what has been done to protect the sensitive customer information from further unauthorized access or use, would provide customers with basic information to help them understand the scope of the incident and its potential ramifications.[139] We also propose to require covered institutions to include contact information sufficient to permit an affected individual to contact the covered institution to inquire about the incident, including 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, so that individuals can more easily seek additional information from the covered institution.[140] All of this information may help an individual assess the risk posed and whether to take additional measures to protect against harm from unauthorized access or use of their information.

---

139 *See* proposed rule 248.30(b)(4)(iv)(A) – (B).

140 *See* proposed rule 248.30(b)(4)(iv)(D). A method or means equivalent to email generally, for example, includes an internet webpage easily allowing for the submission of inquiries.

Similarly, if the information is reasonably possible to determine at the time the notice is provided, information regarding the date of the incident, the estimated date of the incident, or the date range within which the incident occurred would help customers understand the circumstances related to the breach.[141] We understand that a covered institution may have difficulty determining a precise date range for certain incidents because it may only discover an incident well after an initial time of access. As a result, similar to the approach taken by California, the covered institution would only be required to include a date, or date range, if it is possible to determine at the time the notice is provided.[142]

Finally, we propose that covered institutions include certain information to assist individuals in evaluating how they should respond to the incident. Specifically, if the individual has an account with the covered institution, the proposed rule would require inclusion of a recommendation that the customer review account statements and immediately report any suspicious activity to the covered institution.[143] The proposed rule would also require covered institutions to explain what a fraud alert is and how an individual may place a fraud alert in credit reports.[144] Further, the proposed rule would require inclusion of a recommendation that the individual periodically obtain credit reports from each nationwide credit reporting company and have information relating to fraudulent transactions deleted, as well as explain how a credit

---

141 *See* proposed rule 248.30(b)(4)(iv)(C).

142 *See* Cal. Civ. Code sec. 1798.29(d)(2).

143 *See* proposed rule 248.30(b)(4)(iv)(E).

144 *See* proposed rule 248.30(b)(4)(iv)(F). We recognize that, under the Fair Credit Reporting Act (15 U.S.C. 1681a(d)), individuals may obtain "consumer reports" from consumer reporting agencies. Nevertheless, we refer to "credit reports" in proposed rule 248.30(b)(4)(iv)(G), in part, because the Banking Agencies' Incident Response Guidance also includes a requirement that notices include a recommendation that customers obtain "credit reports," and in part, because we believe individuals would generally be more familiar with this term than the term "consumer reports." *See, e.g.,* Consumer Financial Protection Bureau ("CFPB"), *Check your credit*, https://www.consumerfinance.gov/owning-a-home/prepare/check-your-credit/ (explaining how to check credit reports); CFPB, *Credit reports and scores*, https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores/ (explaining how to understand credit reports and scores, how to correct errors and improve a credit record).

report can be obtained free of charge.[145] In particular, information addressing potential protective measures could help individuals evaluate how they should respond to the incident. We also propose for notices to include information regarding FTC and usa.gov guidance on 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.[146] This would give individuals resources for additional information regarding how they can respond to an incident.

We propose that covered institutions should be required to provide the information specified in proposed rule 248.30(b)(4)(iv) in each required notice. While we recognize that relevant information may vary based on the facts and circumstances of the incident, we believe that customers would benefit from the same minimum set of basic information in all notices. We propose, therefore, to permit covered institutions to include additional information, but the rule would not permit omission of the prescribed information in the notices provided to affected individuals.

The proposed rule would require covered institutions to provide the notice in a clear and conspicuous manner and by means designed to ensure that the customer can reasonably be expected to receive actual notice in writing.[147] Notices, therefore, would be required to be reasonably understandable and designed to call attention to the nature and significance of the information required to be provided in the notice.[148] Accordingly, to the extent that a covered institution includes information in the notice that is not required to be provided to customers under the proposed rules or provides notice contemporaneously with other disclosures, the

---

145 *See* proposed rule 248.30(b)(4)(iv)(G)-(H).

146 *See* proposed rule 248.30(b)(4)(iv)(I). *See, e.g.,* Identity Theft: How to Protect Yourself Against Identity Theft and Respond if it Happens, *available at* https://www.usa.gov/identity-theft.

147 *See* proposed rule 248.30(b)(4)(i); *see also* 17 CFR 248.9(a) (delivery requirements for privacy and opt out notices) and 17 CFR 248.3(c)(1) (defining "clear and conspicuous").

148 *See* 17 CFR 248.3(c)(2) (providing examples explaining what is meant by the terms "reasonably understandable" and "designed to call attention").

covered institution would still be required to ensure that the notice is designed to call attention to the important information required to be provided under the proposed rule; additional information generally should not prevent covered institutions from presenting required information in a clear and conspicuous manner. The requirement to provide notices in writing, further, would ensure that customers receive the information in a format appropriate for receiving important information, with accommodation for those customers who agree to receive the information electronically. This proposed requirement to provide notice "in writing" could be satisfied either through paper or electronic means, consistent with existing Commission guidance on electronic delivery of documents.[149] Notification in other formats, including, for example, by a recorded telephone message, may not be retained and referenced as easily as a notification in writing. These requirements would help ensure that customers are provided notifications and alerted to their importance.

We request comment on the notification content, format, and delivery requirements, including the following:

57. Should we require that notices include additional information? If so, what specific information should we include? Please explain why any recommended additional information would be important to include.

58. Is there prescribed notice information that we should eliminate or revise? Please explain. For example, should we add information about security freezes on credit reports, and should that replace fraud alert information? Should the required information on the notice to assist individuals in evaluating how they should respond to the incident be replaced? Please explain. For example, should the notice instead be required to include an appropriate website that describes then-

---

149 *See* Use of Electronic Media by Broker Dealers, Transfer Agents, and Investment Advisers for Delivery of Information; Additional Examples Under the Securities Act of 1933, Securities Exchange Act of 1934, and Investment Company Act of 1940, 61 FR 24644 (May 15, 1996); Use of Electronic Media, 65 FR 25843 (May 4, 2000).

current best practices in how to respond to an incident? Are there other websites, for example, IdentityTheft.gov, that should be included in the notice?

59. Should some of the information we propose to include in the notices only be required in limited circumstances? For example, should we only require including information relating to credit reports if the underlying incident relates to access or use of a subset of sensitive customer information (perhaps only information of a particular financial nature)? Should covered institutions be able to determine whether to provide certain information "as appropriate" on a case-by-case basis? If so, please explain which information and why.

60. In what other formats, if any, should we permit covered institutions to provide notices? What formats do covered institutions customarily use to communicate with individuals (*e.g.*, text messages or some other abbreviated format that might require the use of hyperlinks) and for which types of communications are those formats generally used? To the extent we allow such additional formats, would such notices adequately signal the significance of the information to the individual—or otherwise present disadvantages to covered institutions or individuals?

61. The proposed rule amendments would require that covered institutions provide certain contact information sufficient to permit an individual to contact the covered institution to inquire about the incident. Should we require additional or different contact information? Is the required contact information appropriate or would a general customer service number suffice? Should the amendments also require that covered institutions ensure that they have reasonable policies and procedures in place, including trained personnel, to respond appropriately to customer inquiries and requests for assistance?

62. Should we require that covered institutions include specific and standardized information about steps to protect against identity theft, instead of requiring inclusion of information about online guidance from the FTC and usa.gov?

63. Should we require that covered institutions reference "consumer reports" instead of "credit reports" in notifications under the proposed rules? Would individuals be more familiar with the term "credit report"?

64. To the extent that a covered institution determines it is not reasonably possible to provide in the notice information regarding the date of the incident, the estimated date of the incident, or the date range within which the incident occurred, should that financial institution be required to state this to customers? In addition, should the institution be required to state why it is not possible to make such a determination?

65. Should the notice require that covered institutions describe what has been done to protect the sensitive customer information from further unauthorized access or use? Would this description provide a roadmap for further incidents? If yes, is there other information rather than this description that may help an individual understand what has been done to protect their information?

66. Should we incorporate other prescriptive formatting requirements (*e.g.*, length of notice, size of font, etc.) for the notice requirement under the proposed rules?

67. Should we require covered institutions to follow plain English or plain writing principles?

B. Remote Work Arrangement Considerations

Following the onset of the COVID-19 pandemic in the United States in 2020, the use of remote work arrangements has expanded significantly throughout the labor force. The U.S. Census Bureau recently announced that the number of people primarily working from home

tripled between 2019 and 2021, from 5.7% to 17.9% of all workers.[150] In the financial services industry specifically, the Bureau of Labor Statistics found in its 2021 Business Response Survey that firms reported 27.5% of jobs in the industry currently involve full-time telework, with a total of 45% of jobs involving teleworking "at least some of the time."[151]

Although recent reports indicate that a growing number of workers are returning to the office,[152] as certain members of the securities industry have previously noted, when covered institutions permit their own employees to work from remote locations, rather than one of the firm's offices, it raises particular compliance questions under Regulation S-P.[153] In the case of the proposed rule, a covered institution's policies and procedures under the safeguards rule would need to be reasonably designed to ensure the security and confidentiality of customer information, protect against any threats or hazards to the security or integrity of customer information, and protect against the unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.[154] Similarly, under the

---

150 Press Release, *U.S. Census Bureau releases new 2021 American Community Survey 1-year estimates for all geographic areas with populations of 65,000 or more* (Sept.15, 2022), *available at* https://www.census.gov/newsroom/press-releases/2022/people-working-from-home.html#:~:text=SEPT.,by%20the%20U.S.%20Census%20Bureau.

151 Bureau of Labor Statistics, *Telework during the COVID-19 pandemic: estimates using the 2021 Business Response Survey* (Mar. 2022), *available at* https://www.bls.gov/opub/mlr/2022/article/telework-during-the-covid-19-pandemic.htm#_edn6.

152 *See* Joseph Pisiani and Kailyn Rhone, *U.S. Return-to-Office Rate Rises Above 50% for First Time Since Pandemic Began*, Wall Street Journal (Feb. 1, 2023), *available at* https://www.wsj.com/articles/u-s-return-to-office-rate-rises-above-50-for-first-time-since-pandemic-began-11675285071.

153 *See e.g.,* Letter from Michael Decker, Senior Vice President, Bond Dealers of America, to Jennifer Piorko Mitchell, Office of the Corporate Secretary, FINRA, re FINRA Regulatory Notice 20-42 (Feb. 16, 2021), *available at* https://www.finra.org/sites/default/files/NoticeComment/Bond%20Dealers%20of%20America%20%5BMichael%20Decker%5D%20-%20FINRA_COVID_lessons_final.pdf; letter from Kelli McMorrow, Head of Government Affairs, American Securities Association, to Jennifer Piorko Mitchell, Office of the Corporate Secretary, FINRA, re FINRA Regulatory Notice 20-42 (Feb. 16, 2021), *available at* https://www.finra.org/sites/default/files/NoticeComment/American%20Securities%20Association%20%5BKelli%20McMorrow%5D%20-%202021.02.16%20-%20ASA%20FINRA%20Covid%20Lessons%20Learned.pdf.

154 *See* proposed rule 248.30(b)(2).

proposed amendments to the disposal rule, covered institutions, other than notice-registered broker-dealers, would need to adopt and implement written policies and procedures under the disposal rule that address the proper disposal of consumer information and customer information according to a standard of taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.[155] In satisfying each of these proposed obligations, covered institutions will need to consider any additional challenges raised by the use of remote work locations within their policies and procedures.

In light of these considerations, we request comment on whether the remote work arrangements of the personnel of covered institutions should be addressed under both the safeguards rule and the disposal rule, including as to the following:

68. Should the proposed safeguards rule and/or the proposed disposal rule be amended in any way to account for the use of remote work arrangements by covered institutions? If so, how? How would such amendments impact the costs and benefits of the proposed rule?

69. Are there any additional costs and/or benefits of the proposed rule related to remote work arrangements that the Commission should be aware of? If so, in particular, how would those be impacted by whether or not remote work arrangements by covered institutions have increased, decreased, or remained the same? If so, please explain, and please provide any data available.

70. Are there any specific aspects of the proposed safeguards rule or the disposal rule, relating to compliance with either rule where the covered institution permits employees to work remotely, on which the Commission should provide guidance to covered institutions? If so, please explain.

---

155 *See* proposed rule 240.30(c).

C. Scope of Information Protected under the Safeguards Rule and Disposal Rule

The Commission adopted the safeguards rule and the disposal rule at different times under different statutes – respectively, the GLBA and the FACT Act – that differ in the scope of information they cover. We are proposing to broaden and more closely align the information covered by the safeguards rule and the disposal rule by applying the protections of both rules to "customer information," a newly defined term. We also propose to add a new section that describes the extent of information covered under both rules, which includes nonpublic personal information that a covered institution collects about its own customers and that it receives from a third party financial institution about a financial institution's customers.

We preliminarily believe the scope of information protected by the safeguards rule and the disposal rule should be broader and more closely aligned to provide better protection against unauthorized disclosure of personal financial information, consistent with the purposes of the GLBA[156] and the FACT Act.[157] Applying both the safeguards rule and the disposal rule to a more consistent set of defined "customer information" also could reduce any burden that may have been created by the application of the safeguards rule and the disposal rule to different scopes of information. Further, protecting nonpublic personal information of customers that a financial institution shares with a covered institution furthers congressional policy to protect personal financial information on an ongoing basis.[158] Applying the safeguards rule and the

---

156 The Commission has "broad rulemaking authority" to effectuate "the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of these customers' nonpublic personal information." *Trans Union LLC v. FTC*, 295 F.3d 42, 46 (D.C. Cir. 2002) (quoting 15 U.S.C. 6801(a)).

157 The disposal rule was intended to reduce the risk of fraud or related crimes, including identity theft, by ensuring that records containing sensitive financial or personal information are appropriately redacted or destroyed before being discarded. *See* 108 Cong. Rec. S13,889 (Nov. 4, 2003) (statement of Sen. Nelson).

158 *See* 15 U.S.C. 6801(a) ("It is the policy of the Congress that each financial institution has an affirmative *and continuing obligation* to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.") (emphasis added).

disposal rule to customer information that a covered institution receives from other financial institutions should ensure customer information safeguards are not lost because a third party financial institution shares that information with a covered institution.

1. Definition of Customer Information

Currently, Regulation S-P's protections under the safeguards rule and disposal rule apply to different, and at times overlapping, sets of information.[159] Specifically, as required under the GLBA, the safeguards rule requires broker-dealers, investment companies, and registered investment advisers (but not transfer agents) to maintain written policies and procedures to protect "customer records and information,"[160] which is not defined in the GLBA or in Regulation S-P. The disposal rule requires every covered institution properly to dispose of "consumer report information," a different term, which Regulation S-P defines consistently with the FACT Act provisions.[161]

To align more closely the information protected by both rules, we propose to amend rule 248.30 by replacing the term "customer records and information" in the safeguards rule with a newly defined term "customer information" and by adding customer information to the coverage of the disposal rule.

---

159 *See* Disposal Rule Adopting Release, *supra* note 32, at 69 FR 71323 n.13.

160 *See* 17 CFR 248.30; 15 U.S.C. 6801(b)(1).

161 17 CFR 248.30(b)(2). Section 628(a)(1) of the FCRA directed the Commission to adopt rules requiring the proper disposal of "consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose." 15 U.S.C. 1681w(a)(1). Regulation S-P currently uses the term "consumer report information" and defines it to mean a record in any form about an individual "that is a consumer report or is derived from a consumer report." 17 CFR 248.30(b)(1)(ii). "Consumer report" has the same meaning as in section 603(d) of the Fair Credit Reporting Act (15 U.S.C. 1681(d)). 17 CFR 248.30(b)(1)(i). We are proposing to change the term "consumer report information" currently in Regulation S-P to "consumer information" (without changing the definition) to conform to the term used by other Federal financial regulators in their guidance and rules. *See, e.g.* 16 CFR 682.1(b) (FTC); 17 CFR 162.2(g) (CFTC); 12 CFR Appendix B to Part 30: Interagency Guidelines Establishing Information Security Standards ("OCC Information Security Guidance"), at I.C.2.b; 12 CFR Appendix D-2 to Part 208 ("FRB Information Security Guidance"), at I.C.2.b.

For covered institutions other than transfer agents,[162] the proposed rule would define "customer information" to encompass any record containing "nonpublic personal information" (as defined in Regulation S-P) about "a customer of a financial institution," whether in paper, electronic or other form that is handled or maintained by the covered institution or on its behalf.[163] This definition in the coverage of the safeguards rule is intended to be consistent with the objectives of the GLBA, which focuses on protecting "nonpublic personal information" of those who are "customers" of financial institutions.[164] The proposed definition would also conform more closely to the definition of "customer information" in the safeguards rule adopted by the FTC.[165]

Additionally, adding customer information to the coverage of the disposal rule is also intended to be consistent with the objectives of the GLBA. Under the GLBA, an institution has a "continuing obligation" to protect the security and confidentiality of customers' nonpublic personal information.[166] The proposed rule clarifies that this obligation continues through disposal of customer information. The proposed rule is also intended to be consistent with the objectives of the FACT Act. The FACT Act focuses on protecting "consumer information," a

---

162 We propose a separate definition of "customer information" applicable to transfer agents. *See infra* section II.C.3.

163 *See* proposed rule 248.30(e)(5)(i). As noted below in note 175, transfer agents typically do not have consumers or customers for purposes of Regulation S-P because their clients generally are not individuals, but are the issuer in which investors, including individuals, hold shares. With respect to a transfer agent registered with the Commission, under the proposal *customer* means any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as transfer agent. *See* proposed rule 248.30(e)(4)(ii).

164 *See* 15 U.S.C. 6801(a).

165 *See* 16 CFR 314.2(d) (FTC safeguards rule defining "customer information" to mean "any record containing nonpublic personal information, as defined in 16 CFR 313.3(n) about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates"). The proposed rules would not require covered institutions to be responsible for their affiliates' policies and procedures for safeguarding customer information because we believe that covered institutions affiliates generally are financial institutions subject to the safeguards rules of other Federal financial regulators.

166 *See* 15 U.S.C. 6801(a).

category of information that will remain within the scope of the disposal rule.[167] Adding customer information to the disposal provisions will simplify compliance with the FACT Act by eliminating an institution's need to determine whether its customer information is also consumer information subject to the disposal rule. Institutions should also be less likely to fail to dispose of consumer information properly by misidentifying it as customer information only. In addition, including customer information in the coverage of the disposal rule would conform the rule more closely to the Banking Agencies' Safeguards Guidance.[168] These proposed amendments are intended to be consistent with the Commission's statutory mandates under the GLBA and the FACT Act to adopt final financial privacy regulations and disposal regulations, respectively, that are consistent with and comparable to those adopted by other Federal financial regulators.[169]

We request comment on the proposed definition of "customer information," including the following:

71. Is the proposed definition of "customer information," which includes any records containing nonpublic personal information about a customer of a financial institution that is handled or maintained by the covered institution or on its behalf, too narrow? If so, how should we expand the definition? Should the definition also

---

[167] *See* 15 U.S.C. 1681w(a)(1) *and* proposed rule 248.30(c)(1). "Consumer information" is not included within the scope of the safeguards rule, except to the extent it overlaps with any "customer information," because the safeguards rule is adopted pursuant to the GLBA and therefore is limited to information about "customers."

[168] *See, e.g.*, OCC Information Security Guidance, *supra* note 161 (OCC guidelines providing that national banks and Federal savings associations' must develop, implement, and maintain appropriate measures to properly dispose of customer information and consumer information."); FRB Information Security Guidance, *supra* note 161 (similar Federal Reserve Board provisions for state member banks).

[169] *See* 15 U.S.C. 6804(a) (directing the agencies authorized to prescribe regulations under title V of the GLBA to assure to the extent possible that their regulations are consistent and comparable); *and* 15 U.S.C. 1681w(2)(B) (directing the agencies with enforcement authority set forth in 15 U.S.C. 1681s to consult and coordinate so that, to the extent possible, their regulations are consistent and comparable).

include customer information maintained on behalf of a covered institutions' affiliates?

72. Do covered institutions share customer information with affiliates that are neither financial institutions subject to the safeguards rules of other Federal financial regulators nor service providers? If so, please explain. If so, should customer information be subject to the same protections when a covered institution shares it with such an affiliate?

73. Are there any aspects of the proposed definition that may be too broad? If so, how is it broad? For example, should the definition limit customer information to nonpublic personal information about an institution's own customers that is maintained by or on behalf of the covered institution?

74. Is the safeguards rule too narrow? Should it extend to consumer information that is not customer information (*e.g.*, information from a consumer report about an employee or prospective employee)?

75. Under the proposed amendments, the disposal rule would apply to both customer information and consumer information. Is the proposed amended disposal rule too broad? If so, how should we narrow the coverage? For example, should the disposal rule protect customer information that is not consumer information, *i.e.*, nonpublic personal information, such as transaction information, that does not appear in a consumer report? Are there benefits to having the safeguards rule and the disposal rule apply to a more consistent set of information?

76. For covered institutions that are owned or controlled by affiliates based in another jurisdiction, what is the risk that customer information, including sensitive customer information, may be shared and used by such other affiliates? Would such practices raise concerns about potential harm related to the use or possession of customer information by such foreign affiliates? Should the rule include additional

requirements that would restrict the transmission of such customer information to foreign affiliates and others? If so, what should these be?

2. Safeguards Rule and Disposal Rule Coverage of Customer Information

We also propose to amend rule 248.30 to add a new section that would provide that the safeguards rule and disposal rule apply to both nonpublic personal information that a covered institution collects about its own customers and to nonpublic personal information it receives from a third party financial institution about that institution's customers. Currently, Regulation S-P defines "customer" as "a consumer who has a customer relationship with you." The safeguards rule, therefore, only protects the "records and information" of individuals who are customers of the particular institution and not others, such as individuals who are customers of another financial institution. The disposal rule, on the other hand, requires proper disposal of certain records about individuals without regard to whether the individuals are customers of the particular institution.

Proposed new paragraph (a) would provide that the safeguards rule and the disposal rule apply to all customer information in the possession of a covered institution, and all consumer information that a covered institution maintains or otherwise possesses for a business purpose, as applicable,[170] regardless of whether such information pertains to the covered institution's own customers or to customers of other financial institutions and has been provided to the covered institution.[171] For example, information that a registered investment adviser has received from the custodian of a former client's assets would be covered under both rules if the former client remains a customer of either the custodian or of another financial institution, even though the individual no longer has a customer relationship with the investment adviser. Similarly, any

---

[170] The safeguards rule is applicable to "consumer information" only to the extent it overlaps with "customer information." *See supra* note 166.

[171] Regulation S-P defines "financial institution" generally to mean any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). Rule 248.3(n).

individual's customer information or consumer information that a transfer agent has received from a broker-dealer holding an omnibus account with the transfer agent would be covered under both rules, even where the individual has no account in her own name at the transfer agent, as long as the individual is a customer of the broker-dealer or another financial institution. This approach is consistent with the FTC's safeguards rule.[172]

We request comment on the proposed scope of customer information covered under the safeguards rule and the disposal rule, including the following:

77. Is the proposed scope too broad or too narrow? If so, how should we broaden or narrow the scope? For example, should the rules' protections for "customer information" only extend to nonpublic personal information of the customers of another financial institution if the covered institution received the information from that financial institution (*e.g.*, an employee's or former customer's bank account information that the covered institution received directly from the individual, or prospective customers' information that the covered institution purchased or otherwise acquired from a third party would not be covered)?

78. Should employees' nonpublic personal information be protected under the safeguards rule? Why or why not? Would such coverage reduce the risk that unauthorized access to employee nonpublic personal information, such as a user name or password, could facilitate unauthorized access to customer information?

79. Do covered institutions receive nonpublic personal information about individuals who are not their customers from other financial institutions, such as custodians? If so, please provide examples. Do covered institutions take the same or different

---

[172] 15 CFR 314.1(b) (providing that the FTC's safeguards rule "applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you").

measures in safeguarding and disposing of information of individuals who are not their customers, such as employees or former customers? Please explain.

80. If covered institutions receive nonpublic personal information about individuals who are not their customers, are covered institutions able to determine whether such individuals are customers of other financial institutions? Would that be known as a result of any existing legal obligations?

81. Would the proposed rule result in covered institutions treating all nonpublic personal information about individuals as subject to the safeguards and disposal rules?

82. Should the proposed rule include a section describing scope? Does the scope section help clarify the information that a covered institution would have to protect under the safeguards rule and the disposal rule? Would the rule be clearer if it defined the scope of information protected within the definition of customer information?

3. Extending the Scope of the Safeguards Rule and the Disposal Rule to Cover All Transfer Agents

The proposed amendments would extend both the safeguards rule and the disposal rule to apply to any transfer agent registered with the Commission or another appropriate regulatory agency.[173] As discussed above, the safeguards rule currently applies to brokers, dealers, registered investment advisers, and investment companies, while the disposal rule currently applies to those entities as well as to transfer agents registered with the Commission.

The Safeguards Rule

Among other functions, transfer agents: (i) track, record, and maintain on behalf of issuers the official record of ownership of such issuer's securities; (ii) cancel old certificates,

---

[173] The term "transfer agent" would be defined by proposed rule 248.30(e)(12) to have the same meaning as in section 3(a)(25) of the Exchange Act (15 U.S.C. 78c(a)(25)).

issue new ones, and perform other processing and recordkeeping functions that facilitate the issuance, cancellation, and transfer of both certificated securities and book-entry only securities; (iii) facilitate communications between issuers and securityholders; and (iv) make dividend, principal, interest, and other distributions to securityholders.[174] To perform these functions, transfer agents maintain records and information related to securityholders that may include names, addresses, phone numbers, email addresses, employers, employment history, bank and specific account information, credit card information, transaction histories, securities holdings, and other detailed and individualized information related to the transfer agents' recordkeeping and transaction processing on behalf of issuers. With advances in technology and the expansion of book-entry ownership of securities, transfer agents today increasingly rely on technology and automation to perform the core recordkeeping, processing, and transfer services described above, including the use of computer systems to store, access, and process the customer information related to securityholders they maintain on behalf of issuers.

Like other market participants, systems maintained by transfer agents are subject to threats and hazards to the security or integrity of customer information,[175] which could create a reasonably likely risk of harm to an individual identified with the information. Specifically, the systems maintained by transfer agents are subject to similar types of risks of breach as other covered institutions, and as a consequence, the individuals whose customer information is maintained by transfer agents are subject to similar risks of substantial harm and inconvenience as individuals whose customer information is maintained by other covered institutions. To

---

174 *See* Advanced Notice of Proposed Rulemaking, Concept Release, Transfer Agent Regulations, Exchange Act Release No. 76743 (Dec. 22, 2015) [80 FR 81948, 81949 (Dec. 31, 2015)] ("2015 ANPR Concept Release").

175 As noted above in note 163, transfer agents typically do not have consumers or customers for the purposes of Regulation S-P, because their clients generally are not individual securityholders, but rather the issuers (*e.g.*, companies) in which the individual securityholders invest. However, as noted above, they maintain extensive securityholder records in connection with performing various processing, recordkeeping, and other services on behalf of their issuer clients.

account for this, the proposed definition of "customer information" with respect to a transfer agent would include "any record containing nonpublic personal information…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 handled or maintained by the transfer agent or on its behalf."[176]

In light of these risks, the proposed amendments would require transfer agents to protect the customer information they maintain by adopting and implementing appropriate safeguards in addition to taking measures to dispose of the information properly. Transfer agents would be required to develop, implement, and maintain written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information. They would also be required to develop, implement, and maintain an incident response program, including customer notifications, for unauthorized access to or use of customer information.

The Disposal Rule

Currently, the disposal rule only applies to those transfer agents "registered with the Commission."[177] However, the proposed amendments would also extend the application of the disposal rule to all transfer agents, including those transfer agents that are registered with another appropriate regulatory agency other than the Commission, by defining transfer agent in the proposed definition of a "covered institution" as "a transfer agent registered with the Commission or another appropriate regulatory agency."[178]

When the Commission initially proposed the disposal rule, it noted that the purpose of section 216 of the FACT Act was to "prevent unauthorized disclosure of information contained in a consumer report and to reduce the risk of fraud or related crimes, including identity theft."[179]

---

176 *See* proposed rule 248.30(e)(5)(ii).

177 *See* 17 CFR 248.30(b)(2)(i).

178 Proposed rule 248.30(e)(3). *See also* discussion of Exchange Act Section 17A(d)(1) authority *infra* note 189.

179 Disposal of Consumer Report Information, Exchange Act Release No. 50361 (Sept. 14, 2004) [69 FR 56304 (Sept. 20, 2004)] ("2004 Proposing Release"), at 56308.

Through the disposal rule, the Commission asserted that covered entities' consumers would benefit by reducing the incidence of identity theft losses.[180] At the same time, the Commission indicated that the disposal rule as proposed would impose "minimal costs" on firms in the form of providing employee training, or establishing clear procedures for consumer report information disposal.[181] Further, the Commission proposed that covered entities satisfy their obligations under the disposal rule through the taking of "reasonable measures" to protect against unauthorized access or use of the related customer information, the rule was designed to "minimize the burden of compliance for smaller entities."[182] At adoption, a majority of commenters supported the flexible standard for disposal that the Commission proposed, and no commenter opposed the standard.[183]

The Commission believes that extending the disposal rule now to cover those transfer agents registered with another appropriate regulatory agency would provide the same investor protection benefits and impose the same minimal costs on such firms as in the case of transfer agents registered with the Commission. When coupled with the additional benefit of providing a minimum industry standard for the proper disposal of all customer information or consumer information that any transfer agent maintains or possesses for a business purpose, the Commission preliminarily believes that extending the disposal rule to now cover all transfer agents would be appropriate for the protection of investors, and in the public interest.

Statutory Authority over Transfer Agents

When the Commission initially proposed and adopted the disposal rule, it did so to implement the congressional directive in section 216 of the FACT Act to adopt regulations to require any person who maintains or possesses a consumer report or consumer information

---

180 *Id*. at 56308-09.

181 *Id.*

182 *Id.*

183 *See* Disposal Rule Adopting Release, *supra* note 32.

derived from a consumer report for a business purpose to properly dispose of the information.[184] The Commission determined at that time that, through the FACT Act, Congress intended to instruct the Commission to adopt a disposal rule to apply to transfer agents registered with the Commission.[185] The Commission also stated at that time that the GLBA did not include transfer agents within the list of covered entities for which the Commission was required to adopt privacy rules.[186] Accordingly, the Commission extended the disposal rule only to those transfer agents registered with the Commission to carry out its directive under the FACT Act, while deferring to the FTC to utilize its "residual jurisdiction" under the same congressional mandate, to enact both a disposal rule and broader privacy rules that might apply to transfer agents registered with another appropriate regulatory agency.[187]

Separate from these conclusions, however, under section 17A of the Exchange Act, the Commission has broad authority, independent of either the FACT Act or the GLBA, to prescribe rules and regulations for transfer agents as necessary or appropriate in the public interest, for the protection of investors, for the safeguarding of securities and funds, or otherwise in furtherance of funds, or otherwise in furtherance of the purposes of Title I of the Exchange Act.[188] Specifically, regardless of whether transfer agents initially register with the Commission or another appropriate regulatory agency,[189] section 17A(d)(1) of the Exchange Act authorizes the

---

184 *See* 15 U.S.C. 1681w.

185 *See* 2004 Proposing Release, *supra* note 179, at n.23.

186 *Id.* at n.27.

187 *Id.*

188 15 U.S.C 78q-1.

189 *See* Exchange Act Section 17A(d)(1), 15 U.S.C 78q-1(d)(1) (providing that "no registered clearing agency or registered transfer agent shall . . . engage in any activity as … transfer agent in contravention of such rules and regulations" as the Commission may prescribe); Exchange Act Section 17A(d)(3)(b), 15 U.S.C 78q-1(d)(3)(b) (providing that "Nothing in the preceding subparagraph or elsewhere in this title shall be construed to impair or limit . . . the Commission's authority to make rules under any provision of this title or to enforce compliance pursuant to any provision of this title by any . . . transfer agent . . . with the provisions of this title and the rules and regulations thereunder.").

Commission to prescribe such rules and regulations as may be necessary or appropriate in the public interest, for the protection of investors, or otherwise in furtherance of the purposes of the Exchange Act with respect to any transfer agents, so registered. Once a transfer agent is registered, the Commission "is empowered with broad rulemaking authority over all aspects of a transfer agent's activities as a transfer agent."[190]

Accordingly, as the FTC has not adopted similar disposal and privacy rules to govern transfer agents registered with another appropriate regulatory agency, the Commission is proposing to extend the safeguards rule to apply to any transfer agent registered with either the Commission or another appropriate regulatory agency and extend the disposal rule to apply to transfer agents registered with another appropriate regulatory agency (*i.e.*, not the Commission). Here, the Commission has an interest in addressing the risks of market disruptions and investor harm posed by cybersecurity and other operational risks faced by transfer agents, and extending the safeguards rule and disposal rule to address those risks is in the public interest and necessary for the protection of investors and safeguarding of funds and securities.

Transfer agents are subject to many of the same risks of data system breach or failure that other market participants face. For example, transfer agents are vulnerable to a variety of software, hardware, and information security risks that could threaten the ownership interest of securityholders or disrupt trading within the securities markets.[191] Yet, based on the Commission's experience administering the transfer agent examination program, we are aware that practices among transfer agents related to information security and other operational risks

---

190 *See* Senate Report on Securities Act Amendments of 1975, S. Rep. No. 94-75, at 57.

191 For example, a software or hardware glitch, technological failure, or processing error by a transfer agent could result in the corruption or loss of securityholder information, erroneous securities transfers, or the release of confidential securityholder information to unauthorized individuals. A concerted cyber-attack or other breach could have the same consequences, or result in the theft of securities and other crimes. *See generally*, SEC Cybersecurity Roundtable transcript (Mar. 26, 2014), *available at* https://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt.

vary widely.[192] A transfer agent's failure to account for such risks and take appropriate steps to mitigate them can directly lead to the loss of funds or securities, including through theft or misappropriation.

At the same time, the scope and volume of funds and securities that are processed or held by transfer agents have increased dramatically. The risk of loss of such funds and securities presents significant risks to issuers, securityholders, other industry participants, and the U.S. financial system as a whole. Transfer agents that provide paying agent services on behalf of issuers play a significant role within that system.[193] According to Form TA-2 filings in 2021, transfer agents distributed approximately $3.8 trillion in securityholder dividends and bond principal and interest payments. Critically, because Form TA-2 does not include information relating to the value of purchase, redemption, and exchange orders by mutual fund transfer agents, the $3.8 trillion amount noted above does not include these amounts. If the value of such transactions by mutual fund transfer agents was captured by Form TA-2 it is possible that the $3.8 trillion number would be significantly higher.[194]

By extending the safeguards rule and disposal rule to cover *all* transfer agents, the Commission anticipates the rules would be in the public interest and would help protect investors and safeguard their securities and funds. Specifically, extending the safeguards rule to cover any transfer agent in order to address the risks to the security or integrity of customer information found on the systems they maintain will help prevent securityholders' customer information from being compromised, which, as noted above, could threaten the ownership interest of

---

192 *See* 2015 ANPR Concept Release, *supra* note 174, at 81985.

193 We use the term "paying agent services" here to refer to administrative, recordkeeping, and processing services related to the distribution of cash and stock dividends, bond principal and interest, mutual fund redemptions, and other payments to securityholders. There are numerous, often complex, administrative, recordkeeping, and processing services that are associated with, and in many instances are necessary prerequisites to, the acceptance and distribution of such payments.

194 For example, our staff has observed that, aggregate gross purchase and redemption activity for some of the larger mutual fund transfer agents has ranged anywhere from $3.5 trillion to nearly $10 trillion just for a single entity in a single year.

securityholders or disrupt trading within the securities markets. It also would help establish minimum nationwide standards for the notification of securityholders who are affected by a transfer agent data breach that leads to the unauthorized access or use of their information so that affected securityholders could take additional mitigating actions to protect their customer information, ownership interest in securities, and trading activity. Similarly, extending the disposal rule to cover those transfer agents registered with another appropriate regulatory agency would help protect investors and safeguard their securities and funds by reducing the risk of fraud or related crimes, including identity theft, which can lead to the loss of securities and funds.

The Commission acknowledges that if the proposal is adopted it would also impose costs on transfer agents that would be subject to both the safeguards rule and the disposal rule for the first time.[195] For all transfer agents, such costs would include the development and implementation of the policies and procedures required under the safeguards rule, the ongoing costs of complying with required recordkeeping and maintenance requirements, and, in the event of the unauthorized access or use of their customer information, the costs necessary to comply with the customer notification requirements of the proposal. With respect to transfer agents registered with another appropriate regulatory agency that are not currently subject to the disposal rule, such costs would also include the same costs incurred by the transfer agents registered with the Commission that are currently subject to the disposal rule to establish written policies and procedures for consumer and customer information disposal, as well as the minimal employee training costs necessary to address adherence to those policies and procedures.

However, because many of the transfer agents registered with another appropriate regulatory agency that are not currently subject to the disposal rule are banking entities subject to Federal and state banking laws and other requirements, it is likely that a large percentage of them

---

[195] *See infra* section III.D.2.

already train their employees and have procedures for consumer report information disposal that likely would comply with the disposal rule.[196] Further, although transfer agents would face higher costs of compliance from this proposal than those covered institutions already subject to the safeguards rule and the disposal rule, the Commission believes the additional cost to such transfer agents will be comparable to the costs of compliance that was incurred by covered institutions (such as registered investment advisers and broker dealers) when they first became subject to these rules.[197] When considered in the context of protecting investors and safeguarding securities and funds, as discussed above, the Commission preliminarily believes that such costs are appropriate.

We seek comment on the proposal to extend the application of the safeguards rule and the disposal rule to both cover all transfer agents.

83. What would be the comparative advantages and disadvantages and costs and benefits of expanding the definition of customer information with respect to transfer agents? Is the proposed definition of "customer information" appropriate with respect to transfer agents?

84. Are some transfer agents, for example those that are registered with another appropriate regulatory agency, subject to duplicative or conflicting requirements as those that would be imposed under the safeguards rule? If so, please explain.

85. Should the definition of "customer information" be expanded to cover other stakeholders or individuals whose information may be handled or maintained by a transfer agent, such as employees, investors or contractors? If so, please explain why.

86. Are there particular concerns that transfer agents might have in implementing or meeting the requirements of the safeguards rule? Should we modify any of the

---

196 *See infra* text accompanying notes 367-373.

197 *See* Reg. S-P Release, *supra* note 2.

requirements of the safeguards rule to take into account other regulatory requirements to which some transfer agents might be subject, or the differences between the operations of transfer agents and other covered institutions?

87. Are there other registrants or market participants to whom we should extend the safeguards rule and the disposal rule? If so, which ones?

88. Would transfer agents be subject to any compliance costs under this proposed rule that differ materially from those costs that covered institutions that are already subject to the safeguards rule and the disposal rule will have incurred through both past compliance, as well as the additional costs associated with this proposed rule? If so, please explain why and quantify these costs.

4. Maintaining the Current Regulatory Framework for Notice-Registered Broker-Dealers

The proposed amendments would also continue to maintain the same regulatory treatment for notice-registered broker-dealers as they do under the current safeguards rule and the disposal rule. Notice-registered broker-dealers 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 limited purpose of effecting transactions in security futures products.[198] These notice-registered broker-dealers are currently explicitly excluded from the scope of the disposal rule,[199] but subject to the safeguards rule. However, under substituted compliance provisions, notice-registered broker-dealers are deemed to comply with the safeguards rule where they are subject to, and comply with, the financial privacy rules of the

---

198 *See* Registration of Broker-Dealers Pursuant to section 15(b)(11) of the Securities Exchange Act of 1934, Exchange Act Release No. 44730 (Aug. 21, 2001) [66 FR 45138 (Aug. 27, 2001)] ("Notice-Registered Broker-Dealer Release").

199 *See* 17 CFR 248.30(b)(2)(i).

CFTC,[200] including similar obligations to safeguard customer information.[201] The Commission adopted substituted compliance provisions with regard to the safeguards rule in acknowledgment that notice-registered broker-dealers are subject to primary oversight by the CFTC, and to mirror similar substituted compliance provisions afforded by the CFTC to broker-dealers registered with the Commission.[202] When the Commission thereafter adopted the disposal rule, it excluded notice-registered broker-dealers from the rule's scope noting its belief that Congress did not intend for the Commission's FACT Act rules to apply to entities subject to primary oversight by the CFTC.[203]

For these reasons, the Commission has tailored the proposed amendments to ensure there will be no change in the treatment of notice-registered broker-dealers under the safeguards rule and the disposal rule. First, the proposed rule would define a "covered institution" to include "any broker or dealer," without excluding notice-registered broker-dealers, thus ensuring that Regulation S-P's substituted compliance provisions would still apply to notice-registered broker-dealers with respect to the safeguards rule.[204] Second, although the proposed disposal rule would

---

200 *See* 17 CFR 248.2(c) and 248.30(b). Under the substituted compliance provision in rule 248.2(c), notice-registered broker-dealers operating in compliance with the financial privacy rules of the CFTC are deemed to be in compliance with Regulation S-P, except with respect to Regulation S-P's disposal rule (currently rule 248.30(b)).

201 *See* 17 CFR 160.30.

202 *See* Notice-Registered Broker-Dealer Release, *supra* note 198; *see also* CFTC, Privacy of Customer Information [66 FR 21236 at 21252 (Apr. 27, 2001)].

203 *See* 2004 Proposing Release, *supra* note 179, at n.23 (stating "There is no legislative history on this issue. As discussed in our recent proposal for rules implementing section 214 of the FACT Act, Congress' inclusion of the Commission as one of the agencies required to adopt implementing regulations suggests that Congress intended that our rules apply to brokers, dealers, investment companies, registered investment advisers, and registered transfer agents. Consistent with that proposal, however, notice-registered broker-dealers would be excluded from the scope of the proposed disposal rule."); *see also* Limitations on Affiliate Marketing (Regulation S-AM), Exchange Act Release No. 49985 (July 8, 2004); [69 FR 42302 (July 14, 2004)], at n.22 (stating "We interpret Congress' exclusion of the CFTC from the list of financial regulators required to adopt implementing regulations under section 214(b) of the FACT Act to mean that Congress did not intend for the Commission's rules under the FACT Act to apply to entities subject to primary oversight by the CFTC.").

204 *See* proposed rule 248.30(e)(3); *see also* 17 CFR 248.2(c).

also employ this proposed definition of a "covered institution," it would retain the disposal rule's current exclusion for notice-registered broker-dealers.[205]

This approach will provide notice-registered broker-dealers with the benefit of consistent regulatory treatment under Regulation S-P, without imposing any additional costs, while also maintaining the same investor protections that the customers of notice-registered broker-dealers currently receive. To the extent notice-registered broker-dealers opt to comply with Regulation S-P and the proposed safeguards rule rather than avail themselves of substituted compliance by complying with the CFTC's financial privacy rules, the Commission believes the benefits and costs of complying with the proposed rule would be the same as those for other broker-dealers. Notice-registered broker-dealers should not face additional costs under the proposed amendments to the disposal rule, as they would remain excluded from its scope.

We seek comment on the proposal to maintain the same regulatory framework for notice-registered broker-dealers under the safeguards rule and the disposal rule:

89. Does the current regulatory framework for notice-registered broker-dealers under the safeguards rule and the disposal rule adequately protect investors who are clients of such institutions? If not, how is the current regulatory framework for notice-registered broker-dealers inadequate in this regard?

90. Should the rule alter the scope of either rule's application to notice-registered broker-dealers? If so, what alterations should be considered, and why? What would the costs and benefits be of such alterations in approach?

---

[205] *See* proposed rule 248.30(c)(1). The proposed rule would also include a technical amendment to 17 CFR 248.2(c), which, as to the disposal rule, provides an exception from the substituted compliance regime afforded to notice-registered broker-dealers for Regulation S-P. Specifically, section 248.2(c) would include an amended citation to the disposal rule, to reflect its shift from 17 CFR 248.30(b) to proposed rule 248.30(c). *See* proposed rule 248.2(c).

D. Recordkeeping

The proposed amendments would require covered institutions to make and maintain written records documenting compliance with the requirements of the safeguards rule and of the disposal rule. Specifically, the proposal would amend (i) Investment Company Act rules 31a-1(b) and 31a-2(a) for investment companies that are registered under the Investment Company Act,[206] (ii) Investment Advisers Act rule 204-2 for registered investment advisers,[207] (iii) Exchange Act rule 17a-4 for broker-dealers,[208] and (iv) Exchange Act rule 17Ad-7 for transfer agents.[209] The proposal would also include a recordkeeping provision in proposed rule 248.30(d) under Regulation S-P for investment companies that are not registered under the Investment Company Act ("unregistered investment companies").[210] In each case, the proposed amendments would require the covered institution to maintain written records documenting the covered institution's compliance with the requirements set forth in proposed rule 248.30(b) (procedures to safeguard customer information) and (c)(2) (disposal of consumer information and customer information).

The records required pursuant to Investment Company Act proposed rules 31a-1(b) and 31a-2(a), proposed rule 248.30(d) under Regulation S-P, Investment Advisers Act proposed rule 204-2, Exchange Act proposed rule 17a-4, and Exchange Act proposed rule 17ad-7 would include, for example, records of policies and procedures under the safeguards rule that address administrative, technical, and physical safeguards for the protection of customer information as well as the proposed incident response program for unauthorized access to or use of customer information, including customer notice. Covered institutions would also be required to make and

---

206 *See* proposed rule 270.31a-1(b) and proposed rule 270.31a-2(a).

207 *See* proposed rule 275.204-2(a).

208 *See* proposed rule 240.17a-4(e).

209 *See* proposed rule 240.17ad-7(k). *See also* discussion on redesignation of 17 CFR 240.17Ad-7 as 17 CFR 240.17ad-7 *supra* note 104.

210 *See* proposed rule 248.30(d). Certain investment companies, such as some employees' securities companies, are not required to register under the Investment Company Act.

maintain written records documenting, among other things: (i) its assessments of the nature and scope of any incidents involving unauthorized access to or use of customer information; (ii) steps taken to contain and control such incidents; and (iii) its notifications to affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization, including, where applicable, any determinations, after a reasonable investigation of the facts and circumstances of an 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, and the basis for that determination.[211]

The rule proposals would also require covered institutions to keep records of those written policies and procedures requiring any service providers to take appropriate measures that are designed to protect against unauthorized access to or use of customer information, including notification to the covered institution as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security resulting in unauthorized access to a customer information system maintained by the service provider to enable the covered institution to implement its response program, as well as related records of written contracts and agreements between the covered institution and the service provider.[212] These records would help covered institutions periodically reassess the effectiveness of their policies and procedures, and determine whether they are reasonably designed, and would help our examiners and enforcement program to monitor compliance with the requirements of the amended rules.

With respect to the disposal rule, the proposed rules require that every covered institution adopt and implement written policies and procedures that address the proper disposal of

---

[211] *See* proposed rule 248.30(b)(3)(i)-(iii).

[212] *See* proposed rule 248.30(b)(5)(i)-(ii).

consumer information and customer information.[213] The proposed recordkeeping requirements are not intended to require covered institutions to document every act of disposing of an item of information. For example, a covered institution's periodic review and written documentation of its disposal practices generally should be sufficient to satisfy the proposed recordkeeping requirements as they relate to the disposal rule.

Under the proposed rules, the time periods for preserving records would vary by covered institution to be consistent with existing recordkeeping rules. Broker-dealers would have to preserve the records for a period of not less than three years, in an easily accessible place.[214] Transfer agents would have to preserve the records for a period of not less than three years, in an easily accessible place.[215] Investment companies registered under the Investment Company Act and unregistered investment companies would have to preserve the records, apart from any policies and procedures, for a period of not less than six years, the first two years in an easily accessible place; and in the case of any policies and procedures, 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.[216] Registered investment advisers would have to preserve the records for five years, the first two years in an appropriate office of the investment adviser.[217] These proposed recordkeeping provisions, while varying among covered institutions, should result in the

---

213 *See* proposed rule 248.30(c)(2). While the disposal rule does not currently require covered institutions to adopt and implement written policies and procedures, those adopted pursuant to the current safeguards rule should already cover disposal. *See* Disposal Rule Adopting Release, *supra* note 32, at 69 FR 71325 ("proper disposal policies and procedures are encompassed within, and should be a part of, the overall policies and procedures required under the safeguard rule."). Therefore, proposed rule 248.30(c)(2) is intended primarily to seek sufficient documentation of policies and practices addressing the specific provisions of the disposal rule.

214 *See* proposed rule 240.17a-4(e)(14).

215 *See* proposed rule 270.31a-2(a)(8) (registered investment companies) and proposed rule 248.30(d)(2) (unregistered investment companies). Unregistered investment companies may have a third party maintain and preserve the records required by the proposed rule, but any such unregistered investment company will remain fully responsible for compliance with the recordkeeping requirements under the proposed rule.

216 *See id.*

217 *See* proposed rule 275.204-2(a)(20) and current rule 275.204-2(e)(1).

maintenance of the proposed records for sufficiently long periods of time and in locations in which they would be useful to staff examiners and the enforcement program. The proposal to conform the retention periods to existing requirements is intended to allow covered institutions to minimize their compliance costs by integrating the proposed requirements into their existing recordkeeping systems and record retention timelines.

We request comment on the proposed requirements for making and maintaining records, including the following:

91. Are the records that we propose to require appropriate? Should covered institutions be required to keep any additional or fewer records? If so, what records and why?

92. Should the rule limit the list of required records to assessments, containment or control measures or investigations only for certain information security incidents? Are some information security incidents not sufficiently consequential as compared to the amount of time required to record the institution's response? If so, please explain. How should the rule distinguish between information security incidents that require a record to be made and maintained and those that do not? If a record is not required for certain investigations, should a covered institution nevertheless be required to record a determination 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?

93. Are the proposed periods of time for preserving records appropriate, or should certain records be preserved for different periods of time? Should the recordkeeping time periods be the same across covered institutions? Would the costs associated with preserving records for periods of time consistent with covered institutions' existing recordkeeping requirements be less than if all covered institutions were required to keep these records for the same period of time?

94. Are the rule proposals sufficiently explicit about the specific records that covered institutions must maintain? The proposed amendments for investment companies and registered investment advisers require these covered institutions to make and maintain written records documenting compliance with paragraphs (b)(1) and (c)(2) of Regulation S-P. In contrast, the proposed amendments for broker-dealers and transfer agents, specifically identify the records that should be maintained and preserved. Would investment companies and registered investment advisers benefit from additional specificity, such as requiring that investment companies and registered advisers keep the same records as those proposed to be required for broker-dealers and transfer agents? On the other hand, are the proposed rules for broker-dealers and transfer agents too granular? Please explain why or why not. Should the rule specifically require that a covered institution keep records of requests to delay notice from the Attorney General of the United States or any other specific records? In what respect should the rule proposals be made more or less explicit?

E. Exception from the Annual Notice Delivery Requirement

The GLBA requires financial institutions to provide customers with annual notices informing them about the institution's privacy policies.[218] In certain circumstances, institutions must also provide their customers with an opportunity to opt out before the institution shares their information.[219] Regulation S-P includes provisions implementing these notice and opt out requirements for broker-dealers, investment companies and registered investment advisers.[220]

---

218 15 U.S.C. 6803(a). GLBA provisions regarding disclosure of nonpublic personal information are set forth in Title V, Subtitle A of GLBA, sections 501-509, codified at 15 U.S.C. 6801-6809.

219 15 U.S.C. 6802(b). Under Regulation S-P, an institution's customer is a "consumer" that has a continuing relationship with the institution. 17 CFR 248.3(j). Regulation S-P defines a "consumer" as "an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative." 17 CFR 248.3(g).

220 Regulation S-P provisions requiring institutions to provide notice and opt out to customers are set

In the 2015 Fixing America's Surface Transportation Act ("FAST Act"), Congress added new section 503(f) to GLBA ("statutory exception").[221] This provision provides an exception to the annual notice delivery requirements for a financial institution that meets certain requirements, and became effective when it was enacted on December 4, 2015.[222]

We are proposing amendments to the annual notice provision requirement in Regulation S-P to include the exception to the annual notice delivery added by the statutory exception.[223] In addition, we propose to provide timing requirements for delivery of annual privacy notices if a broker-dealer, investment company, or registered investment adviser that qualifies for the annual notice exception later changes its policies and practices in such a way that it no longer qualifies for the exception.[224]

1. Current Regulation S-P requirements for privacy notices

Currently, Regulation S-P generally requires a broker-dealer, investment company or registered investment adviser to provide an initial privacy notice to its customers not later than when the institution establishes the customer relationship and annually after that for as long as the customer relationship continues.[225] If an institution chooses to share nonpublic personal information with a nonaffiliated third party other than as disclosed in an initial privacy notice, the institution must send a revised privacy notice to its customers.[226]

---

forth in 17 CFR 248.1 through 248.18. Rule 248.5 sets forth requirements for annual notices and their delivery. *See* Reg. S-P Release, *supra* note 2.

221 *See* FAST Act, Pub. L. 114094, section 75001, adding section 503(f) to the GLBA, codified at 15 U.S.C. 6803(f).

222 *Id.*

223 *See* proposed rule 248.5(e)(1).

224 *See* proposed rule 248.5(e)(2). In developing this proposal, as directed by GLBA, we consulted and coordinated with the CFTC, CFPB, FTC and the National Association of Insurance Commissioners, including regarding consistency and comparability with the regulations prescribed by these entities. *See* 15 U.S.C 6804(a)(2). The proposed amendment implementing the exception under GLBA section 503(f) is designed to be consistent and comparable to those of the CFTC, CFPB, and FTC.

225 17 CFR 248.4; 248.5.

226 17 CFR 248.8. Regulation S-P provides certain exceptions to the requirement for a revised

Regulation S-P also requires that before an institution shares nonpublic personal information with nonaffiliated third parties, the institution must provide the customer with an opportunity to opt out of sharing, except in certain circumstances.[227] A broker-dealer, investment company, or registered investment adviser is not required to provide customers the opportunity to opt out if the institution shares nonpublic personal information with nonaffiliated third parties (i) pursuant to a joint marketing arrangement with third party service providers, subject to certain conditions,[228] (ii) related to maintaining and servicing customer accounts, securitization, effecting certain transactions, and certain other exceptions[229] and (iii) related to protecting against fraud and other liabilities, compliance with certain legal and regulatory requirements, consumer reporting, and certain other exceptions.[230]

The types of information required to be included in the initial, annual, and revised privacy notices are identical. Each privacy notice must describe the categories of information the institution shares and the categories of affiliates and nonaffiliates with which it shares nonpublic personal information.[231] The privacy notices also must describe the type of information the institution collects, how it protects the confidentiality and security of nonpublic personal information, a description of any opt out right, and certain disclosures the institution makes under the FCRA.[232]

2. Proposed amendment

---

privacy notice, including if the institution is sharing as permitted under rules 248.13, 248.14, and 248.15 or to a new nonaffiliated third party that was adequately disclosed in the prior privacy notice.

227 17 CFR 248.10.

228 17 CFR 248.13.

229 17 CFR 248.14.

230 17 CFR 248.15.

231 *See* 17 CFR 248.6(a)(2)-(5) and 248.6(a)(9).

232 *See* 17 CFR 248.6(a)(1) (information collection); 248.6(a)(8) (protecting nonpublic personal information), 248.6(a)(6) (opt out rights); 248.6(a)(7) (disclosures the institution makes under section 603(d)(2)(A)(iii) of the FCRA (15 U.S.C. 1681a(d)(2)(A)(iii)), notices regarding the ability to opt out of disclosures of information among affiliates).

Section 248.5 of Regulation S-P sets forth the requirements for an annual privacy notice, including delivery. We are proposing to add a new paragraph (e) to the section, which would include the statutory exception from the annual privacy notice requirement.[233]

a. Conditions for the exception

To qualify for the statutory exception, a financial institution must satisfy two conditions.[234] First, an institution must share nonpublic personal information only in accordance with the exceptions in GLBA sections 502(b)(2) and (e).[235] These sections set forth exceptions to the requirement to provide customers an opportunity to opt out of the institution's information sharing with nonaffiliated third parties. Second, an institution relying on the exception cannot have changed its policies and practices with regard to disclosing nonpublic personal information from those that were disclosed in the most recent disclosure sent to consumers.[236]

Our proposed amendment to Regulation S-P would implement the statutory exception. In particular, our proposed amendment would provide that a broker-dealer, investment company, or registered investment adviser is not required to deliver an annual privacy notice if it satisfies two conditions that reflect those the FAST Act added to the GLBA. First, an institution relying on the exception could only provide nonpublic personal information to nonaffiliated third parties in accordance with the exceptions set forth in Regulation S-P sections 248.13, 248.14 and 248.15, which implement the exceptions to the opt out requirement in GLBA sections 502(b) and (e).[237]

Second, an institution cannot have changed its policies and practices with regard to disclosing nonpublic personal information from those it most recently disclosed to the

---

233 The proposal also would clarify that the rule includes an exception by amending the general requirement in paragraph 248.5(a)(1) that institutions provide the annual privacy notices to add the words "Except as provided by paragraph (e) of this section …".

234 *See* 15 U.S.C. 6803(f).

235 *See* 15 U.S.C. 6803(f)(1).

236 *See* 15 U.S.C. 6803(f)(2).

237 Proposed rule 248.5(e)(1)(i).

customer.[238] Specifically, an institution would satisfy this condition if the institution's policies and practices regarding the information described under paragraphs 248.6(a)(2) through (5) and (9), each of which relates to the disclosure of nonpublic personal information, are unchanged from those included in the institution's most recent privacy notice sent to customers. We are not including in the exception the other information that an institution is required to include in its privacy notices pursuant to paragraph 248.6(a) because such other information either does not relate to the disclosure of nonpublic personal information[239] or is not relevant to the exception.[240] Our proposed approach to the condition is designed to be consistent with and comparable to that of the CFTC, CFPB, and FTC, which reference the same disclosures of nonpublic personal information in the conditions to the exceptions to their annual privacy notice delivery requirements.[241]

b. Resumption of annual privacy notice delivery

The statutory exception states that a financial institution that meets the requirements for the annual privacy notice exception will not be required to provide annual privacy notices "until such time" as that financial institution fails to comply with the conditions to the exception, but

---

238 Proposed rule 248.5(e)(1)(ii).

239 *See* paragraph 248.6(a)(1) (categories of information the institution collects) and paragraph 248.6(a)(8) (policies and practices with respect to confidentiality and security).

240 *See* paragraph 248.6(a)(6) (requiring the notice to describe the customer's right to opt out of the information sharing, which would not be applicable for institutions that qualify for the proposed exception) and paragraph 248.6(a)(7) (requiring an institution's privacy notice to include any disclosures the institution makes under FCRA section 603(d)(2)(A)(iii), which describe sharing with an institution's affiliates and do not affect whether the statutory exception is satisfied); *see also* 15 U.S.C. 603(d)(2)(iii) (excluding from the term "consumer report" communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that such information not be communicated among such persons).

241 *See* CFTC, Privacy of Consumer Financial Information – Amendment to Conform Regulations to the Fixing America's Surface Transportation Act, 83 FR 63450 (Dec. 10, 2018), at n.17; CFPB, Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P) 83 FR 40945 (Aug. 17, 2018), at 40950; FTC, Privacy of Consumer Financial Information Rule Under the Gramm-Leach-Bliley Act, 84 FR 13150 (Apr. 4, 2019), at 13153.

does not specify a date by which the annual privacy notice delivery must resume.[242] Under our proposed amendment, when an institution would need to resume delivering annual privacy notices depends on whether or not it must issue a revised privacy notice.[243]

First, if a financial institution changes its policies so that it triggers the existing requirement to issue a revised privacy notice under rule 248.8, that institution would be required to provide an annual privacy notice in accordance with the timing requirement in paragraph 248.5(a).[244] As noted above, Regulation S-P generally requires an institution to provide an initial privacy notice to an individual who becomes the institution's customer no later than when it establishes a customer relationship.[245] Paragraph 248.5(a) requires a financial institution to provide a privacy notice to its customers "not less than annually" during the continuation of any customer relationship. Thus, the rule provides institutions with the flexibility to select a specific date during the year to provide annual privacy notices to all customers, regardless of when a particular customer relationship began.[246]

We propose to use the same approach to the resumption of delivery of annual privacy notices when a change in practice requires an institution to send a revised notice to customers.[247] The revised privacy notice would be treated as analogous to an initial notice for purposes of determining the timing of the subsequent delivery of annual privacy notices. This would allow institutions to preserve their existing approach to selecting a delivery date for annual privacy

---

242 *See supra* note 231.

243 Proposed rule 248.5(e)(2).

244 Proposed rule 248.5(e)(2)(i).

245 Rule 248.5(a)(1).

246 Paragraph 248.5(a)(1) requires privacy notices to be delivered annually, which means at least once in any period of 12 consecutive months during which the relationship exists. An institution can define the 12-consecutive-month period, but must apply it to the customer on a consistent basis. Paragraph 248.5(a)(2) illustrates how to apply a 12-consecutive-month period to a given customer.

247 *See* 17 CFR 248.8.

notices, thereby avoiding the potential burdens of determining delivery dates based on a new approach.

In the second circumstance, if the institution's change in policies or practices does not require a revised privacy notice, the institution would be required to provide an annual privacy notice to customers within 100 days of the change.[248] This 100-day period is intended to provide timely delivery of the updated privacy notice to customers who were not informed prior to the institution's change in policies or practices. Moreover, we preliminarily believe that a 100-day period also generally avoids imposing significant additional costs on the institution. Any 100-day period will accommodate the institution delivering the privacy notice alongside any quarterly reporting to customers. Proposed paragraph 248.5(e)(2)(iii) provides an example for each scenario described above in which an institution must resume delivering annual privacy notices.

The proposed timing requirements for when an institution no longer meets requirements for the exception and must resume delivering annual privacy notices are designed to be consistent with the existing timing requirements for privacy notice delivery in Regulation S-P, where applicable. The proposed timing requirements also are intended to be consistent with parallel CFTC, CFPB, and FTC rules.[249] They also are intended to provide clarity to institutions when a change in policies and practices prevent an institution from relying on the annual privacy notice delivery exception. In addition, providing timing provisions consistent with those of the CFTC, CFPB, and FTC would facilitate privacy notice delivery for affiliated financial institutions subject to GLBA that are not broker-dealers, investment companies, or registered investment advisers.

We request comment on the proposed exception to the annual privacy notice delivery requirement provisions, including the following:

---

[248] Proposed rule 248.5(e)(2)(ii).

[249] *See* 17 CFR 160.5(D) (CFTC); 12 CFR 1016.5(e)(2) (CFPB); 16 CFR 313.5(e)(2) (FTC).

95. The proposed annual privacy notice exception is conditioned on a broker-dealer, investment company, or registered investment adviser not changing policies and practices related to the disclosure of nonpublic personal information (*i.e.*, information on policies and practices required to be in a privacy notice under paragraphs 248.6(a)(2) through (5) and (9)). Should the exception remain available when the institution makes minor or non-substantive changes to its policies and practices? If so, how should we define the scope of changes that would allow use of the exception?

96. Should the proposed amendment include a provision for timing in these circumstances? Should the rule require an institution to provide notice by the time it has changed its disclosure policies and practices so that it no longer meets the proposed conditions of the rule in all circumstances? Should the proposed 100-day time period for resumption of delivery of annual privacy notices be shorter or longer? For example, should the period be shorter, such as 30, 60, or 90 days? Should the period be longer, such as 120 or 150 days? Should it be a qualitative standard? Or a qualitative standard with an upper ceiling? Please explain.

F. Request for Comment on Limited Information Disclosure When Personnel Leave Their Firms

The Commission requests comment on adding an exception from the notice and opt out requirements that would permit limited information disclosure when personnel move from one brokerage or advisory firm to another. The 2008 Proposal included an exception from the notice and opt out requirements to permit limited disclosures of investor information when a registered representative of a broker-dealer or a supervised person of a registered investment adviser (collectively, "departing personnel") moved from one brokerage or advisory firm to another. The exception that was previously proposed would have permitted firms with departing personnel to share certain limited customer contact information and supervise the information

transfer, and required them to retain the related records.[250] To limit the risk of identity theft or other abuses, the shared information could not include any customer's account number, Social Security number, or securities positions.[251] In the 2008 Proposal, the Commission noted that most firms seeking to rely on this proposed exception would not have needed to revise their GLBA privacy notices, because they already state in the notices that their disclosures of information not specifically described include disclosures permitted by law, which would include disclosures made pursuant to the proposed exception and the other exceptions provided in section 15 of Regulation S-P.[252] Although a few commenters supported the exception as proposed, many expressed concerns about at least certain aspects of the exception.[253]

As noted above, the Commission is not adding an exception from the notice and opt out requirements in connection with this proposal. However, the Commission requests comment on whether to permit the limited disclosure of certain investor information when departing personnel move from one brokerage or advisory firm to another, including whether an exception from this proposal's notice and opt out requirements would be appropriate:

97. Would adopting such an exception from the notice and opt out provisions of Regulation S-P be appropriate in light of the GLBA's goals? If so, is there a need for an exception to permit a limited disclosure of investor information when departing personnel moves from one brokerage or advisory firm to another? If so, what are other limitations, benefits, risks, or other considerations related to such an exception?

---

250 *See* 2008 Proposal, *supra* note 38, at 13702-04.

251 *See id*. *See* 2008 Proposal, *supra* note 38, at 13703, n.94.

252 *See* 2008 Proposal, *supra* note 38, at 13703, n.94.

253 *See e.g.*, Letter from Brendan Daly, Compliance Manager, Commonwealth Financial Network (May 12, 2008); Letter from Alan E. Sorcher, Managing Director and Associate General Counsel, SIFMA (May 12, 2008) ; Letter from Michael J. Mungenast, Chief Executive Officer and President, ProEquities, Inc.; Julius L. Loeser, Chief Regulatory and Compliance Counsel, Comerica Tower at Detroit Center, Corporate Legal Department (May 9, 2008); and Letter from Becky Nilsen, Chief Executive Officer, Desert Schools Federal Credit Union (May 12, 2008).

G. Other Current Commission Rule Proposals

1. Covered Institutions Subject to the Regulation SCI Proposal and the Exchange Act Cybersecurity Proposal

a. Discussion

i. Introduction

In addition to the Regulation S-P proposal, the Commission is proposing the Exchange Act Cybersecurity Proposal and is proposing to amend Regulation SCI.[254] As discussed in more detail below, certain types of entities that would be subject to the proposed amendments to Regulation S-P would also be subject to those proposed rules, if adopted.[255] As a result, such entities could be subject to multiple requirements to maintain policies and procedures that address certain types of cybersecurity risk,[256] as well as obligations to provide multiple forms of disclosure or notification related to a cybersecurity event under the various proposals.[257] While the Commission preliminarily believes that these requirements are nonetheless appropriate, it is seeking comment on the proposed amendments, given the following: (1) each proposal has a different scope and purpose; (2) the policies and procedures related to cybersecurity that would be required under each of the proposed rules would not be inconsistent; (3) the public disclosures or notifications required by the proposed rules would require different types of information to be disclosed, largely to different audiences at different times; and (4) it should be appropriate for entities to comply with the proposed requirements.

---

254 *See* Exchange Act Cybersecurity Proposal and Regulation SCI Proposal, *supra* note 57.

255 *See* 17 CFR 242.1000 through 1007 (Regulation SCI); Regulation SCI Proposal, *supra* note 57; 17 CFR 248.1 through 248.30 (Regulation S-P); and Exchange Act Cybersecurity Proposal, *supra* note 57.

256 As discussed in more detail in the Exchange Act Cybersecurity Proposal, NIST defines "cybersecurity risk" as "an effect of uncertainty on or within information and technology." *See* Exchange Act Cybersecurity Proposal, *supra* note 57.

257 For example, with respect to cybersecurity, both Regulation SCI (currently and as it would be amended) and the Exchange Act Cybersecurity Proposal have or would have provisions requiring policies and procedures to address certain types of cybersecurity risks. The proposed amendments to Regulation S-P also would require policies and procedures regarding cybersecurity risks to the extent that customer information or consumer information is stored on an electronic information system that could potentially be compromised (*e.g.*, on a computer).

The specific instances in which the regulations, currently and as proposed to be amended, may relate to each other are discussed briefly below. In addition, we encourage interested persons to provide comments on the discussion below.

More specifically, the Commission encourages commenters to identify any areas where they believe the requirements of the proposed amendments to Regulation S-P and the requirements of Regulation SCI (currently and as it would be amended) and the Exchange Act Cybersecurity Proposal is particularly costly or creates practical implementation difficulties, provide details on what in particular about implementation would be difficult, and how the duplication will be costly or create such difficulties, and to make recommendations on how to minimize these potential impacts. In addition, the Commission encourages comments that explain how to achieve the goal of this proposal to reduce or help mitigate the potential for harm to individuals whose sensitive customer information has been accessed or used without authorization. To assist this effort, the Commission is seeking specific comment below on this topic.

b. Covered Institutions That Are or Would Also Be Subject to Regulation SCI and the Exchange Act Cybersecurity Proposal

Various covered institutions under this proposal are or would be subject to Regulation SCI (currently and as it would be amended) and the Exchange Act Cybersecurity Proposal.[258] For example, alternative trading systems ("ATSs") that trade certain stocks exceeding specific volume thresholds are SCI Entities[259] and would also be covered institutions subject to the requirements of the proposed amendments to Regulation S-P.[260] Therefore, if the proposed

---

258 *See supra* note 3 and surrounding text as to the meaning of "covered institution."

259 An "SCI Entity" is currently defined to include an ATS that trades certain stocks exceeding specific volume thresholds. As noted below, the Commission is proposing in the Regulation SCI Proposal to expand the scope of entities that would be considered SCI Entities. *See* 17 CFR 242.1000 and Regulation SCI Proposal, *supra* note 57.

260 *See* 17 CFR 242.1000 (defining the terms "SCI alternative trading system," "SCI self-regulatory system," and "Exempt clearing agency subject to ARP," and including all of those defined terms in the definition of "SCI Entity"). The definition of "SCI Entities" also includes plan processors and SCI competing consolidators.

amendments to Regulation S-P are adopted (as proposed), broker dealers that operate ATSs would be subject to its requirements in addition to the requirements of Regulation SCI that apply to the ATS (currently and as it would be amended).

The Commission is also proposing to revise Regulation SCI to expand the definition of "SCI entity" to include broker-dealers that exceed an asset-based size threshold or a volume-based trading threshold in national market system ("NMS") stocks, exchange-listed options, agency securities, or U.S. treasury securities.[261] These entities would also be Market Entities[262] for the purposes of the Exchange Act Cybersecurity Proposal, if adopted as proposed. If the amendments to Regulation SCI are adopted and the proposed amendments to Regulation S-P are adopted (as proposed), these additional Market Entities would be subject to Regulation SCI and also would be subject to the requirements of the proposed amendments to Regulation S-P as well as the requirements of the Exchange Act Cybersecurity Proposal (if adopted).

Additionally, broker-dealers and transfer agents that would be subject to the Exchange Act Cybersecurity Proposal also would be subject to some or all of the requirements of Regulation S-P (currently and as it would be amended).[263]

---

261 *See* Regulation SCI Proposal, *supra* note 57. *See* paragraph (a)(1)(i)(D) of the Exchange Act Cybersecurity Proposal proposed Rule. To be subject to the Exchange Act Cybersecurity Proposal, the broker-dealer would either be a carrying broker-dealer, have regulatory capital equal to or exceeding $50 million, have total assets equal to or exceeding $1 billion, or operate as a market maker. *See also* paragraphs (a)(1)(i)(A), (C), (D), and (E) of the Exchange Act Cybersecurity Proposal proposed rule.

262 *See supra* note 71 for a description of the entities subject to the definition of "Market Entity" under the Exchange Act Cybersecurity Proposal.

263 Broadly, Regulation S-P's requirements apply to all broker-dealers, except for "notice-registered broker-dealers" (as defined in 17 CFR 248.30), who in most cases will be deemed to be in compliance with Regulation S-P where they instead comply with the financial privacy rules of the CFTC, and are otherwise explicitly excluded from certain of Regulation S-P's obligations. *See* 17 CFR 248.2(c). For the purposes of this section II.G. of this release, the term "broker-dealer" when used to refer to broker-dealers that are subject to Regulation S-P (currently and as it would be amended) excludes notice-registered broker-dealers. Currently, transfer agents registered with the Commission ("registered transfer agents") (but not transfer agents registered with another appropriate regulatory agency) are subject to Regulation S-P's disposal rule. *See* 17 CFR 248.30(b). However, no transfer agent is currently subject to any other portion of Regulation S-P, including the safeguards rule. *See* 17 CFR 248.30(a). Under the proposed amendments to Regulation S-P, both those transfer agents registered with the Commission, as well as those registered with another appropriate regulatory agency (as defined in 15 U.S.C. 78c(34)(B)) would

c. Policies and Procedures to Address Cybersecurity Risks

i. Different Scope of the Policies and Procedures Requirements

Each of the policies and procedures requirements has a different scope and purpose. Regulation SCI (currently and as it would be amended) limits the scope of its requirements to certain systems of the SCI Entity that support securities market related functions. Specifically, it does and would require an SCI Entity to have reasonably designed policies and procedures applicable to its *SCI systems* and, for purposes of security standards, its *indirect SCI systems*.[264] While certain aspects of the policies and procedures required by Regulation SCI (as it exists today and as proposed to be amended) are designed to address certain cybersecurity risks (among other things),[265] the policies and procedures required by Regulation SCI focus on the SCI entities' operational capability and the maintenance of fair and orderly markets.

Similarly, Regulation S-P (currently and as it would be amended) also has a distinct focus. The policies and procedures required under Regulation S-P, both currently and as proposed to be amended, are limited to protecting a certain type of information—customer records or information and consumer report information[266]—and they apply to such information even when stored outside of SCI systems or indirect SCI systems. Furthermore, these policies and procedures need not address other types of information stored on the systems of the broker-

---

be subject to both the disposal rule and the safeguards rule.

264 *See* 17 CFR 242.1001(a)(1). Regulation SCI also requires that each SCI Entity's policies and procedures must, at a minimum, provide for, among other things, regular reviews and testing of SCI systems and indirect SCI systems, including backup systems, to identify vulnerabilities from internal and external threats. 17 CFR 242.1001(a)(2)(iv).

265 *See* 17 CFR 242.1000 (defining "indirect SCI systems"). The distinction between SCI systems and indirect SCI systems seeks to encourage SCI Entities that their SCI systems, which are core market-facing systems, should be physically or logically separated from systems that perform other functions (*e.g.*, corporate email and general office systems for member regulation and recordkeeping). *See* Regulation Systems Compliance and Integrity, Release No. 34-73639 (Dec. 5, 2014) [79 FR 72251], at 79 FR at 72279-81 ("Regulation SCI 2014 Adopting Release"). Indirect SCI systems are subject to Regulation SCI's requirements with respect to security standards.

266 Or as proposed herein, "customer information" and "consumer information." *See* proposed rules 248.30(e)(5) and (e)(1), respectively.

dealer or transfer agent. Consequently, while Regulation SCI and Regulation S-P may relate to each other, each serves a distinct purpose, and the Commission believes it would be appropriate to apply both requirements to SCI Entities that are covered institutions.

The policies and procedures requirements of the Exchange Act Cybersecurity Proposal are broader in scope with respect to cybersecurity than either the current or proposed forms of Regulation SCI or Regulation S-P. The Exchange Act Cybersecurity Proposal would require Market Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.[267] Unlike Regulation SCI, these requirements would therefore cover both SCI systems and information systems that are not SCI systems. And, unlike Regulation S-P, the proposed requirements would also encompass information beyond customer information and consumer information. As discussed below, however, the narrower scope of the cybersecurity-related requirements discussed in this proposal are not intended to be inconsistent with the policies and procedures that would be required under the Exchange Act Cybersecurity Proposal, despite the differences in scope and purpose, which could reduce duplicative burdens for entities to comply with both requirements.[268]

To illustrate, a covered institution could use one comprehensive set of policies and procedures to satisfy the cybersecurity-related requirements of the Regulation S-P proposed amendments and the cybersecurity-related policies and procedures requirements of the Regulation SCI Proposal and the Exchange Act Cybersecurity Proposal, so long as the cybersecurity-related policies and procedures required under Regulation S-P and Regulation SCI fit within and are consistent with the scope of the policies and procedures required under the Exchange Act Cybersecurity Proposal, and the Exchange Act Cybersecurity Proposal policies

---

[267] *See* paragraphs (b) and (e) of the Exchange Act Cybersecurity Proposal (setting forth the requirements of Covered Entities and Non-Covered Entities, respectively, to have policies and procedures to address their cybersecurity risks).

[268] *See infra* section III.D.1.a.

and procedures also address the more narrowly-focused cybersecurity-related policies and procedures requirements under the Regulation S-P and Regulation SCI proposals.

ii. Consistency of the Policies and Procedures Requirements

The safeguards rule currently requires broker-dealers (but not transfer agents) to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[269] The safeguards rule further provides that these policies and procedures must: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.[270] Additionally, the disposal rule currently requires broker-dealers *and* transfer agents that maintain or otherwise possess consumer report information for a business purpose to properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.[271]

The proposed amendments to the Regulation S-P safeguards rule would require policies and procedures to include a response program for unauthorized access to or use of customer information. Further, the response program would need to be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including procedures, among others, 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 and types of customer information that may have been accessed or used without

---

269 *See* 17 CFR 248.30(a).

270 *See* 17 CFR 248.30(a)(1) through (3).

271 *See* 17 CFR 248.30(b)(2). Regulation S-P currently defines the term "disposal" to mean: (1) the discarding or abandonment of consumer report information; or (2) the sale, donation, or transfer of any medium, including computer equipment, on which consumer report information is stored. *See* 17 CFR 248.30(b)(1)(iii).

authorization;[272] and (2) take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information.[273]

The Exchange Act Cybersecurity Proposal would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks to these proposed requirements of Regulation S-P. First, under the Exchange Act Cybersecurity Proposal, a Covered Entity's[274] policies and procedures would require measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems and the information residing on those systems.[275] Second, under the Exchange Act Cybersecurity Proposal, a Covered Entity's policies and procedures would require incident response measures designed to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure, among other things, the protection of the Covered Entity's information systems and the information residing on those systems.[276] Therefore, the incident response program policies and procedures requirements under the Regulation S-P proposal, which are specifically tailored to address unauthorized access to or use of customer information, would serve a different purpose than, and are not intended to be inconsistent with, the broader cybersecurity and information protection

---

272 Regulation SCI's obligation to take corrective action may include a variety of actions, such as determining the scope of the SCI event and its causes, among others. *See* Regulation SCI 2014 Adopting Release, *supra* note 265, at 72251, 72317. *See also* Regulation SCI sec. 242.1002(a).

273 *See supra* section II.A. As discussed, the response program also would need to have procedures to notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization 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, 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. *See id*.

274 *See supra* note 71 for a description of the entities proposed as "Covered Entities" under the Exchange Act Cybersecurity Proposal.

275 *See* paragraph (b)(1)(iv) of the Exchange Act Cybersecurity Proposal proposed Rule; *see also* Exchange Act Cybersecurity Proposal, *supra* note 57 (discussing this requirement in more detail).

276 *See* paragraph (b)(1)(v) of the Exchange Act Cybersecurity Proposal proposed Rule; *see also* Exchange Act Cybersecurity Proposal, *supra* note 57 (discussing this requirement in more detail).

requirements of the incident response policies and procedures required under the Exchange Act Cybersecurity Proposal.

Accordingly, policies and procedures implemented by a broker-dealer that are reasonably designed in compliance with the requirements of the Exchange Act Cybersecurity Proposal discussed above also should generally satisfy the existing policies and procedures requirements of the Regulation S-P safeguards rule to protect customer records or information against unauthorized access or use that could result in substantial harm or inconvenience to any customer, to the extent that such information is stored electronically and, therefore, falls within the scope of the Exchange Act Cybersecurity Proposal.[277] In addition, reasonably designed policies and procedures implemented by a broker-dealer or transfer agent in compliance with the requirements of the Exchange Act Cybersecurity Proposal also should generally satisfy the existing requirements of the disposal rule related to properly disposing of consumer report information, to the extent that such information is stored electronically and, therefore, falls within the scope of the Exchange Act Cybersecurity Proposal.

In addition, with respect to service providers, the proposed amendments to the safeguards rule would require broker-dealers, other than notice-registered broker-dealers, and transfer agents registered with the Commission or another appropriate regulatory agency to include written policies and procedures within their response programs that require their service providers, pursuant to a written contract, to take appropriate measures that are designed to protect against unauthorized access to or use of customer information, including notification to the broker-dealer

---

[277] To the extent an entity's policies and procedures under the Exchange Act Cybersecurity Proposal would, or do, not satisfy the policies and procedures requirements in this proposal, we believe that the requirements proposed here, such as procedures to notify affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization, could be added to and should fit within the policies and procedures required under the Exchange Act Cybersecurity Proposal that more comprehensively address cybersecurity risks to the extent that such information is stored electronically. Furthermore, any burdens from the proposal that do not fit within the requirements of the Exchange Act Cybersecurity Proposal may relate to the scope of Regulation S-P and would be appropriate given their purpose.

or transfer agent as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security resulting in unauthorized access to a customer information system maintained by the service provider to enable the broker-dealer or transfer agent to implement its response program expeditiously.[278]

The Exchange Act Cybersecurity Proposal also would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks that relate to service providers. First, as part of the Exchange Act Cybersecurity Proposal's risk assessment requirements, a Covered Entity's policies and procedures under that proposal would need to require periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and information residing on those systems.[279] This element of the policies and procedures would need to require that the Covered Entity identify its service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's information systems and any of the Covered Entity's information residing on those systems, and assess the cybersecurity risks associated with the Covered Entity's use of these service providers.[280]

Second, under the Exchange Act Cybersecurity Proposal, a Covered Entity's policies and procedures would require oversight of service providers that receive, maintain, or process the Covered Entity's information, or are otherwise permitted to access the Covered Entity's information systems and the information residing on those systems, pursuant to a written contract between the Covered Entity and the service provider. Through that written contract the service providers would be required to implement and maintain appropriate measures that are designed

---

278 *See supra* section II.A.3.

279 *See* paragraph (b)(1)(i)(A) of the Exchange Act Cybersecurity Proposal proposed Rule; *see also* Exchange Act Cybersecurity Proposal, *supra* note 57, at section II.B.1.a. (discussing this requirement in more detail).

280 *See* paragraph (b)(1)(i)(A)(2) of the Exchange Act Cybersecurity Proposal proposed Rule.

to protect the Covered Entity's information systems and information residing on those systems.[281] Unlike the Exchange Act Cybersecurity Proposal, however, Regulation S-P's proposed policy and procedure requirements related to service providers would specifically require notification to a covered institution as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security resulting in unauthorized access to a customer information system maintained by the service provider, in order to enable the covered institution to implement its response program. Therefore, reasonably designed policies and procedures implemented by a broker-dealer or transfer agent pursuant to the requirements of the Exchange Act Cybersecurity Proposal largely would satisfy these proposed requirements of Regulation S-P, to the extent that such information is stored electronically.[282]

The proposed amendments to the disposal rule would require broker-dealers, other than notice-registered broker-dealers, and transfer agents registered with the Commission or another appropriate regulatory agency that maintain or otherwise possess consumer information or customer information for a business purpose, to properly dispose of this information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. Any broker-dealer or transfer agent subject to the disposal rule would be required to adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information in accordance with this standard.[283]

The Exchange Act Cybersecurity Proposal would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks as this proposed requirement of the disposal rule. First, a Covered Entity's policies and procedures under the

---

281 *See* paragraphs (b)(1)(iii)(B) of the Exchange Act Cybersecurity Proposal proposed Rule; *see also* Exchange Act Cybersecurity Proposal, *supra* note 57 (discussing this requirement in more detail).

282 *See supra* section II.A.3.

283 *See* proposed rule 248.30(c).

Exchange Act Cybersecurity Proposal would need to include controls: (1) requiring standards of behavior for individuals authorized to access the Covered Entity's information systems and the information residing on those systems, such as an acceptable use policy;[284] (2) identifying and authenticating individual users, including but not limited to implementing authentication measures that require users to present a combination of two or more credentials for access verification;[285] (3) establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication;[286] (4) restricting access to specific information systems of the Covered Entity or components thereof and the information residing on those systems solely to individuals requiring access to the systems and information as is necessary for them to perform their responsibilities and functions on behalf of the covered entity;[287] and (5) securing remote access technologies.[288]

Second, under the Exchange Act Cybersecurity Proposal, a Covered Entity's policies and procedures would need to include measures designed to protect the Covered Entity's information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the Covered Entity's information systems and the information that resides on the systems.[289] The periodic assessment would need to take into account: (1) the sensitivity level and importance of the information to the Covered Entity's business operations; (2) whether any of the information is personal information; (3) where and how the information is accessed, stored and transmitted, including the monitoring of information in transmission; (4) the

---

284 *See* paragraph (b)(1)(ii)(A) of the Exchange Act Cybersecurity Proposal proposed Rule.

285 *See* paragraph (b)(1)(ii)(B) of the Exchange Act Cybersecurity Proposal proposed Rule.

286 *See* paragraph (b)(1)(ii)(C) of the Exchange Act Cybersecurity Proposal proposed Rule.

287 *See* paragraph (b)(1)(ii)(D) of the Exchange Act Cybersecurity Proposal proposed Rule.

288 *See* paragraphs (b)(1)(ii)(A) through (E) of the Exchange Act Cybersecurity Proposal proposed Rule; *see also* Exchange Act Cybersecurity Proposal, *supra* note 57 (discussing these requirements in more detail).

289 *See* paragraph (b)(1)(iii)(A) of the Exchange Act Cybersecurity Proposal proposed Rule; *see also* Exchange Act Cybersecurity Proposal, *supra* note 57 (discussing these requirements in more detail).

information systems' access controls and malware protection; and (5) the potential effect a cybersecurity incident involving the information could have on the Covered Entity and its customers, counterparties, members, registrants, or users, including the potential to cause a significant cybersecurity incident.[290] A broker-dealer or transfer agent that implements these requirements of the Exchange Act Cybersecurity Proposal should generally satisfy the proposed requirements of the disposal rule that customer information or consumer information held for a business purpose must be properly disposed of, to the extent that such information is stored electronically and, therefore, falls within the scope of the Exchange Act Cybersecurity Proposal.

For these reasons, the more narrowly focused existing and proposed policies and procedures requirements of Regulation S-P that address particular cybersecurity risks should fit within and are not intended to be inconsistent with the broader policies and procedures required under the Exchange Act Cybersecurity Proposal that more comprehensively address cybersecurity risks. Therefore, it should be appropriate for a broker-dealer or transfer agent to comply with the policies and procedures requirements of the Exchange Act Cybersecurity Proposal (if adopted) and the existing and proposed cybersecurity-related policies and procedures requirements of Regulation S-P with an augmented set of policies and procedures that addresses the requirements of both rules, to the extent that such information is stored electronically and, therefore, falls within the scope of the Exchange Act Cybersecurity Proposal.

d. Disclosure

The proposed amendments to Regulation S-P and Regulation SCI, and the Exchange Act Cybersecurity Proposal also have similar, but distinct, requirements related to notification about certain cybersecurity incidents. The proposed amendments to Regulation S-P would require broker-dealers, other than notice-registered broker-dealers, and transfer agents registered with the Commission or another appropriate regulatory agency to notify affected individuals whose

---

290 *See* paragraphs (b)(1)(iii)(A)(1) through (5) of the Exchange Act Cybersecurity Proposal proposed Rule.

sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.[291] These broker-dealers and transfer agents would not have to provide notice if, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, they determine 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.[292] Moreover, if the cybersecurity incident is or would be an SCI event under the current or proposed requirements of Regulation SCI, a Covered Entity that is or would be subject to the current and proposed requirements of Regulation SCI also could be required to disseminate certain information about the SCI event to certain of its members, participants, or in the case of an SCI broker-dealer, customers, as applicable, promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event has occurred.

Under the Exchange Act Cybersecurity Proposal, a Market Entity that is a Covered Entity would, if it experiences a "significant cybersecurity incident," be required to disclose a summary description of each such incident that has occurred during the current or previous calendar year and to provide updated disclosures if the information required to be disclosed materially changes, including after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes. These disclosures would be required to be made by filing Part II of proposed Form SCIR on EDGAR,[293] posting a copy of the form on its corporate internet website, and, in the case of a

---

291 *See supra* section II.A.4.

292 *See id.*

293 The Exchange Act Cybersecurity Proposal would also require Covered Entities to publicly disclose summary descriptions of the cybersecurity risks that could materially affect the covered entity's business and operations and how the covered entity assesses, prioritizes, and addresses those cybersecurity risks on Part II of proposed Form SCIR. *See* Exchange Act Cybersecurity Proposal, *supra* note 57 (discussing this requirement in more detail).

carrying or introducing broker-dealer, by sending the disclosure to its customers using the same means that the customer elects to receive account statements.

However, despite these similarities, there are distinct differences. First, the Exchange Act Cybersecurity Proposal, Regulation SCI (currently and as proposed to be amended), and Regulation S-P (as proposed to be amended) require different types of information to be disclosed. Second, the disclosures generally would be made to different persons: (1) the public at large in the case of the Exchange Act Cybersecurity Proposal;[294] (2) members, participants, or customers, as applicable, of the SCI entity in the case of the Regulation SCI Proposal;[295] and (3) affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization or, in some cases, all individuals whose information resides in the customer information system that was accessed or used without authorization in the case of Regulation S-P (as proposed to be amended).[296]

Additionally, the notification provided about certain cybersecurity incidents is different under each of these proposals given the distinct goals of each proposal. For example, the

---

294 A carrying broker-dealer would be required to make the disclosures to its customers as well through the means by which they receive account statements. As discussed above, the Exchange Act Cybersecurity Proposal would require Covered Entities to make the public disclosures by 1) filing Part II of Form SCIR with the Commission electronically through the EDGAR system, and 2) posting a copy of the Part II of Form SCIR most recently filed on an easily accessible portion of its business Internet website that can be viewed by the public without the need of entering a password or making any type of payment or other consideration. *See* Exchange Act Cybersecurity Proposal, *supra* note 57 (discussing this requirement in more detail).

295 Regulation SCI, as amended, would require SCI entities to disseminate information required under sec. 242.1002(c)(1) and (c)(2) of Regulation SCI promptly to those members, participants, or in the case of an SCI broker-dealer, customers, of the SCI entity that any responsible SCI personnel has reasonably estimated may have been affected by the SCI event, or to any additional members, participants, or in the case of an SCI broker-dealer, customers, that any responsible SCI personnel subsequently reasonably estimates may have been affected by the SCI event. *See* Regulation SCI Proposal, *supra* note 57 (discussing this requirement in more detail).

296 Under the Regulation S-P and Regulation SCI proposals, there could be circumstances in which a compromise involving sensitive customer information at a broker-dealer that is an SCI entity could result in two forms of notification being provided to customers for the same incident. In addition, under the Exchange Act Cybersecurity Proposal, the broker-dealer also may need to publicly disclose a summary description of the incident via EDGAR and the entity's business Internet website, and, in the case of an introducing or carrying broker-dealer, send a copy of the disclosure to its customers.

requirement to disclose summary descriptions of certain cybersecurity incidents from the current or previous calendar year publicly on EDGAR under the Exchange Act Cybersecurity Proposal serves a different purpose than the customer notification obligation proposed by the Regulation S-P amendments, which would provide more specific information to individuals affected by a security compromise involving their sensitive customer information, so that those individuals may take remedial actions if they so choose.[297] For these reasons, the customer notification requirements of the proposed amendments to Regulation S-P are proposed to apply to covered institutions even if they would be subject to the disclosure requirements of Regulation SCI and/or the Exchange Act Cybersecurity Proposal (as proposed).

a. Request for Comment

The Commission requests comment on the multiple requirements under Regulation S-P (as currently exists and as proposed to be amended), the Exchange Act Cybersecurity Proposal, and Regulation SCI (as currently exists and as proposed to be amended). In addition, the Commission is requesting comment on the following matters:

98. Would it be costly or create practical implementation difficulties to apply the proposed requirements of Regulation S-P to have policies and procedures related to addressing cybersecurity risks to covered institutions if these institutions also would be required to have policies and procedures under Regulation SCI (currently and as it would be amended) and/or the Exchange Act Cybersecurity Proposal (if it is adopted) that address certain cybersecurity risks? If so, explain why. If not, explain why not. Conversely, would there be benefits to this approach? Why or

---

[297] Among other things, the disclosure requirements for certain cybersecurity incidents under the other proposals would serve the following purposes: 1) with respect to the Exchange Act Cybersecurity Proposal, the public disclosure would provide greater transparency about the Covered Entity's exposure to material harm as a result of the cybersecurity incident, and provide a way for market participants to evaluate the Covered Entity's cybersecurity risks and vulnerabilities; 2) with respect to the Regulation SCI Proposal, the dissemination would provide market participants who have been affected by an SCI event, including customers of an SCI broker-dealer, with information they can use to evaluate the event's impact on their trading and other activities to develop an appropriate response.

why not? Are there ways the policies and procedures requirements of the proposed amendments to Regulation S-P could be modified to minimize these potential impacts while achieving the separate goals of this proposal? If so, explain how and suggest specific modifications.

99. Would it be costly or create practical implementation difficulties to require covered institutions to provide notification to affected individuals under Regulation S-P (as proposed), as well as requiring disclosure for certain cybersecurity-related incidents under the Exchange Act Cybersecurity Proposal and Regulation SCI? If so, explain why. If not, explain why not. Conversely, would there be benefits to this approach? Why or why not? Are there ways the notification requirements of the proposed amendments to Regulation S-P could be modified to minimize the potential impacts while achieving the separate goals of this proposal? If so, explain how and suggest specific modifications.

2. Investment Management Cybersecurity

On February 9, 2022, the Commission proposed new rules and amendments relating to the cybersecurity practices and response measures of registered investment advisers, registered investment companies, and business development companies ("covered IM entities").[298] The Investment Management Cybersecurity Proposal would require written cybersecurity policies and procedures reasonably designed to address cybersecurity risks; disclosures regarding certain cybersecurity risks and significant cybersecurity incidents; confidential reporting to the Commission within 48 hours of having a reasonable basis to conclude that a significant

---

[298] *See* Investment Management Cybersecurity Proposal, *supra* note 55. The Commission has pending proposals to reopen comments for the Investment Management Cybersecurity Proposal, and to address cybersecurity risk with respect to different entities, types of covered information or systems, and products. The Commission encourages commenters to review those proposals to determine whether it might affect their comments on this proposal. *See also* Corporation Finance Cybersecurity Proposal, *supra* note 55; Exchange Act Cybersecurity Proposal and Regulation SCI Proposal, *supra* note 57.

cybersecurity incident has occurred or is occurring; and certain cybersecurity-related recordkeeping [299]

If the Investment Management Cybersecurity Proposal and this proposal are both adopted as proposed, covered IM entities would be required to comply with certain similar requirements under both sets of rules. Both sets of rules would require covered IM entities to have policies and procedures regarding measures to detect, respond to, and recover from certain security incidents. Both also address oversight over certain service providers as a part of the required policies and procedures, specifically, requiring the service provider to have appropriate measures that are designed to protect customer, fund, or adviser information, as applicable, pursuant to a written contract.[300]

In addition to similar policies and procedures requirements, covered IM entities would potentially be required to make disclosures to the public and report to the Commission under the Investment Management Cybersecurity Proposal, as well as provide notice to an affected

---

[299] *See* Investment Management Cybersecurity Proposal, *supra* note 55, for a full description of the proposed requirements. The Investment Management Cybersecurity Proposal includes recordkeeping requirements for advisers and funds – proposed amendments to rule 204-2 under the Advisers Act and new rule 38a-2 under the Investment Company Act would require copies of cybersecurity policies and procedures, annual review and written report, documentation related to cybersecurity incidents, including those reported or disclosed, and cybersecurity risk assessments. These recordkeeping requirements center around cybersecurity incidents that jeopardize the confidentiality, integrity, or availability of an adviser or fund's information or information systems, which may include customer information, but also includes other information, such as trading or investment information. In contrast, as discussed in section II.C, the proposed amendments to Regulation S-P require written records documenting compliance with the requirements of the safeguards rule and of the disposal rule.

[300] The Commission proposed the Adviser Outsourcing Proposal in October 2022, which would prohibit registered investment advisers from outsourcing certain services or functions without first meeting minimum due diligence and monitoring requirements. *See* Advisers Outsourcing Proposal, *supra* note 94. Registered investment advisers that would be subject to the Adviser Outsourcing Proposal, if adopted, would also be subject to Regulation S-P, as proposed to be amended. The Adviser Outsourcing Proposal is meant to address service providers that perform covered functions (those necessary for the investment adviser to provide its investment advisory services in compliance with the Federal securities laws, and that, if not performed or performed negligently, would be reasonably likely to cause a material negative impact on the adviser's clients or on the adviser's ability to provide investment advisory services). *See id*. The Commission encourages commenters to review the Adviser Outsourcing Proposal to determine whether it might affect their comments on this proposal.

individual under Regulation S-P, for the same incident. The disclosure and reporting that would be required under the Investment Management Cybersecurity Proposal, however, differ in purpose from the notification that would be provided to individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization under the proposed amendments to Regulation S-P.[301]

The disclosures and reporting contemplated in the Investment Management Cybersecurity Proposal would generally require disclosure of information appropriate to a wider audience of current and prospective advisory clients and fund shareholders, and would better inform their investment decisions, as well as provide reporting to the Commission of significant cybersecurity incidents.[302] For example, advisers would be required to describe cybersecurity risks that could materially affect the advisory services they offer and how they assess, prioritize, and address cybersecurity risks created by the nature and scope of their business. The Investment Management Cybersecurity Proposal would also require disclosure about significant cybersecurity incidents to prospective and current clients, shareholders, and prospective shareholders. These disclosures are intended to improve such persons' ability to evaluate and understand relevant cybersecurity risks and incidents and their potential effect on adviser and fund operations. In contrast, as discussed in section II.A.4.f, the notices required under this proposal would provide more specific information to individuals whose sensitive customer information notification was, or is reasonably likely to have been, accessed or used without authorization, so that they can take remedial actions as they deem appropriate.[303] In other words,

---

301 *See* proposed rule 248.30(b)(4).

302 *See* Investment Management Cybersecurity Proposal, *supra* note 55, proposed Form ADV-C reporting to the Commission includes both general and specific questions related to the significant cybersecurity incident, such as the nature and scope of the incident as well as whether any disclosure has been made to any clients and/or investors.

303 *See* proposed rule 248.30(b)(4)(iv) (includes information regarding a description of the incident, type of sensitive customer information accessed or used without authorization, and what has been done to protect the sensitive customer information from further unauthorized access or use, as well as contact information sufficient to permit an affected individual to contact the covered institution).

the Investment Management Cybersecurity Proposal would provide more general information appropriate to the wider audience of current and prospective clients, shareholders, and prospective shareholders, where this proposal would provide more specific information to individual customers about their customer information.

We intend that even if this proposal as well as the Investment Management Cybersecurity are adopted as proposed, covered IM entities would be able to avoid duplicative compliance efforts, including by, for example, developing one set of policies and procedures addressing all of the requirements from these proposals, using similar descriptions in the disclosures regarding the same incident, or providing the required disclosures as a single notice, where appropriate.[304]

We request comment on the application of the proposal and the Investment Management Cybersecurity Proposal, including the following:

100. How would covered IM entities comply with the policies and procedures requirements contemplated in this proposal? Would they do so by having an integrated set of cybersecurity policies and procedures? If not, what costs and burdens would covered IM entities incur? If so, what operational or practical difficulties may arise because of these combined policies and procedures?
101. Should we modify any of the proposed requirements under this proposal for policies and procedures, service provider oversight, and/or notification of certain incidents, in order to minimize potential duplication of similar requirements under the Investment Management Cybersecurity Proposal?
102. What operational or practical difficulties, if any, may arise for covered IM entities that choose to comply with the disclosure requirements contemplated in this proposal and the Investment Management Cybersecurity Proposal by making

---

[304] *See infra* section III.D.1.a.

substantially similar disclosures to market participants and customers? To the extent the proposed disclosure and notification requirements would result in duplication of effort, what revisions would minimize such duplication but also ensure investors and customers receive the information necessary to protect themselves and make investment decisions?

103. Should we require notice to the Commission when notification is provided to individuals under this proposal? If yes, what form should that notification take (for example, a copy of what is provided to affected individuals under this proposal, or something similar to the significant cybersecurity incident reporting that would be required under the Investment Management Cybersecurity Proposal for covered IM entities)?[305] Should the timing of any such notification to the Commission be the same, before or later than notification to the affected individuals?[306]

104. Do commenters believe there are additional areas of potential duplication or similarities between this proposal and the Investment Management Cybersecurity Proposal that we should address in this proposal? If so, please provide specific examples and whether the duplication or similarities should be addressed and if so, how.

H. Existing Staff No-Action Letters and Other Staff Statements

Staff is reviewing certain of its no-action letters and other staff statements addressing Regulation S-P to determine whether any such letters, statements, or portions thereof, should be withdrawn in connection with any adoption of this proposal. We list below the letters and other staff statements that are being reviewed as of the date of any adoption of the proposed rules or

---

305 *See supra* note 302.

306 The Investment Management Cybersecurity Proposal would require advisers to provide information regarding a significant cybersecurity incident in a structured format through a series of check-the-box and fill-in-the-blank questions on new Form ADV-C. *See* Investment Management Cybersecurity Proposal, *supra* note 55, at section II.B.

following a transition period after such adoption. If interested parties believe that additional letters or other staff statements, or portions thereof, should be withdrawn, they should identify the letter or statement, state why it is relevant to the proposed rule, and how it or any specific portion thereof should be treated and the reason therefor. To the extent that a letter or statement listed relates both to the proposal and another topic, the portion unrelated to the proposal is not being reviewed in connection with any adoption of this proposal.

Letters and Statements to be reviewed

Name of Letter or Statement	**Date Issued**
Staff Responses to Questions about Regulation S-P	January 23, 2003
Certain Disclosures of Information to the CFP Board	March 11, 2011; December 11, 2014
Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies	April 16, 2019

I. Proposed Compliance Date

We propose to provide a compliance date twelve months after the effective date of any adoption of the proposed amendments in order to give covered institutions sufficient time to develop and adopt appropriate procedures to comply with any of the proposed changes and associated disclosure and reporting requirements, if adopted. The Commission recognizes that many covered institutions would review their policies and procedures at least annually. This compliance date would allow covered institutions to develop and adopt appropriate procedures in alignment with a regularly scheduled review. Based on our experience, we believe the proposed compliance date would provide an appropriate amount of time for covered institutions to comply with the proposed rules, if adopted.

We request comment on the proposed compliance date, and specifically on the following items:

105. Is the proposed compliance date appropriate? If not, why not? Is a longer or shorter period necessary to allow covered institutions to comply with one or more

of these particular amendments, if adopted (for example, 18 months if longer, 6 months if shorter)? If so, what would be a recommended compliance date?

106. Should we provide a different compliance date for different types of entities? For example, should we provide a later compliance date for smaller entities, and if so what should this be (for example, 18 or 24 months)? How should we define a "smaller entities" for this purpose? Should any such definition be different depending on the type of covered institution and, if so, how?

III. ECONOMIC ANALYSIS

A. Introduction

The Commission is mindful of the economic effects, including the costs and benefits, of the proposed rules and amendments. Section 3(f) of the Exchange Act, section 2(c) of the Investment Company Act, and section 202(c) of the Investment Advisers Act provide that when engaging in rulemaking that requires us to consider or determine whether an action is necessary or appropriate in or consistent with the public interest, to also consider, in addition to the protection of investors, whether the action will promote efficiency, competition, and capital formation. Section 23(a)(2) of the Exchange Act also requires us to consider the effect that the rules would have on competition, and prohibits us from adopting any rule that would impose a burden on competition not necessary or appropriate in furtherance of the Exchange Act. The analysis below addresses the likely economic effects of the proposed amendments, including the anticipated and estimated benefits and costs of the amendments and their likely effects on efficiency, competition, and capital formation. The Commission also discusses the potential economic effects of certain alternatives to the approaches taken in this proposal.

The proposed amendments would require every broker-dealer,[307] every investment company, every registered investment adviser, and every transfer agent to notify affected

---

[307] Notice registered broker-dealers subject to and complying with the financial privacy rules of the CFTC would be deemed to be in compliance with the proposed provision through the substituted

customers[308] of certain data breaches.[309] To that end, the proposed amendments would require these covered institutions to develop, implement, and maintain written policies and procedures that include an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access or use of customer information, and that includes a customer notification component for cases where sensitive customer information has been, or is reasonably likely to have been, accessed or used without authorization.[310] The proposal would also extend existing rules for safeguarding customer records and information by broadening the scope of covered records to "customer information" and extending the covered population to transfer agents,[311] impose various related recordkeeping requirements,[312] and include in the regulation an existing statutory exception to annual privacy notice requirements.[313]

The proposed amendments would affect the aforementioned covered institutions as well as customers who would receive the proposed notices. The proposed amendments would also have indirect effects on third-party service providers that receive, maintain, process or otherwise are permitted access to customer information on behalf of covered institutions: under the proposed amendments, unauthorized use of or access to sensitive customer information via third-party service providers would fall under the proposed customer notification requirement and

---

compliance provisions of Regulation S-P. *See supra* section II.C.4.

308 As discussed above, "customers" includes not only customers of the aforementioned SEC-registered entities, but also customers of other financial institutions whose information comes into the possession of covered institutions. In addition, with respect to a transfer agent, "customers" refers to "any natural person who is a shareholder securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent." *See* proposed rule 248.30(e)(4).

309 Notification would be required in the event that the sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization, unless such 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 of 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. *See* proposed rule 248.30(b)(4)(i).

310 *See id.; see also supra* section II.A.

311 *See* proposed rule 248.30(a) and 248(e)(3).

312 *See* proposed rule 248.30(d).

313 *See* proposed rule 248.5(e).

covered institutions would be required to enter into a written contract with these service providers regarding measures to protect against unauthorized access to or use of customer information and notification to the covered institution in the event of a breach.[314]

We believe that the main economic effects of the proposal would result from the proposed notification and incident response program requirements applicable to all covered institutions.[315] For reasons discussed later in this section, we believe the proposed extension of existing provisions of Regulation S-P to transfer agents would have more limited economic effects.[316] Finally, we anticipate the proposed recordkeeping requirements, and the proposed incorporation of the existing statutory exception to annual privacy notice requirements, to have minimal economic effects as discussed further below.[317]

Broadly speaking, we believe the main economic benefits of the proposed notification and incident response program requirements, as well as the proposed extension of Regulation S-P to all transfer agents, would result from reduced exposure of the broader financial system to cyberattacks. These benefits would result from covered institutions allocating additional resources towards information safeguards and cybersecurity to comply with the proposed new requirements and/or to avoid reputational harm resulting from the mandated notifications.[318] More directly, customers would benefit from reduced risk of their information being compromised, and—insofar as the proposed notices improve customers' ability to take mitigating actions—by allowing customers to mitigate the effects of compromises that occur nonetheless. The main economic costs from these new requirements would be reputational costs

---

314 *See infra* section III.D.1.b.

315 *See infra* section III.D.1.

316 *See infra* section III.D.2.

317 *See infra* sections III.D.3 and III.D.4.

318 While the scope of the safeguards rule and the proposed amendments is not limited to cybersecurity, in the contemporary context, their main economic effects are realized through their effects on cybersecurity. *See infra* note 343.

borne by firms that would not otherwise have notified customers of a data breach, increased expenditures on safeguards to avoid such reputational costs, and compliance costs related to the development and implementation of required policies and procedures.[319]

Because all states require some form of customer notification of certain data breaches,[320] and many entities are likely to already have response programs in place,[321] we generally anticipate that the economic benefits and costs of the proposed notification requirements will—in the aggregate—be limited. Our proposal would, however, afford many individuals greater protections by, for example, defining "sensitive customer information" more broadly than the current definitions used by certain states;[322] providing for a 30-day notification deadline that is shorter than the timing currently mandated by many states, including in states providing for no deadline or those allowing for various delays; and providing for a more sensitive notification trigger than in most states.[323]

Further, in certain states, state customer notification laws do not apply to entities subject to or in compliance with the GLBA, and our proposal would help ensure customers receive notice of a breach in these circumstances.[324]

For these reasons, the requirements being proposed here would improve customers' knowledge of when their sensitive information has been compromised. Specifically, we expect that the proposed minimum nationwide standard for notifying customers of data breaches, along

---

319 Throughout this economic analysis, "compliance costs" refers to the direct costs that *must* be borne in order to avoid violating the Commission's rules. This includes costs related to the development of policies and procedures required by the regulation, costs related to delivery of the required notices, and the direct costs of any other required action. As used here, "compliance costs" excludes costs that are not required, but may nonetheless arise as a consequences of the Commission's rules (*e.g.*, reputation costs resulting from disclosure of data breach, or increased cybersecurity spending aimed at avoiding such reputation costs).

320 *See infra* section III.C.2.a.

321 *See infra* section III.C.3.

322 *See supra* section II.A.4.b and *infra* section III.D.1.c.iii.

323 *See infra* section III.D.1.c.iv.

324 *See infra* section III.D.1.c.ii.

with the preparation of written policies and procedures for incident response, would result in more customers being notified of data breaches as well as faster notifications for some customers, and that both these effects would improve customers' ability to act to protect their personal information. Moreover, such improved notification would—in many cases—become public and impose additional reputational costs on covered institutions that fail to safeguard customers' sensitive information. We expect that these potential additional reputational costs would increase the disciplining effect on covered institutions, incentivizing them to improve customer information safeguards, reduce their exposure to data breaches, and thereby improve the cyber-resilience of the financial system more broadly.

To the extent that a covered institution does not currently have policies and procedures to safeguard customer information and respond to unauthorized access to or use of customer information, it would bear costs to develop and implement the required policies and procedures for the proposed incident response program. Moreover, transfer agents—who have heretofore not been subject to any of the customer safeguard provisions of Regulation S-P—would face additional compliance costs related to the development of policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information as already required by current Regulation S-P.[325]

As adopting policies and procedures involves fixed costs, doing so is almost certain to impose a proportionately larger compliance cost on smaller covered institutions, which would—in principle—reduce smaller covered institutions' ability to compete with their larger peers (*i.e.*, for whom the fixed costs are spread over more customers).[326] However, given the considerable competitive challenges arising from economies of scale and scope already faced by smaller firms, we do not anticipate that the costs associated with this proposal would significantly alter

---

[325] That is, the existing provisions of Regulation S-P not currently applicable to registered transfer agents. *See* 17 CFR 248.30(a).

[326] *See infra* section III.D.1.a.

these challenges. Similarly, although the proposed amendments may lead to improvements to economic efficiency and capital formation, existing state rules are similar in many respects to this proposal and so we do not expect the proposed amendments to have a significant impact on economic efficiency or capital formation vis-à-vis the baseline.

Many of the benefits and costs discussed below are difficult to quantify. Doing so would involve estimating the losses likely to be incurred by a customer in the absence of mitigation measures, the efficacy of mitigation measures implemented with a given delay, and the expected delay before notification can be provided under the proposed rules. In general, data needed to arrive at such estimates are not available to the Commission. Thus, while we have attempted to quantify economic effects where possible, much of the discussion of economic effects is qualitative in nature. The Commission seeks comment on all aspects of the economic analysis, including submissions of data that could be used to quantify some of these economic effects.

B. Broad Economic Considerations

In a perfectly competitive market, market forces would lead firms to "efficiently" safeguard customers' information: firms that fail to provide the level of safeguards demanded by customers would be driven out of the market by those that do.[327] Among the several assumptions required to obtain this efficient outcome is that of customers having complete and perfect information about the firm's product or service and the processes and service provider relationships by which they are being provided, including customer information safeguards. In the context of covered institutions—firms whose services frequently involve custody of highly-sensitive customer information—this assumption is unrealistic. Customers have little visibility into the internal processes of a firm and its service providers, so it is impossible for them to

---

[327] In the highly stylized standard model of perfect competition presented in many introductory micro-economic texts, this "efficient" safeguarding of customer information would correspond to producing the one homogenous good (*i.e.*, a service of a certain quality) demanded by the representative customer at its marginal cost. *See, e.g.*, David M. Kreps, A Course in Microeconomic Theory, Princeton University Press (1990).

directly observe whether a firm is employing adequate customer information safeguards.[328] Moreover, firms often lack incentives to disclose when such information is compromised (and likely have substantial incentives to avoid such disclosures), limiting customers' (current or prospective) ability to penalize (*i.e.*, avoid) covered institutions who fail to protect customer information.[329] The resulting information asymmetry prevents market forces from yielding economically efficient outcomes. This market failure serves as the economic rationale for the proposed regulatory intervention.

The information asymmetry about specific information breaches that have occurred, and—more generally—about covered institutions' efforts at avoiding such breaches, can lead to two inefficiencies. First, the information asymmetry prevents individual customers whose information has been compromised from taking timely actions (*e.g.*, increased monitoring of account activity, or placing blocks on credit reports) necessary to mitigate the consequences of such compromises. Second, the information asymmetry can lead covered institutions to generally devote too little effort (*i.e.*, "underspend") toward safeguarding customer information, thereby increasing the probability of information being compromised in the first place.[330] In other words, information asymmetry prevents covered institutions that spend more effort on safeguarding customer information from having customers recognize their extra efforts.

---

328 Here, "adequate safeguards" can be thought of as the level of safeguards that would be demanded by the representative customer in a world where the level of firms' efforts (and the costs of these efforts) were observable.

329 The release of information about data breaches can lead to loss of customers, reputational harm, litigation, or regulatory scrutiny. *See, e.g.,* Press release, U.S. Fed. Trade Comm'n, *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach* (July 22, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach.

330 For example, in a recent survey of financial firms, 58% of the respondents self-reported "underspending" on cybersecurity. *See* McKinsey & Co. and Institute of International Finance, *IIF/McKinsey Cyber Resilience Survey* (Mar. 2020) ("IIF/McKinsey Report"), https://www.iif.com/portals/0/Files/content/cyber_resilience_survey_3.20.2020_print.pdf. A total of 27 companies participated in the survey, with 23 having a global footprint. Approximately half of respondents were European or U.S. Globally Systemically Important Banks (G-SIBs). *See also* Investment Management Cybersecurity Proposal *supra* note 55.

The proposed amendments could mitigate these inefficiencies in three ways. First, by ensuring customers receive timely notice when their information is compromised, they would allow customers to take appropriate remedial actions. Second, by revealing when such events occur, they would help customers to draw inferences about a covered institution's efforts toward protecting customer information which could help inform their choice of covered institution,[331] and in so doing influence firms' efforts toward protecting customer information.[332] Third, by imposing a regulatory requirement to develop, implement, and maintain policies and procedures, the proposed amendments might further enhance firms' cybersecurity preparations and would restrict firms' ability to limit efforts in these areas and thereby mitigate the inefficiency from a competitive "race to the bottom."[333]

The effectiveness of the proposed amendments at mitigating these problems would depend on several factors. First, it would depend on the degree to which customer notification provides actionable information to customers that helps mitigate the effects of the compromise of sensitive customer information. Second, it would also depend on the degree to which the prospect of issuing such notices—and the prospect of resulting reputational harm, litigation, and regulatory scrutiny—helps alleviate underspending on safeguarding customer information.[334] Finally, the effectiveness of the proposed amendments would also depend on the extent to which

---

[331] In the case of transfer agents such effects would be mediated through firms' choice of transfer agents and therefore less direct. Nonetheless we believe that, all else being equal, firms would prefer to avoid employing the services of transfer agents that allow their investors' information to be compromised.

[332] *See, e.g.,* Richard J. Sullivan & Jesse Leigh Maniff, *Data Breach Notification Laws*, 101 ECON. REV. 65 (2016) ("Sullivan & Maniff").

[333] The "bottom" in such a race is a level of cybersecurity spending that is too low from an efficiency standpoint.

[334] Although empirical evidence on the effectiveness of notification breach laws is quite limited, extant studies suggest that such laws protect consumers from harm. *See* Sasha Romanosky, Rahul Telang, & Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y. ANSYS & MGMT 256 (2011). *See also* Sullivan & Maniff, *supra* note 332.

they induce improvements to existing practices (*i.e.*, the extent to which they strengthen customer safeguards and increase notification relative to the baseline).

C. Baseline

The market risks and practices, regulation, and market structure relevant to the affected parties in place today form the baseline for our economic analysis. The parties directly affected by the proposed amendments ("covered institutions"[335]) include every broker-dealer (3,509 entities),[336] every investment company (13,965 distinct legal entities),[337] every investment adviser (15,129 entities)[338] registered with the Commission, and every transfer agent (402 entities)[339] registered with the Commission or another appropriate regulatory agency. In addition, the proposed amendments would affect current and prospective customers of covered institutions as well as certain service providers to covered institutions.[340]

1. Safeguarding Customer Information -- Risks and Practices

Over the last two decades, the widespread adoption of digitization and the migration toward internet-based products and services has radically changed the manner in which firms interact with customers. The financial services industry has been at the forefront of these trends and now represents one the most digitally mature sectors of the economy.[341] This progress came with a cost: increased exposure to cyberattacks that threaten not only the financial firms

---

335 *See infra* section III.C.3.

336 Of these, 502 are dually-registered as investment advisers. *See infra* section III.C.3.a.

337 Many of these distinct legal entities represent different series of a common registrant. Moreover, many of the registrants are themselves part of a larger family of companies. We estimate there are 1,093 such families. *See infra* section III.C.3.c.

338 *See infra* section III.C.3.b.

339 *See infra* section III.C.3.d.

340 *See infra* section III.C.3.e.

341 *See* Michael Grebe, et al., *Digital Maturity Is Paying Off*, BCG (June 7, 2008), *available at* https://www.bcg.com/publications/2018/digital-maturity-is-paying-off.

themselves, but also their customers. Cyber threat intelligence surveys consistently find the financial sector to be among the most attacked industries.[342]

The trend toward digitization has increasingly turned the problem of safeguarding customer records and information into one of cybersecurity.[343] Because financial firms are part of one of the most attacked industries, the problem of cybersecurity is acute, as the customer records and information in their possession can be quite sensitive (*e.g.*, personal identifying information, bank account numbers, financial transactions) and the compromise of which could lead to substantial harm.[344] Not surprisingly, the financial sector is one of the biggest spenders on cybersecurity measures: a recent survey found that non-bank financial firms spent an average of approximately 0.4% of revenues—or $2,348/employee/year—on cybersecurity.[345]

While spending on cybersecurity measures in the financial services industry is considerable, it may nonetheless be inadequate—even in the estimation of financial firms themselves. According to one recent survey, 58% of financial firms self-reported

---

342 *See, e.g.*, IBM, *X-Force Threat Intelligence Index 2022* (Feb. 2022), *available at* https://www.ibm.com/security/data-breach/threat-intelligence.

343 This is not to say that this is exclusively a problem of cybersecurity. Generally however, the risks associated with purely physical forms of compromise are of a smaller magnitude, as large-scale compromise using physical means is cumbersome. The largest publicly known incidents of compromised information have appeared to involve electronic access to digital records, as opposed to physical access to records or computer hardware. For a partial list of recent data breaches and their causes *see*, *e.g.*, Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (Nov. 8, 2022), *available at* https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited Dec. 29, 2022); Drew Todd, *Top 10 Data Breaches of All Time*, SECUREWORLD (Sept. 14, 2022), *available at* https://www.secureworld.io/industry-news/top-10-data-breaches-of-all-time (last visited Dec. 29, 2022).

344 *See supra* note 342.

345 Julie Bernard et al., *Reshaping the Cybersecurity Landscape,* DELOITTE INSIGHTS (July 24, 2020), *available at* https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (last visited Feb. 13, 2023). These spending totals represent self-reported shares of information technology budgets devoted to cybersecurity. As such they are unlikely to include additional indirect costs such as the cost of employee time spent on compliance with cybersecurity procedures.

"underspending" on cybersecurity measures.[346] And while adoption of cybersecurity best practices has been accelerating overall, some firms continue to lag in their adoption.[347]

As discussed in more detail below, the Commission does not currently require covered institutions to notify customers (or the Commission) in the event of a data breach, so statistics relating to data breaches at covered institutions are not readily available. However, data compiled from notifications required under various state laws[348] indicates that in 2021 the number of data breaches reported in the U.S. rose sharply to 1,862—a 68% increase over the prior year.[349] Of these, 279 (15%) were reported by firms in the financial services industry. It is estimated that the average total cost of a data breach for a U.S. firm in 2022 was $9.44/ million.[350] The bulk of these costs is attributed to detection and escalation (33%), lost business (32%), and post-breach response (27%); customer notification is estimated to account for only a small fraction (7%) of these costs.[351] Thus, for the U.S. financial industry as a whole, this implies aggregate notification costs under the baseline on the order of $200 million, which—

---

346 *See* IIF/McKinsey Report, *supra* note 330.

347 *See* EY and Institute of International Finance, *12th Annual EY/IIF Global Bank Risk Management Survey* (2022), *available at* https://www.iif.com/portals/0/Files/content/32370132_ey-iif_global_bank_risk_management_survey_2022_final.pdf (stating 58% of surveyed banks' Chief Risk Officers cite "inability to manage cybersecurity risk" as the top strategic risk); s*ee also* Sage Lazzaro, *Public cloud security 'just barely adequate,' experts say,* VENTUREBEAT (July 9, 2021), *available at* https://venturebeat.com/business/public-cloud-security-just-barely-adequate-experts-say/ (noting that the majority of surveyed security professionals believe the cloud service providers "should be doing more on security.")

348 *See infra* section II.A.4.

349 *See* Identity Theft Resource Center, Data Breach Annual Report (Jan. 2022) ("ITRC Data Breach Annual Report"), *available at* https://www.idtheftcenter.org/wp-content/uploads/2022/04/ITRC_2021_Data_Breach_Report.pdf.

350 An increase of 4% over the prior year; *see* IBM, *Cost of a Data Breach Report 2022* (July 2022) ("IBM Cost of Data Breach Report"), https://www.ibm.com/downloads/cas/3R8N1DZJ. While the report does not provide estimates for U.S. financial services firms specifically, it estimates that world-wide, the cost of a data breach for financial services firms averaged $5.97 million, and that average costs for U.S. firms are approximately twice the world-wide average.

351 *See id*.

given the greater exposure of financial firms to cyber threats—almost surely represent a lower bound.[352]

2. Regulation

Two features of the existing regulatory framework are most relevant to the proposed amendments. First are the regulations already in place that require covered institutions to notify customers in the event that their information is compromised in some way. Second are regulations that affect covered institutions' efforts toward safeguarding customers' information. While the relevance of the former is obvious, the latter is potentially more significant: regulations aimed at increasing firms' efforts toward safeguarding customer information reduce the need for data breach notifications in the first place. In this section, we summarize these two aspects of the regulatory framework.

a. Customer Notification Requirements

All 50 states and the District of Columbia impose some form of data breach notification requirement under state law. These laws vary in detail from state to state, but have certain common features. State laws trigger data breach notification obligations when some type of "personal information" of a state's resident is either accessed or acquired in an unauthorized manner, subject to various common exceptions. For the vast majority of states (47), a notification obligation is triggered only when there is unauthorized acquisition, while a handful of states (4) require notification whenever there is unauthorized access.[353]

Generally, states can be said to adopt either a basic or an enhanced definition of personal information. A typical example of a basic definition specifies personal information as the

---

352 The $200 million figure is based on 7% (the customer notification portion) of an average cost of $9.44 million multiplied by 279 data breaches. *See supra* notes 349 and 350.

353 *See, e.g.*, notification requirements in California (Cal. Civ. Code sec. 1798.82(a)) and Texas (Tex. Bus. & Com. Code sec. 521.002) triggered by the acquisition of certain information by an unauthorized person, as compared to notification requirements in Florida (Fla. Stat. sec. 501.171) and New York (N.Y. Gen. Bus. Law sec. 899-AA) triggered by unauthorized access to personal information. "States" in this discussion includes the 50 U.S. states and the District of Columbia, for a total of 51. All state law citations are to the August 2022 versions of state codes.

customer name linked to one or more pieces of nonpublic information such as Social Security number, driver's license number (or other state identification number), or financial account number together with any required credentials to permit access to said account.[354] A typical enhanced definition will include additional types of nonpublic information that trigger the notification requirement; examples include: passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.[355] Enhanced definitions would also trigger notification when a username or email address in combination with a password or security question and answer that would permit access to an online account is compromised.[356] Most states (39) adopt some form of enhanced definition, while a minority (12) adopt a basic definition.

Most states (43) provide an exception to the notification requirement if, following a breach of security, the entity investigates and determines that there is no reasonable likelihood that the individual whose personal information was breached has experienced or will experience certain harms ("no-harm exception").[357] Although the types of harms vary by state, they most commonly include: "harm" generally (12), identity theft or other fraud (10), misuse of personal information (8). Figure 1 plots the frequency of the various types of harms referenced in states' no-harm exceptions.

---

354 *See, e.g.*, Kan. Stat. sec. 50-7a01(g) or Minn. Stat. sec. 325E.61(e).

355 *See, e.g.*, Md. Comm. Code sec. 14-3501, (defining "personal information" to include credit card numbers, health information, health insurance information, and biometric data such as retina or fingerprint).

356 *See*, *e.g.*, Arizona Code sec. 18-551 (defining "personal information" to include an individual's user name or email address, in combination with a password or security question and answer, that allows access to an online account).

357 *See, e.g.*, Fla. Stat. sec. 501.171(4)(c). A variation on this exception provides for notification only if the investigation reveals a risk of misuse. *See*, *e.g.*, Utah Code 13-44-202(1). Eight states, including California and Texas, do not have a no-harm exception.

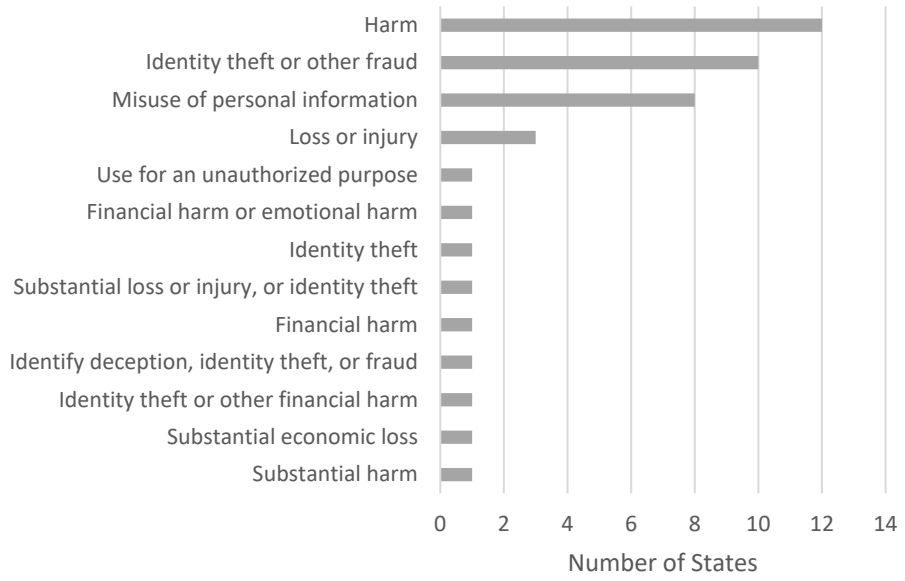

Figure 1: Frequency of types of harms referenced by state statutes with no-harm exceptions to notification requirements. Data source: State law in 2022.

In general, state laws provide a general principle for timing of notification (*e.g.*, delivery shall be made "without unreasonable delay," or "in the most expedient time possible and without unreasonable delay").[358] Some states augment the general principle with a specific deadline (*e.g.*, notice must be made "in the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of determination that the breach occurred" unless certain exceptions apply."[359] Figure 2 plots the frequency of different notification deadlines in state laws.

---

358 *See, e.g.*, Cal. Civ. Code sec. 1798.82(a) (disclosure to be made "in the most expedient time possible and without unreasonable delay" but allowing for needs of law enforcement and measures to determine the scope of the breach and restore the system).

359 *See, e.g.*, Colo. Reg. Stat. sec. 6-1-716 (notice to be made "in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system"); Fla. Stat. sec. 501.171(4)(a) (notice to be made "as expeditiously as practicable and without unreasonable delay … but no later than 30 days after the determination of a breach" unless delayed at the request of law enforcement or waived pursuant to the state's no-harm exception).

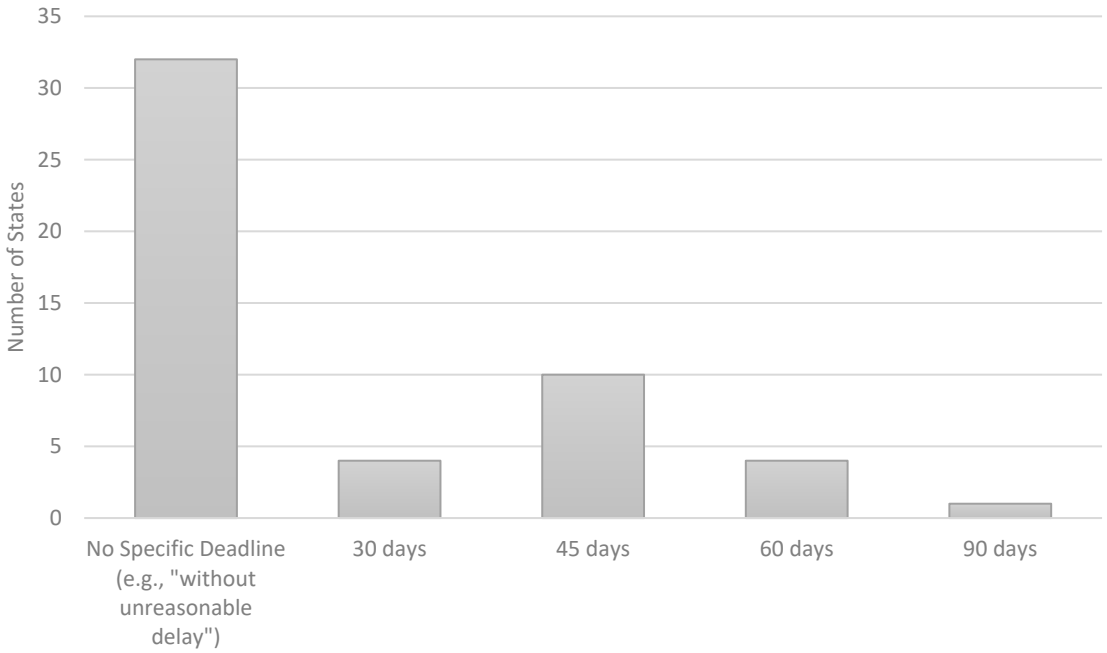

Figure 2: Frequency of notification deadlines in state laws. Data source: State law in 2022.

State laws generally require persons or entities that own or license computerized data that includes private information to notify residents of the state when a data breach results in the compromise of their private information. In addition, state laws generally require persons and entities that do not own or license such computerized data, but that maintain such computerized data for other entities, to notify the affected entity in the event of a data breach (so as to allow that entity to notify affected individuals).[360] Therefore, we understand that all proposed covered institutions are already complying with one or more state notification laws. Variations in these state laws, however, could result in residents of one state receiving notice while residents of another receive no notice, or receive it later, for the same data breach incident.

Covered institutions may use service providers to perform certain business activities and functions, such as trading and order management, information technology functions and cloud

---

360 *See, e.g.*, Cal. Civ. Code sec. 1798.82(b); D.C. Code 28-3852(b); N.Y. Gen. Bus. Law sec. 899-AA(3); Tex. Bus. & Com. Code sec. 521.053(c). South Dakota does not have such a provision (SDCL sec. 22-40-19 through 22-40-26). In some states, notification from the service provider to the information owner is required only in the case of fraud or misuse. *See, e.g.*, Miss. Code sec.75-24-29 (requiring notification if the information was or is reasonably believed to have been acquired by an unauthorized person for fraudulent purposes); Colo. Rev. Stat. sec. 6-1-716 (requiring notification if misuse of personal information about a Colorado resident occurred or is likely to occur).

computing services. As a result of this outsourcing, service providers may receive, maintain, or process customer information, or be permitted to access it, and therefore a security incident at the service provider could expose information at or belonging to the covered institution. In some cases, these service providers may be required to notify customers directly under state notification laws (*i.e.*, when the service provider owns or licenses the customer data). We anticipate however, that more frequently service providers would fall under provisions of state laws that require persons and entities that maintain computerized data to notify the data owners in the event of a breach.[361] We also understand contracts between covered institutions and service providers could, and may already, call for the service provider to notify the covered institution of a data breach. Thus, we anticipate that most service providers contracting with covered institutions that would be affected by this proposal are already notifying covered institutions of data breaches, pursuant to either contract or state law.[362]

b. Customer Information Safeguards

Regulation S-P currently requires all currently covered institutions to adopt written policies and procedures reasonably designed to: (i) insure the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (iii) protect against unauthorized access to or use of customer records and information that could result in substantial harm or inconvenience to any customer.[363]

---

361 Many service providers may not own the data and may not have knowledge as to which customers are potentially affected by a data breach (e.g., database, email, or server hosting providers). In such cases, it would generally not be possible for service providers to notify affected customers directly.

362 Several state laws provide that a covered institution may contract with the service provider such that the service provider directly notifies affected individuals of a data breach. We do not have information on the frequency of such arrangements. *See*, *e.g.*, Fla. Stat. sec. 501.171(6)(b); Ala. Code sec. 8-38-8.

363 *See* Reg. S-P Release, *supra* note 2; *see also* Disposal Rule Adopting Release, *supra* note 32 (requiring written policies and procedures under Regulation S-P). *See* Compliance Programs of Investment Companies and Investment Advisers, Investment Advisers Act Release No. 2204 (Dec. 17, 2003) [68 FR 74714 (Dec. 24, 2003)], at n.22 ("Compliance Program Release") (stating

Covered institutions that hold transactional accounts for consumers may also be subject to Regulation S-ID.[364] Such entities must develop and implement a written identity theft program that includes policies and procedures to identify relevant types of identity theft red flags, detect the occurrence of those red flags, and respond appropriately to the detected red flags.[365] As some compromise of customer information is generally a prerequisite for identity theft, it is reasonable to expect that some of the policies and procedures implemented to effect compliance with Regulation S-ID incorporate red flags related to the potential compromise of customer information.[366]

Some covered institutions may also be subject to other regulators' rules implicating customer information safeguards. Transfer agents supervised by one of the banking agencies, would be subject to the Banking Agencies' Incident Response Guidance.[367] The Banking Agencies' guidelines require covered financial institutions to develop a response program covering assessment, notification to relevant regulators and law enforcement, incident containment, and customer notice.[368] The guidelines require customer notification if misuse of

---

expectation that policies and procedures would address safeguards for the privacy protection of client records and information and noting the applicability of Regulation S-P).

364 Regulation S-ID applies to "financial institutions" or "creditors" that offer or maintain "covered accounts." Entities that are likely to qualify as financial institutions or creditors and maintain covered accounts include most registered brokers, dealers, and investment companies, and some registered investment advisers. *See* Reg. S-P Release, *supra* note 2; *see also* Identity Theft Red Flag Rules, Investment Advisers Act Release No. 3582 (Apr. 10, 2013) [78 FR 23637 (Apr. 19, 2013)] ("Identity Theft Release").

365 In addition, affected entities must also periodically update their identity theft programs. *See* Reg. S-P Release, *supra* note 2. Other rules also require updates to policies and procedures at regular intervals: s*ee*, *e.g*., Rule 38a-1 under the Investment Company Act; FINRA Rule 3120 (Supervisory Control System); and FINRA Rule 3130 (Annual Certification of Compliance and Supervisory Processes).

366 In a 2017 Risk Alert, the SEC Office of Compliance Inspections and Examinations noted that in a sampling of registrants, nearly all broker-dealers and most advisers had specific cybersecurity and Regulation S-ID policies and procedures. *See* EXAMS Risk Report, Observations from Cybersecurity Examinations (Aug. 7, 2017), *available at* https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf. *See also* Identity Theft Release, *supra* note 364.

367 *See* Banking Agencies' Incident Response Guidance, *supra* note 47.

368 *See id.* at Supplement A, section II.A.

sensitive customer information "has occurred or is reasonably possible."[369] They also require notices to occur "as soon as possible," but permit delays if "an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay."[370] Under the guidelines, "sensitive customer information" means "a customer's name, address, or telephone number, in conjunction with the customer's Social Security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account."[371] In addition "any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number" is also considered sensitive customer information under the guidelines.[372] The guidelines also state that the OCC Information Security Guidance directs every financial institution to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.[373]

In addition, certain ATSs are subject to obligations regarding their systems that relate to securities market functions under Regulation SCI aimed at enhancing the capacity, integrity, resiliency, availability, and security of those systems.[374]

We also understand that advisers to private funds may be subject to the Federal Trade Commission's recently amended Standards for Safeguarding Customer Information ("FTC Safeguards Rule") that contains a number of modifications to the existing rule with respect to

---

369 *See id.* at Supplement A, section III.A.

370 *See id.* at Supplement A, section III.A.

371 *See id.* at Supplement A, section III.A.1.

372 *See id.* at Supplement A, section III.A.1.

373 *See id.* at Supplement A, section I.C.

374 *See* Rule 1001 of Regulation SCI. *See supra* note 57.

data security requirements to protect customer financial information.[375] The FTC Safeguards Rule generally requires financial institutions to develop, implement, and maintain a comprehensive information security program that consists of the administrative, technical, and physical safeguards the financial institution uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.[376] The rule also requires financial institutions to design and implement a comprehensive information security program with various elements, including incident response. In addition, it requires financial institutions to take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for customer information and require those service providers by contract to implement and maintain such safeguards.[377]

A variety of guidance is available to institutions seeking to address information security risk, particularly through the development of policies and procedures. These include the NIST and CISA voluntary standards[378] discussed elsewhere in this release, both of which include assessment, containment, and notification elements similar to this proposal. We do not have extensive data spanning all types of covered institutions on their use of these or similar guidelines or on their development of written policies and procedures to address incident response. However, past Commission examination sweeps of broker-dealers and investment advisers suggest that such practices are widespread.[379] Thus, we believe that institutions seeking

---

375 Issuers that are excluded from the definition of investment company – such as private funds that are able to rely on section 3(c)(1) or 3(c)(7) of the Investment Company Act – would not be subject to Regulation S-P. However, registered investment advisers are covered institutions for purposes of this proposal.

376 16 CFR 314.2(c). The FTC Safeguards Rule does not contain a notification requirement.

377 16 CFR 314.4(d).

378 *See* NIST Computer Security Incident Handling Guide and CISA Cybersecurity Incident Response Playbook *supra* note 81.

379 *See* OCIE, SEC, *Cybersecurity Examination Sweep Summary* (Feb. 3, 2015), *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf (written policies and procedures, for both the broker-dealers (82%) and the advisers (51%), discuss mitigating the effects of a cybersecurity incident and/or outline the plan to recover from such an incident. Similarly, most of the broker-dealers (88%) and many of the advisers (53%) reference

to develop written policies and procedures likely would have encountered these and similar standards and may have included the critical elements of assessment and containment, as well as notification; we request public comment on this assumption.

c. Annual Notice Delivery Requirement

Under the baseline,[380] a broker-dealer, investment company, or registered investment adviser must generally provide an initial privacy notice to its customers not later than when the institution establishes the customer relationship and annually after that for as long as the customer relationship continues.[381] If an institution chooses to share nonpublic personal information with a nonaffiliated third party other than as disclosed in an initial privacy notice, the institution must generally send a revised privacy notice to its customers.[382]

The types of information required to be included in the initial, annual, and revised privacy notices are identical. Each privacy notice must describe the categories of information the institution shares and the categories of affiliates and non-affiliates with which it shares nonpublic personal information.[383] The privacy notices also must describe the type of information the institution collects, how it protects the confidentiality and security of nonpublic personal information, a description of any opt out right, and certain disclosures the institution makes under the FCRA.[384]

---

published cybersecurity risk management standards).

380 For the purposes of the economic analysis, the baseline does not include the exception to the annual notice delivery requirement provided by the FAST Act. This statutory exception was self-effectuating and became effective on Dec. 4, 2015. *See supra* note 221 and accompanying text.

381 17 CFR 248.4 and 248.5.

382 17 CFR 248.8. Regulation S-P provides certain exceptions to the requirement for a revised privacy notice, including if the institution is sharing as permitted under rules 248.13, 248.14, and 248.15 or to a new nonaffiliated third party that was adequately disclosed in the prior privacy notice.

383 *See* 17 CFR 248.6(a)(2)-(5) and 248.6(a)(9).

384 *See* 17 CFR 248.6(a)(1) (information collection); 248.6(a)(8) (protecting nonpublic personal information), 248.6(a)(6) (opt out rights); 248.6(a)(7) (disclosures the institution makes under section 603(d)(2)(A)(iii) of the FCRA (15 U.S.C. 1681a(d)(2)(A)(iii)), notices regarding the ability to opt out of disclosures of information among affiliates).

3. Market Structure

The amendments being proposed here would affect four categories of covered institutions: broker-dealers other than notice-registered broker-dealers, registered investment advisers, investment companies, and transfer agents registered with the Commission or another appropriate regulatory agency. These institutions compete in several distinct markets and offer a wide range of services, including: effecting customers' securities transactions, providing liquidity, pooling investments, transferring ownership in securities, advising on financial matters, managing portfolios, and consulting to pension funds. Many of the larger covered institutions belong to more than one category (*e.g.*, a dually-registered broker-dealer / investment adviser), and thus operate in multiple markets. In the rest of this section we first outline the market for each class of covered institution and then consider service providers.

a. Broker-Dealers

Registered broker-dealers include both brokers (persons engaged in the business of effecting transactions in securities for the account of others)[385] as well as dealers (persons engaged in the business of buying and selling securities for their own accounts).[386] Most brokers and dealers maintain customer relationships, and are thus likely to come into the possession of sensitive customer information.[387] In the market for broker-dealer services, a relatively small set of large- and medium-sized broker-dealers dominate while thousands of smaller broker-dealers compete in niche or regional segments of the market.[388] Broker-dealers provide a variety of services related to the securities business, including (1) managing orders for customers and routing them to various trading venues; (2) providing advice to customers that is in connection with and reasonably related to their primary business of effecting securities transactions; (3)

---

385 *See* 15 U.S.C. 78c(a)(4).

386 *See* 15 U.S.C. 78c(a)(5).

387 Such information would include the customers' names, tax numbers, telephone numbers, broker, brokerage account numbers, etc.

388 *See* Regulation Best Interest: The Broker-Dealer Standard of Conduct, Release No. 34-86031 (June 5, 2019) [84 FR 33318 (July 12, 2019)], at 33406.

holding customers' funds and securities; (4) handling clearance and settlement of trades; (5) intermediating between customers and carrying/clearing brokers; (6) dealing in corporate debt and equities, government bonds, and municipal bonds, among other securities; (7) privately placing securities; and (8) effecting transactions in mutual funds that involve transferring funds directly to the issuer. Some broker-dealers may specialize in just one narrowly defined service, while others may provide a wide variety of services.

Based on an analysis of FOCUS filings from year-end 2021, there were 3,509 registered broker-dealers. Of these, 502 were dually-registered as investment advisers. There were over 72 million customer accounts reported by carrying brokers.[389] However, the majority of broker-dealers are not "carrying broker-dealers" and therefore do not report the numbers of customer accounts.[390] Therefore, we expect that this figure of 72 million understates the total number of customer accounts because many of the accounts at carrying broker dealers have corresponding accounts with non-carrying brokers. Both carrying and non-carrying broker-dealers potentially possess sensitive customer information for the accounts that they maintain.[391] Because non-carrying broker-dealers do not report on the numbers of customer accounts, it is not possible to ascertain with any degree of confidence the distribution of customer accounts across the broader broker-dealer population.

b. Investment Advisers

Registered investment advisers provide a variety of services to their clients, including: financial planning advice, portfolio management, pension consulting, selecting other advisers, publication of periodicals and newsletters, security rating and pricing, market timing, and conducting educational seminars.[392] Although advisers engaged in any of these activities are

---

389 Form X-17A-5 Schedule I, Item I8080 (as of July 1, 2022).

390 *See* General Instructions to Form CUSTODY (as of Sept. 30, 2022).

391 This information includes name, address, age, and tax identification or Social Security number. *See* FINRA Rule 4512.

392 *See* Form ADV.

likely to possess sensitive customer information, the degree of sensitivity will vary widely across advisers. An adviser that offers advice only on personalized investment advice may not hold much customer information beyond address, payment details, and the customer's overall financial condition. On the other hand, an adviser that performs portfolio management services will possess account numbers, tax identification numbers, access credentials to brokerage accounts, and other highly sensitive information.

Based on Form ADV filings received up to June 1, 2022, there were 15,129 SEC-registered investment advisers with a total of 51 million individual clients[393] and $128 trillion in assets under management.[394] Practically all (97%) of these advisers reported providing portfolio management services to their clients.[395] Over half (56%) reported having custody[396] of clients' cash or securities either directly or through a related person with client funds in custody totaling $46 trillion.[397]

---

393 Form ADV, Items 5D(a-b) (as of June 1 2022).

394 Broadly, regulatory assets under management is the current value of assets in securities portfolios for which the adviser provides continuous and regular supervisory or management services. *See* Form ADV, Part 1A Instruction 5.b.

395 Form ADV, Items 5G(2-5) (as of June 1 2022).

396 Here, "custody" means "holding, directly or indirectly, client funds or securities, or having any authority to obtain possession of them." An adviser also has "custody" if "a related person holds, directly or indirectly, client funds or securities, or has any authority to obtain possession of them, in connection with advisory services [the adviser] provide[s] to clients." *See* 17 CFR 275.206(4)-2(d)(2).

397 Form ADV, Items 9A and 9B (as of June 1 2022).

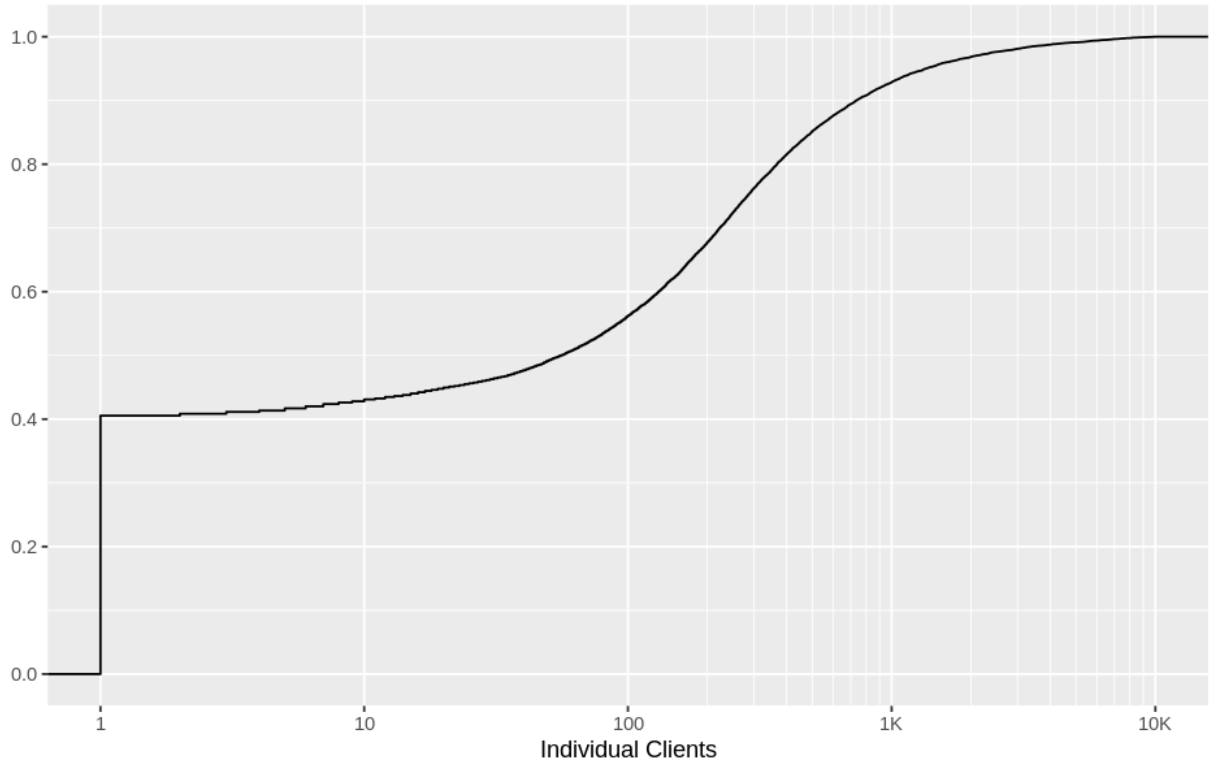

Figure 3: Cumulative distribution of the number of clients across investment advisers. Data source: Form ADV, Items 5D(a-b) (as of June 1, 2022).

Figure 3 plots the cumulative distribution of the number of individual clients handled by SEC-registered investment advisers. The distribution is highly skewed: thirteen advisers each have more than one million clients while 95% of advisers have fewer than 2,000 clients. Many such advisers are quite small, with half reporting fewer than 62 clients.[398]

Similarly, most SEC-registered investment advisers are limited geographically. SEC-registered investment advisers must generally make a "notice filing" with a state in which they have a place of business or six or more clients.[399] Figure 4 plots the frequency distribution of the number the number of such filings. Based on notice filings, half of SEC-registered investment advisers operate in fewer than four states, and 38% operate in only one state.[400]

---

398 Form ADV, Item 5.A (as of June 1, 2022).

399 *See* General Instructions to Form ADV (as of June 1, 2022).

400 Form ADV, Item 2.C (as of June 1 2022). This includes 1,867 advisers who do not make any notice filings.

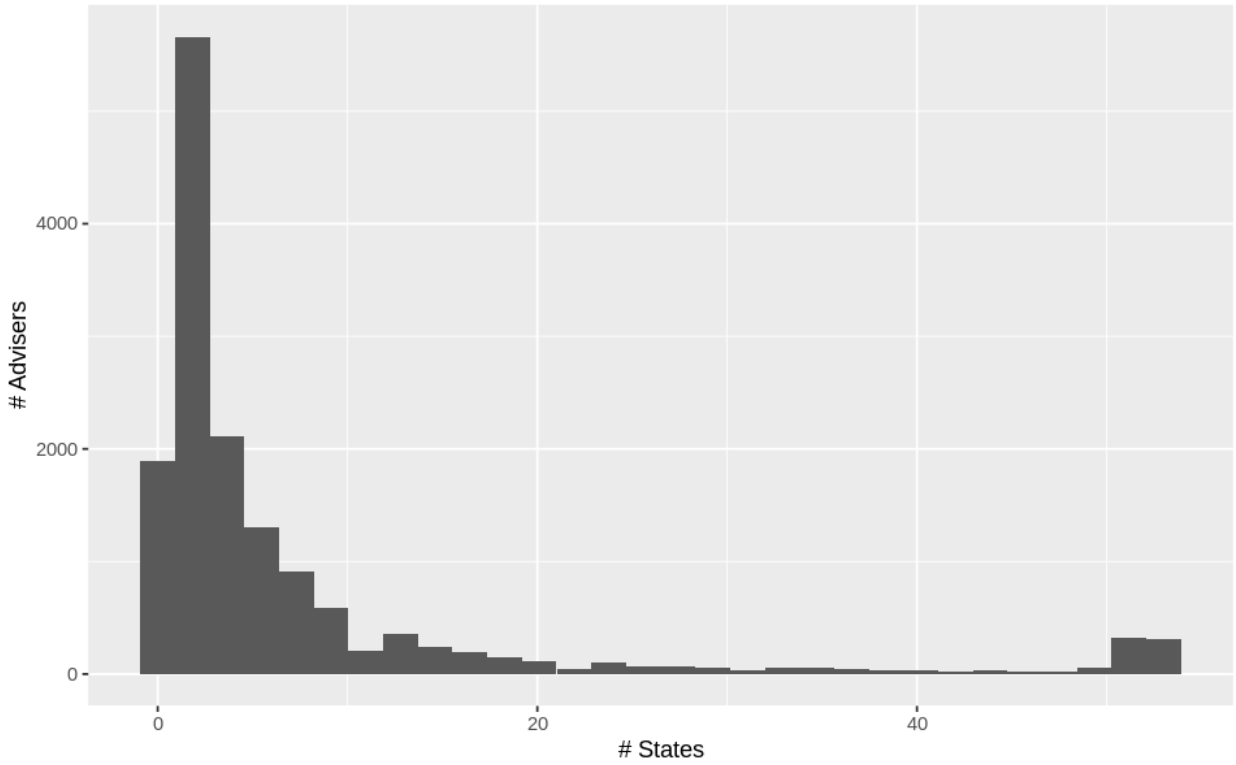

Figure 4: Number of state notice filings by SEC-registered investment advisers. Data source: Form ADV, Item 2.C (as of June 1, 2022).

c. Investment Companies

Investment companies are companies that issue securities and are primarily engaged in the business of investing in securities. Investment companies invest money they receive from investors on a collective basis, and each investor shares in the profits and losses in proportion to that investor's interest in the investment company. Investment companies that would be subject to the proposed rules include registered open-end and closed-end funds, business development companies ("BDCs"), Unit Investment Trusts ("UITs"), and employee securities' companies. Because they are not operating companies, investment companies do not have "customers" as such, and thus are unlikely to possess significant amounts of nonpublic "customer" information in the conventional sense. They may, however, have access to nonpublic information about their investors.

Table 1 summarizes the investment company universe that would be subject to the proposed rules. In total, as of the end of 2021, there were 13,965 investment companies,

including 12,420 open-end management investment companies, 681 closed-end managed investment companies, 662 UITs, 103 BDCs, and 43 employees' securities companies. Many of the investment companies that would be subject to the proposed rules are part of a "family" of investment companies.[401] Such families often share infrastructure for operations (*e.g.*, accounting, auditing, custody, legal) and potentially marketing and distribution. We believe that many of the compliance costs and other economic costs discussed in the following sections would likely be borne at the family level.[402] We estimate that there were up to 1,144 distinct operational entities (families and unaffiliated investment companies) in the investment company universe.

---

401 As used here, "family" refers to a set of funds reporting the same family investment company name (Form N-CEN Item B.5), or filing under the same registrant name (Form N-CEN Item B.1.A).

402 For example, each investment company in a family is likely to share common policies and procedures.

Table 1: Investment companies subject to proposed rule amendments, summary statistics. For each type of investment company, this table presents estimates of the number of investment companies and investment company families. Data sources: 2021 N-CEN filings,[a] Division of Investment Management Business Development Company Report (2022).[b]

Inv. Co. Type	# Inv. Co.	# Families[c]	# Unaffiliated[d]	# Entities[e]
Open-End[f]	12,420	426	106	532
Closed-End[g]	681	89	142	231
UIT[h]	662	51	216	267
BDC[i]	103	-	-	103
ESC[j]	43	-	-	43
Other[k]	56	12	12	24
Total[l]	13,965	578	476	1,144

[a] Year 2021 Form N-CEN filings (as of Nov 8, 2022).
[b] SEC, Business Development Company Report (updated June 2022), available at https://www.sec.gov/open/datasets-bdc.html.
[c] Number of families calculated from affiliation reported by registrants on Item B.5 of Form N-CEN.
[d] Number of registrants reporting no family affiliation.
[e] Number of distinct entities, *i.e.*, the sum of distinct families (# Families) and unaffiliated registrants (# Unaffiliated).
[f] Form N-1A filers; includes all open-end funds, including ETFs registered on Form N-1A.
[g] Form N-2 filers not classified as BDCs.
[h] Form N-3, N-4, N-6, N-8B-2, and S-6 filers.
[i] BDCs listed in the Business Development Company Report (note b) which have made a filing in 2022 (as of Aug. 9 2022)
[j] Form 40-APP filers [not classified as BDCs].
[k] Includes N-3 and S-6 filers.
[l] Cells do not sum to totals as investment company families may span multiple investment company types.

d. Transfer Agents

Transfer agents maintain records of security ownership and are responsible for processing changes of ownership ("transfers"), communicating information from the firm to its security-holders (*e.g.*, sending annual reports), replacing lost stock certificates, etc. However, in practice most U.S.-registered securities are held in "street name," where the ultimate ownership information is not maintained by the transfer agent, but rather in a hierarchal ledger. In this structure, securities owned by individuals are not registered in the name of the individual with the transfer agent. Rather the individual's broker maintains the records of the individual's ownership claim on securities. Brokers, in turn, have claims on securities held by a single nominee owner[403] who maintains records of the claims of the various brokers. This arrangement

[403] In the U.S., this is generally Cede & Co, a partnership organized by the Depository Trust & Clearing Corporation.

makes securities lending feasible and facilitates rapid transfers. In such cases, the transfer agent is not aware of the ultimate owner of the securities and therefore does not hold sensitive information belonging to those owners.

Despite the prevalence of securities held in street name, a large number of individuals nonetheless hold securities directly through the transfer agent. Securities held directly may be held either in the form of a physical stock certificate or in book-entry form through the Direct Registration System ("DRS"). In either case, the transfer agent would need to maintain sensitive information about the individuals who own the securities. For example, to handle a request for replacement certificate, the transfer agent would need to confirm the identity of the individual making such a request and to maintain a record of such confirmation. Similarly, to effect DRS transfers a transfer agent would need to provide a customer's identification information in the message to DRS.

In 2022, there were 335 transfer agents registered with the Commission, with an additional 67 registered with the Banking Agencies.[404] On average, each transfer agent reported 1.2 million individual accounts, with the largest reporting 56 million.[405] Figure 5 plots the cumulative distribution of the number of individual accounts reported by transfer agents registered with the Commission. Approximately one third of SEC-registered transfer agents reported no individual accounts,[406] and half reported fewer than ten thousand individual

---

404 Form TA-1 (as of June 20, 2022).

405 Form TA-2 Items 5(a) (as of June 20, 2022).This analysis is limited to the 151 transfer agents that filed form TA-2.

406 Some registered transfer agents outsource many functions—including tracking the ownership of securities in individual accounts—to other transfer agents ("service companies"). *See* Form TA-1 Item 6 (as of June 20, 2022).

accounts.

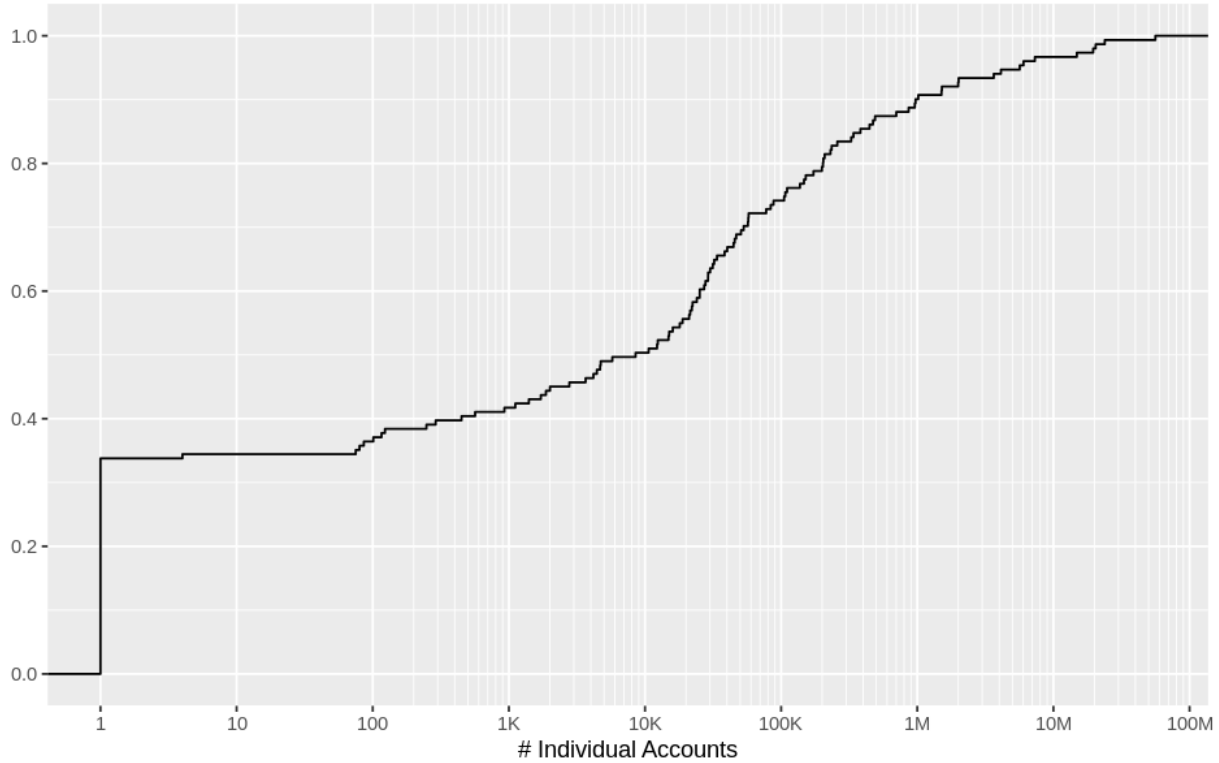

Figure 5: Cumulative distribution of the number of individual accounts (logarithmic scale) across SEC registered transfer agents. Data source: Form TA-2, Items 5(a) (as of June 20, 2022).

e. Service Providers

The proposed policies and procedures provisions would require covered institutions, pursuant to a written contract between the covered institution and its service providers, to require the service providers to take appropriate measures that are designed to protect against unauthorized access to or use of customer information.[407] These contracting requirements on a covered institution would affect a third party service provider that "receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to [the] covered institution."[408]

Covered institutions' relationships with a wide range of service providers would be affected. Specialized service providers with offerings geared toward outsourcing of covered

---

407 *See infra* section III.D.1.b.

408 Proposed rule 248.30(e)(10).

institutions' core functions would generally fall under the proposed contracting requirements. Those offering of customer relationship management, customer billing, portfolio management, customer portals (*e.g.,* customer trading platforms), customer acquisition, tax document preparation, proxy voting, and regulatory compliance (*e.g.,* AML/KYC) would likely fall under the proposed contracting requirements. In addition, various less-specialized service providers could potentially fall under these requirements. Service providers offering Software-as-a-Service (SaaS) solutions for email, file storage, and similar general-purpose services could potentially be in a position to receive, maintain, or processes customer information. Similarly, providers of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), as well as those offering more "traditional" consulting services (*e.g.,* IT contractors) would in many cases be "otherwise [] permitted access to customer information" and could fall under the contracting provisions.

Due to data limitations, we are unable to quantify or characterize in much detail the structure of these various service provider markets.[409] However, it has long been recognized that the financial services industry is increasingly relying on service providers through various forms of outsourcing[410].

D. Benefits and Costs of the Proposed Rule Amendments

The proposed amendments can be divided into four main components. First, they would create a requirement for covered institutions to adopt incident response programs, including notification to customers in the event sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. Second, they would broaden the scope of

---

[409] As noted above, potential service providers include a wide range of firms fulfilling a variety of functions. The internal organization of covered entities, including their reliance on service providers, is not generally publicly observable. Although certain regulatory filings shed a limited light on the use of third-party service providers (*e.g.*, transfer agents' reliance on third parties for certain functions), we are unaware of any data sources that provide detail on the reliance of covered institutions on third-party service providers.

[410] *See* Bank for International Settlements, *Outsourcing in Financial Services* (Feb. 15, 2005), *available at* https://www.bis.org/publ/joint12.htm.

information covered by the safeguards rule and the disposal rule[411] and extend the application of the safeguards rule to transfer agents. Third, they would require covered institutions to maintain and retain records related to the foregoing. Fourth, they would include in regulation an existing statutory exemption for annual privacy notices. We discuss costs and benefits of each provision in turn.

1. Response Program

The proposed amendments would require covered institutions to "develop, implement, and maintain written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information"[412] which must include a response program "designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures."[413] Under the proposal, covered institutions' response programs would be required to address incident assessment, containment, as well as customer notification.[414]

The question of how best to structure the response to a cyber-incident has received considerable attention from firms, IT consultancies, government agencies, standards bodies, and industry groups, resulting in numerous reports with recommendations and summaries of best practices.[415] While the emphasis of these reports varies, certain key components are common across many cybersecurity incident response programs. For example, NIST's Computer Security Incident Handling Guide identifies four main phases to cyber incident handling: (1) preparation; (2) detection and analysis; (3) containment, eradication, and recovery; and (4) post-incident activity.[416] The assessment, containment, and notification prongs of the proposed policies and

---

411 17 CFR 248.30(a) and 17 CFR 248.30(b), respectively.

412 Proposed rule 248.30(b)(1).

413 Proposed rule 248.30(b)(3).

414 Proposed rule 248.30(b)(3).

415 *See supra* section III.C.1.

416 *See* NIST Computer Security Incident Handling Guide, *supra* note 81.

procedures requirement correspond to the latter three phases of the NIST recommendations. Similar analogues are found in other reports, recommendations, and other regulators' guidelines.[417] Thus, the proposed procedures of the incident response program are substantially consistent with industry best practices and these other regulatory documents that seek to develop effective policies and procedures in this area.

In addition to helping ensure that customers are notified when their data is breached, the proposed requirements for policies and procedures to address assessment and containment of incidents are likely to have various other benefits. Having reasonably-designed strategies for incident assessment and containment ex ante could reduce the frequency and scale of breaches through more effective intervention and improved managerial awareness. Any such improvements to covered institutions' processes would benefit their customers (*i.e.* by reducing harms to customers resulting from data breaches), as well as the covered institutions themselves (*i.e.* by reducing the expected costs of handling data breaches).

In the remainder of this section, we first consider the benefits and costs associated with requiring covered institutions to develop, implement, and maintain written policies and procedures for a response program generally. We then consider costs and benefits of the proposed service provider provisions. We conclude this section with an analysis of the proposed notification requirements vis-à-vis the notification requirements already in force under the various existing state laws.

a. Written Policies and Procedures

Written policies and procedures are a practical prerequisite for organizations to implement standard operating procedures, which have long been recognized as necessary to improving outcomes in critical environments.[418] While we are not aware of any studies that

---

417 *See* text accompanying note 367.

418 Other Commission regulations, such as the Investment Company Act and Investment Advisers Act compliance rules, require policies and procedures. 17 CFR 270.38a-1(a)(1), 275.206(4)-7(a). The utility of written policies and procedures is recognized outside the financial sector as well;

assess the efficacy of written policies and procedures specifically in the context of financial regulation, we expect that requiring written policies and procedures for the proposed response program would improve its effectiveness in a number of ways. Although data breach incidents are increasingly common,[419] they are nonetheless a relatively rare event for any given covered institution. As the process for handling them is unlikely to be routine for a covered institution' staff, written policies and procedures can help ensure that the covered institution's personnel know what corrective actions to take and when. Moreover, written policies and procedures can help ensure that the incident is handled in an optimal manner. Finally, establishing incident response procedures ex ante can facilitate discussion among the covered institution's staff and expose flaws in the incident response procedures before they are used in a real response.

As noted in section III.C , all states and the District of Columbia generally require businesses to notify their customers when certain customer information is compromised, but they do not typically require the adoption of written policies and procedures for the handling of such incidents.[420] However, despite the lack of explicit statutory requirements, covered institutions—especially those with a national presence—may have developed and implemented written policies and procedures for a response program that incorporates various standard elements, including the ones being proposed here: assessment, containment, and notification.[421] Given the

---

for example, standardized written procedures have been increasingly embraced in the field of medicine. *See e.g.*, Robert L. Helmreich, *Error Management as Organizational Strategy*, *In Proceedings of the IATA Human Factors Seminar, Vol. 1*. Citeseer (1998); *see also* Alex, Joseph Chaparro Keebler, Elizabeth Lazzara & Anastasia Diamond, *Checklists: A Review of Their Origins, Benefits, and Current Uses as a Cognitive Aid in Medicine*, *Ergonomics in Design*: 2019 Q. HUM. FAC. APP. 27 (2019): 106480461881918.

419 *See* ITRC Data Breach Annual Report, *supra* note 349 (noting that in 2021, there were more data compromises reported in the United States than in any year since the first state data breach notice law became effective in 2003).

420 *See e.g.*, Cal. Civil Code sec. 1798.82 and N.Y. Gen. Bus. Law. sec. 899-AA.

421 Various industry guidebooks, frameworks, and government recommendations share many common elements, including the ones being proposed here. *See e.g.* NIST Computer Security Incident Handling Guide, *supra* note 81; *see also* CISA Incident Response Playbook, *supra* note 75.

numerous and distinct state data breach laws, it would be difficult for larger covered institutions operating in multiple states to comply effectively with existing state laws without having some written policies and procedures in place. As such covered institutions are generally larger, they are more likely to have compliance staff dedicated to designing and implementing regulatory policies and procedures, which could include policies and procedures regarding incident response. Moreover, to the extent covered institutions that have already developed written policies and procedures for incident response have based such policies and procedures on common cyber incident response frameworks (*e.g.*, NIST Computer Security Incident Handling Guide, CISA Cybersecurity Incident Response Playbook),[422] generally accepted industry best practices, or other applicable regulatory guidelines,[423] these large covered institutions' written policies and procedures are likely to include the proposed elements of assessment, containment, and notification, and to be substantially consistent with the proposed rule's requirements.

Thus, we do not anticipate that the proposed requirement for written policies and procedures would result in substantial new benefits from its application to large covered institutions, those with a national presence, or those already subject to comparable Federal regulations.[424] For the same reasons, it is unlikely to impose significant new costs for these institutions. Here, we expect the main cost associated with the proposed requirement to be the cost of reviewing existing policies and procedures to verify that they satisfy the new requirement. We further expect that these costs—although not significant—would ultimately be passed on to customers of these institutions.[425]

---

422 *See supra* notes 75 and 81.

423 For example, the Banking Agencies' Guidance states that covered institutions that are subsidiaries of U.S. bank holdings companies should develop response programs that include assessment, containment, and notification elements. *See supra* discussion of Banking Agencies' Incident Response Guidance in text accompanying note 367.

424 The nature of the transfer agent and registered investment company business largely precludes geographic catering and that these entities will all have a "national presence."

425 Costs incurred by larger covered institutions as a result of the proposed amendments will generally be passed on to their customers in the form of higher fees. However, smaller covered

We expect that the proposed written policies and procedures requirement would have more substantial benefits and costs for smaller covered institutions without a national presence, such as small registered investment advisers and broker-dealers who cater to a clientele based on geography, as compared to larger covered institutions. For smaller covered institutions the potential reputational cost of a cybersecurity breach is likely to be relatively small,[426] while the cost of developing and implementing written policies and procedures for a response program is proportionately large.[427] Moreover, these smaller covered institutions could potentially comply effectively with the relevant state data breach notification laws without adopting written policies and procedures to deal with customer notification: they may only need to consider—on an ad hoc basis—the notification requirements of the small number of states in which their customers reside.

Thus, we expect that for such covered institutions, the proposed amendments would likely impose additional compliance costs related to amending their existing written policies and procedures for safeguarding customer information.[428] While these smaller covered institutions could potentially pass some of these costs on to customers in the form of higher fees, their ability to do so may be limited due to the presence of larger competitors with more customers.[429] In addition, covered institutions that improve their customer notification procedures in response to the proposed amendments could suffer reputational costs resulting from the additional notifications.[430]

---

institutions—which are likely to face higher average costs—may not be able to do so. *See infra* section III.E.

426 Smaller firms generally have a lower franchise value (the present value of the future profits that a firm is expected to earn as a going concern) and lower brand equity (the value of potential customers' perceptions of the firm). Thus, the costs of potential reputational harm are typically lower than at larger firms.

427 *See supra* discussion in section III.A following note 317.

428 As required under existing Regulation S-P, 17 CFR 248.30.

429 *See supra* section III.C.3.

430 *See supra* section III.B; *see also infra* section III.D.1.c.

Although the relevant baseline for the analysis of this proposal incorporates only regulations currently in place, we note that several concurrent Commission proposals would impose broader policies and procedures requirements relating to cybersecurity and data protection on some covered institutions.[431] Insofar as these related proposals are adopted, the response program being proposed here would represent a refinement of elements addressing incident response and recovery found in the concurrent proposals.[432] Thus, we anticipate that costs of developing the response programs being proposed here could largely be subsumed in the costs of developing policies and procedures for these concurrent proposals (if adopted).

The benefits ensuing from smaller, more geographically limited covered institutions incorporating incident response programs to their written policies and procedures can be expected to arise from improved efficacy in notifying affected customers and—more generally—from improvements in the manner in which such incidents are handled with aforementioned attendant benefits to customers and to the covered institutions themselves.[433]

Lacking data on the improvements to efficacy — whether it be efficacy of customer notification, incident assessment, or incident containment — that would result from widespread adoption of written response programs, we cannot quantify the economic benefits of the proposed requirements. Similarly, quantifying the indirect economic costs such as reputational cost of any potential increased efficacy in customer notification is not feasible. However, as noted earlier, the effects of these requirements are likely to be small for covered institutions with a national presence who—we understand—are likely to already have such programs in place. For such institutions, we expect direct compliance costs to be largely limited to reviews of

---

431 *See* Investment Management Cybersecurity Proposal, *supra* note 55, Exchange Act Cybersecurity Proposal and Regulation SCI Proposal, *supra* note 57. *See also supra* section II.G.

432 For example, the response program proposed here provides further specificity to the "Cybersecurity Incident Response and Recovery" element of the policies and procedure required under the Investment Management Cybersecurity Proposal. *See* Investment Management Cybersecurity Proposal, *supra* note 55, at section II.A.1.e.

433 *See supra* text accompanying notes 415-418.

existing policies and procedures.[434] Smaller, more geographically limited covered institutions—which are less likely to have written policies and procedures to address incident response—we expect would be more likely to bear the full costs associated with adopting and implementing such procedures.[435]

The proposed requirements could potentially provide great benefit in a specific incident, for example in the case of a data breach at an institution that does not currently have written policies and procedures and was unprepared to promptly respond in keeping with law, and best practice. Such an institution would also bear the highest cost in complying with the proposal. In the aggregate, however, considering the proposed amendments in the context of the baseline, these benefits and costs are likely to be limited. As we have noted above, all states have previously enacted data breach notification laws with substantially similar aims and, therefore, we think it likely that many institutions have written policies and procedures to support compliance with these laws. In addition, we anticipate that larger covered institutions with a national presence—who account for the bulk of covered institutions' customers—have already developed written incident response programs consistent with the proposed requirements in most respects.[436] Thus, the benefits and costs of requiring written incident response programs would largely be limited to smaller covered institutions without a national presence—institutions whose policies affect relatively few customers.

b. Service Provider Provisions

The proposed amendments would require that a covered institution's incident response program include written policies and procedures that cover activity by service providers.[437] Specifically, these policies and procedures would require covered institutions, pursuant to a

---

434 We expect these reviews to be generally smaller than the costs of adopting and implementing said procedures as discussed in section IV.

435 Administrative costs associated with developing and implementing policies and procedures are estimated to be $11,375. *See infra* section IV.

436 *See supra* discussion in this section.

437 Proposed rule 248.30(b)(5)(i).

written contract between the covered institution and its service providers, to require the service providers to take appropriate measures that are designed to protect against unauthorized access to or use of customer information, including notification to the covered institution in the event of any breach in security resulting in unauthorized access to a customer information system maintained by the service provider to enable the covered institution to implement its response program. Under the proposed amendments, "service provider" is defined broadly, as "any person or entity that is a third party and receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution."[438] Thus, the proposed requirement could affect contracts with a broad range of entities, including potentially email providers, customer relationship management systems, cloud applications, and other technology vendors.

As modern business processes increasingly rely on third-party service providers, ensuring consistency in regulatory requirements increasingly requires consideration of the functions performed by service providers, and how these functions interact with the regulatory regime. Ignoring such aspects would create opportunities for regulatory arbitrage through outsourcing of functions to unregulated service providers. Thus, the proposed requirement would function to strengthen the benefits of the proposal by helping ensure that the proposed requirements have similar effects regardless of how a covered institution chooses to implement its business processes (*i.e.*, whether those processes are implemented in-house or outsourced).

For service providers that provide specialized services aimed at covered institutions, the proposed requirement would create additional market pressure to enhance service offerings so as to facilitate covered institutions' compliance with the proposed requirements.[439] These service providers would have increased market pressure to adapt their services to facilitate covered

---

438 Proposed rule 248.30(e)(10).

439 A service provider involved in any business-critical function likely "receives, maintains, processes, or otherwise is permitted access to customer information". *See* proposed rule 248.30(e)(10).

institutions' compliance with the proposed amendments. This would entail costs for the service providers, including the actual cost of adapting business processes to accommodate the requirements, as well as costs related to renegotiating service agreements with covered institutions to include the required contractual provisions. It is difficult for us to quantify these costs, as we have no data on the number of specialized service providers used by covered institutions and on the ease with which they could adapt business processes to satisfy the new contractual provisions. That said, we preliminarily believe that these costs are justified and would not represent an undue cost as both the specialized service providers and the covered institutions contracting with them are adapted to operating in a highly-regulated industry, and would be accustomed to adapting their business processes to meet regulatory requirements. We further expect that such costs would largely be passed on to covered institutions and ultimately their customers.[440]

With respect to more generic service providers (*e.g.*, email, customer-relationship management), the situation could be quite different. For these providers, covered institutions are likely to represent a small fraction of their customer base. These generic service providers may be unwilling to adapt their business processes to the regulatory requirements of a small subset of their customers. Under the proposed requirement, some covered institutions could find that some of their existing generic service providers would be unwilling to take the steps necessary to facilitate covered institutions' compliance with the proposed amendments. In such cases, the covered institutions would need to switch service providers and bear the associated switching costs, while the service providers would suffer loss of customers.[441] Although these costs would be offset by benefits arising from enhanced efficacy of the regulation,[442] they would be

---

440 *See supra* note 425.

441 These costs include the direct costs associated with reviewing and renegotiating existing agreements as well as indirect costs arising from service providers requiring additional compensation for providing the required contractual guarantees.

442 From the perspective of current or potential customers, the implications of customer information

particularly acute for smaller covered institutions which lack bargaining power with generic service providers and would in many cases be forced to switch providers.

Moreover, in some cases generic service providers may have the business processes in place to facilitate covered institutions' compliance, but may be unwilling to enter into suitable written contracts. This situation is likely to arise with large, best-of-breed generic service providers with large market share, and could lead to perverse outcomes where the aims of the proposed amendments are undermined.[443] For example, large, established server hosting providers could be particularly unwilling to make contractual accommodations.[444] At the same time, these hosting providers would have the greatest economic incentive—and means—to reduce generic vulnerabilities within their control.[445] Thus, if a covered institution is forced to switch away from a large, established hosting provider unwilling to amend its contractual terms, it is likely to end up relying on a smaller, less established hosting provider that—while more amenable to specific contractual language—may be less capable of addressing the generic vulnerabilities within its control.[446] Given the increasing reliance of firms on such generic service providers,[447] switching could generate substantial costs and bring with it reduced ability to protect customer information if such generic service providers are either unwilling to

---

safeguard failures are similar whether the failure occurs at a covered institution, or at one of its third-party service providers.

443 For example, it is unlikely that a small investment adviser would be able to effect any changes in its contracts with large providers of generic services.

444 For such service providers, the profits earned from covered institutions may not be sufficient to justify creating a separate contractual regime. Moreover, actually adapting business processes—processes that apply to many different types of customers—to satisfy the contractual terms applicable to only a small subset of customers is likely to be cost prohibitive and impracticable.

445 While a hosting provider can address "generic" vulnerabilities that apply to all customers (*e.g.,* vulnerabilities in the physical and virtual access controls to the servers), it may not be able to mitigate vulnerabilities "specific" to a given customer (*e.g.,* security flaws in applications deployed by customers).

446 Smaller, "upstart" service providers may be more willing to provide unrealistic contractual assurances as the risk to their (more limited) reputations is lower.

447 *See supra* section III.C.3.e.

contractually agree to certain provisions or unable to address the vulnerabilities within their control.

Finally, even in cases where service providers are willing to adapt processes and contractual terms to meet covered institutions requirements, the task of renegotiating service agreements could—in itself—impose substantial contracting costs on the parties. Contracting costs are likely to be most acute for larger covered institutions, which may have hundreds of contracts that would require renegotiation. These additional costs would likely be passed on to customers in the form of higher fees.

c. Notification Requirements

The proposed requirements would provide for a strong minimum standard for data breach notification, applicable to the sensitive customer information of all customers of covered institutions (including customers of other financial institutions whose information has been provided to a covered institution)[448] regardless of their state of residence. The "strength" of a data breach notification standard is a function of its various provisions and how these provisions interact to provide customers with thorough, timely, and accurate information about when their information has been compromised. Customers receiving notices that are more thorough, timely, and accurate have a better chance of taking effective remedial actions, such as placing holds on credit reports, changing passwords, and monitoring account activity. These customers would also be better able to abandon institutions that have allowed their information to be compromised. Similarly, non-customers who learn of a data breach, for example from individuals notified as a result of the minimum standard, could use this information to avoid covered institutions that allow compromises to occur.

As discussed in section III.C.2.a all 50 states and the District of Columbia already have data breach laws generally applicable to compromises of their residents' information. Thus, the

---

[448] *See* proposed rule 248.30(a); *see also infra* section III.D.1.c.i.

benefits of the proposed minimum standard for notification to customers (vis-à-vis the baseline) would vary depending on each customer's state of residence, with the greatest benefits accruing to customers that reside in states with "weaker" data breach laws.

Unfortunately, with the data available, it is not practicable to decompose the marginal contributions of the various state law provisions to the overall "strength" of state data breach laws. Consequently, it is not possible for us to quantify the benefits of the proposed minimum standard to customers residing in the various states. Thus, in considering the benefits of the proposed notification requirement, we limit consideration to the "strength" of individual provisions of the proposal vis-à-vis the corresponding provisions under state laws, and consider the number of customers that could potentially benefit from each.

Similarly—albeit to a somewhat lesser extent—the costs to covered institutions will also vary depending on the geographical distribution of each covered institution's customers. Generally, the costs associated with this proposal will be greater for covered institutions whose customers reside in states with weaker data breach laws than for those whose customers reside in states with stronger data breach laws. In particular, smaller covered institutions whose customers are concentrated in states with weak state data breach laws are likely to face proportionately higher costs.

In the rest of this section, we consider key provisions of the proposed notification requirements, their potential benefits to customers (vis-à-vis existing state notification laws), and their costs.

i. Effect with Respect to Customers of Other Financial Institutions

The scope of customer information subject to protection under the proposed amendments extends to "all customer information in the possession of a covered institutions, and all consumer information that a covered institution maintains or otherwise possesses for a business purpose, as applicable, regardless of whether such information pertains to individuals with whom the

covered institution has a customer relationship, or pertains to the customers of other financial institutions and has been provided to the covered institution."[449]

This aspect of the proposal would generally extend the benefits of the proposed amendments, and in particular of the proposed notification requirements,[450] to a wide range of individuals such as prospective customers, account beneficiaries, recipients of wire transfers, or any other individual whose customer information a covered institution comes to possess, so long as the individuals are customers of a financial institution.

We do not anticipate that extending the scope of information covered by the proposed amendments to include these additional individuals would have a significant effect on costs faced by covered institutions resulting from a data breach.[451] We further anticipate that costs of preventative measures taken by covered institutions to protect customers in response to the proposed amendments would generally be effective at protecting these additional individuals.[452] However, we acknowledge that in certain instances, this may not be the case. For example, information about prospective customers used for sales or marketing purposes may be housed in separate systems from the covered institution's "core" customer account management systems and require additional efforts to secure. That said, given that the distinction between customers and other individuals is generally not relevant under existing state notification laws—which apply to information pertaining to residents of a given state—we expect that most covered institutions will have already undertaken to protect and provide notifications of data breaches to these additional individuals.

ii. Effect with Respect to GLBA Safe Harbors

---

449 Proposed rule 248.30(a).

450 As described in more detail in the following subsections.

451 These costs would include additional reputational harm and litigation as well as increased notice delivery costs.

452 For example, measures aimed at strengthening information safeguards such as improved user access control.

A number of state data breach laws provide exceptions to notification for entities subject to and in compliance with the GLBA. These "GLBA Safe Harbors" may result in customers not receiving any data breach notification from registered investment advisers, broker dealers, investment companies, or transfer agents. The proposal would help ensure customers receive notice of breach in cases where they may not currently because notice is not required under state law.

Based on an analysis of state laws, we found that 11 states provide a GLBA Safe Harbor.[453] Together, these states account for 15% of the U.S. population, or approximately 8 million customers who may potentially benefit from this provision.[454] While we do not have data on the exact geographical distribution of customers across all covered institutions, we are able to identify registered investment advisers whose customers reside exclusively in GLBA Safe Harbor states.[455] We estimate that there are 215 such advisers, representing 1.4% of the adviser population.[456] These advisers represent up to 11,000 clients, and tend to be small, with a median regulatory assets under management of $223 million. We expect that a similar percentage of broker-dealers would be found to be operating exclusively in GLBA Safe Harbor states.

Changing the effect of the GLBA Safe Harbors is not likely to impose significant direct compliance costs on most covered institutions. For the reasons outlined above, most covered institutions have customers from states without a GLBA Safe Harbor and we therefore expect they have existing procedures for notifying customers under state law. However, covered institutions whose customer base is limited to these GLBA Safe Harbor states may not have

---

453 States with GLBA Safe Harbors include Arizona, Iowa, Kentucky, Minnesota, Missouri, Nevada, New Mexico, Oregon, South Carolina, Tennessee, and Utah.

454 Estimates of the numbers of potential customers based on state population adjusted by the percentage of households reporting direct stock ownership (15.2%). *See* U.S. Census Bureau, *Apportionment Report* (2020)*, available at* https://www2.census.gov/programs-surveys/decennial/2020/data/apportionment/apportionment-2020-table01.xlsx; *see also* Federal Reserve Board*, Survey of Consumer Finances* (2019), *available at* https://www.federalreserve.gov/econres/scfindex.htm.

455 Based on Form ADV, Item 2.C*; see also supra* note 399.

456 *See id*.

implemented any procedures to notify customers in the event of a data breach. These covered institutions would face proportionately higher costs than entities with some notification procedures already in place.

iii. Accelerating Timing of Customer Notification

Under the proposed amendments, a covered institution would be required to provide notice to customers in the event of a data breach as soon as practicable, but not later than 30 days after becoming aware that a data breach has occurred. As discussed in section III.C.2.a, existing state laws vary in terms of notification timing. Most states (32) do not include a specific deadline, but rather require that the notice be given in an expedient manner and/or that it be provided without unreasonable delay; these states account for 61% of the U.S. population with approximately 31 million potential customers residing in these states.[457] Four states have a 30-day deadline; we estimate that 5 million customers reside in these states. The remaining 15 states provide for longer notification deadlines; we estimate that 14 million customers reside in these states. For the 14 million customers residing in these 15 states, the proposed 30-day deadline would tighten the notification timeframes by between 15 to 60 days.[458] In addition, the 30-day deadline we are proposing is likely to tighten notification timeframes for approximately 31 million customers residing in states with no specific deadline; however, the aggregate effects on these 31 million customers may be limited insofar as the relevant state laws are not generally interpreted as allowing delays in notification greater than 30 days.[459] Finally, because the proposal would not provide for broad exceptions to the 30-day notification requirement,[460] in

---

457 *See supra* Figure 2.

458 State deadlines are either 30, 45, 60, or 90 days.

459 The timing language in state laws without specific language varies, but generally suggests that notices must be prompt. For example, California requires that such notice be given "in the most expedient time possible and without unreasonable delay;" *see* Cal. Civil Code sec. 1798.82.

460 *See supra* note 359.

many cases it would tighten notification timeframes even for the 5 million customers residing in states with a 30-day deadline.[461]

Tighter notification deadlines should increase customers' ability to take effective measures to counter threats resulting from their sensitive information being compromised. Such measures may include placing holds on credit reports or engaging in more active monitoring of account and credit report activity. In practice, however, when it takes a long time to discover a data breach, a relatively short delay between discovery and customer notification may have little impact on customers' ability to take effective countermeasures.[462]

Based on data from the Washington Attorney General's Office,[463] in 2021 it took an average of 170 days (standard deviation: 209 days) from the time a breach occurred to its discovery. This suggests that time to discovery is likely to prevent issuance of timely customer notices in most cases.[464] However, as plotted in Figure 6, while some firms take many months—

---

461 For example, in Washington the median notification delay in 2021 was 37 days, even though the state statute requires notice be given "without unreasonable delay, and no more than thirty calendar days after the breach was discovered, unless the delay is at the request of law enforcement as provided in subsection (3) of this section, or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system" RCW 19.255.010(8).

462 In other words, the utility of a notice is likely to exhibit decay. For example, if a breach is discovered immediately, the utility of receiving a notification within 1 day is considerably greater than the utility of receiving a notification in 30 days. However, if a breach is discovered only after 200 days, the difference in expected utility from receiving a notification on day 201 vs day 231 is smaller: with each passing day some opportunities to prevent the compromised information from being exploited are lost (e.g., unauthorized wire transfer), with each passing day opportunities to discover the compromise grow (e.g., noticing an unauthorized transaction), and with each passing day the compromised information becomes less valuable (e.g., passwords, account numbers, addresses, etc., change over time).

463 Washington State Office of the Attorney General, *Data Breach Notifications*, *available at* https://data.wa.gov/Consumer-Protection/Data-Breach-Notifications-Affecting-Washington-Res/sb4j-ca4h (last visited Mar. 7, 2023). We rely on data from Washington State as it provides the most detail on the life cycle of incidents.

464 With respect to the time to discovery of a data breach, we believe that data from Washington State is fairly representative of the broader U.S. population. Similarly, data from California regarding breach notices sent to more than 500 California residents indicates that the average time from discovery to notification in 2021 was 197 days. State of California Department of Justice, Office of the Attorney General, *Search Data Security Breaches* (2023), *available at* https://oag.ca.gov/privacy/databreach/list (last visited Feb. 22, 2023). According to IBM, in 2021 it took an average of 212 days to identify a data breach. *See* IBM Cost of Data Breach Report, *supra* note 350.

even years—to discover a data breach, others do so in a matter of days: 15% of firms were able to detect a breach within 2 weeks, and 20% were able to do so within 30 days. Thus, while the proposed 30-day notification deadline may not substantially improve the timeliness of customer notices in many cases, in some cases it could.

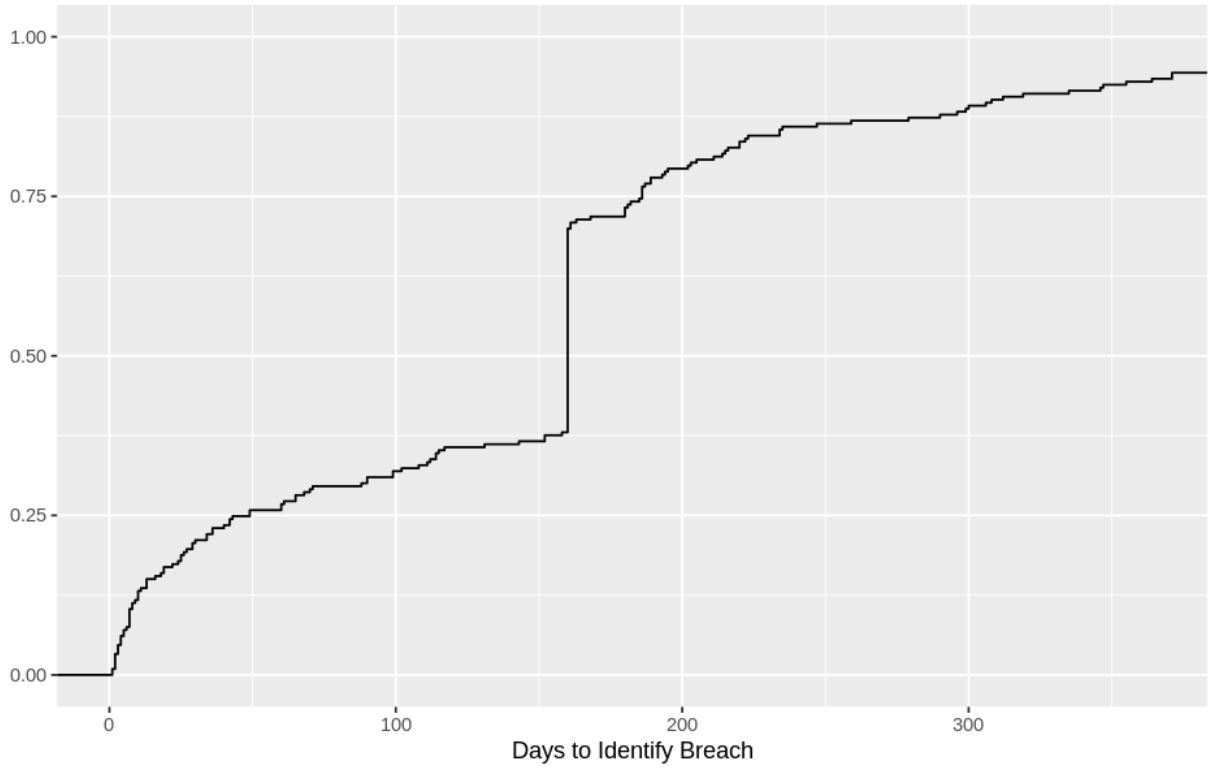

Figure 6: Cumulative distribution of the number of days between a breach and its discovery based on breaches in 2021 affecting residents of Washington State. For clarity, the plot is truncated at 500 days. The maximum number of days to discovery is 2,039 days. The discontinuity at 160 days is due to a ransomware attack that affected 68 entities. Data Source: Washington State Office of the Attorney General, *supra* note 463.

While we do not preliminarily believe that the proposed 30-day deadline to customer notifications would impose significant direct costs relative to a longer deadline (or relative to having no fixed deadline), the shorter deadline could potentially lead to indirect costs arising from the reporting deadline potentially interfering with incident containment efforts. Based on data from the Washington Attorney General's Office for 2021, "containment" of data breaches generally occurs quickly—4.4 days on average.[465] However, according to IBM's study for 2021,

[465] In the data provided by the Washington Attorney General, "containment" (data field *DaysToContainBreach*) is defined as "the total number of days it takes a notifying entity to end

it takes an average of 75 days to "contain" a data breach.[466] The discrepancy suggests that there exists some ambiguity in the interpretation of "containment," raising the possibility that the 30-day notification deadline could require customer notification to occur before some aspects of incident containment have been completed and potentially interfering with efforts to do so.[467]

In some circumstances, requiring customers to be notified within 30 days may hinder law enforcement investigation of an incident by potentially making an attacker aware of the attack's detection. While the proposal would allow the covered institution to delay notification in specific circumstances related to national security, most law enforcement investigations would not rise to this level.[468] Thus, the proposed 30-day customer notification requirement could impose costs on the public insofar as it interferes with law enforcement investigations that do not raise national security concerns and, thus, decreases recoveries or impedes deterrence.

iv. Broader Scope of Information Triggering Notification

In the proposal, "sensitive customer information" is defined more broadly than in most state statutes,[469] yielding a customer notification trigger that is broader in scope than the various state law notification triggers included under the baseline.[470] The broader scope of information triggering the notice requirements would cover more data breaches impacting customers than the notice requirements under the baseline. This increased sensitivity could benefit customers who would be made aware of more cases where their information has been compromised. At the same time, the increased sensitivity could lead to false alarms—cases where the "sensitive

---

the exposure of consumer data, after discovering the breach." *See supra* note 463.

466 In the IBM study, "containment" refers to "the time it takes for an organization to resolve a situation once it has been detected and ultimately restore service." *See* IBM Cost of Data Breach Report, *supra* note 350.

467 For example, the notice may prompt additional attacks aimed at taking advantage of vulnerabilities that cannot be adequately addressed in a 30 day timeframe.

468 *See* proposed rule 248.30(b)(4)(iii).

469 *See* proposed rule 248.30(e)(9).

470 *See supra* section III.C.2.a.

customer information" divulged does not ultimately harm the customer. Such false alarms could be problematic if they reduce customers' sensitivity to data breach notices. In addition, the proposed scope will also likely imply additional costs for covered institutions, which may need to adapt their processes for safeguarding information to encompass a broader set of customer information, and may need to issue additional notices.[471]

In the proposal, "sensitive customer information" is defined as "any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information."[472] The proposed definition's basis in "any component of customer information" creates a broader scope than under state notification laws. In addition to identification numbers, PINs, and passwords, many other pieces of nonpublic information have the potential to satisfy this standard. For example, many financial institutions have processes for establishing identity that require the user to provide a number of pieces of information that—on their own—are not especially sensitive (*e.g.*, mother's maiden name, name of a first pet, make and model of first car), but which—together—could allow access to a customer's account. The compromise of some subset of such information would thus potentially require a covered institution to notify customers under the proposed amendments.

The definitions of information triggering notice requirements under state laws are generally much more circumscribed, and can be said to fall into one of two types: basic and enhanced.[473] Basic definitions are used by 12 states, which account for 20% of the U.S. population. In these states, only the compromise of a customer's name together with one or more enumerated pieces of information triggers the notice requirement. Typically, the enumerated information is limited to Social Security number, a driver's license number, or a

---

471 Estimates of administrative costs related to notice issuance are discussed in section IV.

472 *See* proposed rule 248.30(e)(9).

473 *See supra* section III.C.2.a.

financial account number combined with an access code. For the estimated 10 million customers residing in these states, a covered institution's compromise of the customer's account login and password would not necessarily result in a notice, nor would a compromise of his credit card number and PIN.[474] Such compromises could nonetheless lead to substantial harm and inconvenience.

Thus, the proposed amendments would significantly enhance the notification requirements applicable to these customers.

States adopting enhanced definitions for information triggering notice requirements extend the basic definition to include username/password and username/security question combinations. They may also include additional enumerated items whose compromise (when linked with the customer's name) can trigger the notice requirement (*e.g.*, biometric data, tax identification number, and passport number). For the estimated 40 million customers residing in the states with enhanced definitions, the benefits from the proposed amendment will be somewhat more limited. However, even for these customers, the proposal would tighten the effective notification requirement. There are many pieces of information not covered by the enhanced definitions the compromise of which could potentially lead to substantial harm or inconvenience. For example, under California law, the compromise of information such as a customer's email address in combination with a security question and answer would only trigger the notice requirement if that information would—in itself—permit access to an online account; moreover, the compromise of information such as a customer's name, combined with her transaction history, account balance, or other information not specifically enumerated would not trigger the notice requirement under California law.[475]

The broader scope of information triggering a notice requirement under the proposed amendments would benefit customers. As noted earlier, many pieces of information not covered

---

474 *See supra* text accompanying note 354.

475 Cal. Civ. Code sec. 1798.82.

under state data breach laws could, when compromised, cause substantial harm or inconvenience. Under the proposed amendments, data breaches involving such information could require customer notification in cases where state law does not, and thus potentially increase customers' ability to take actions to mitigate the effects of such breaches. At the same time, there is some risk that the broader minimum standard will lead to notifications resulting from data compromises that—while troubling—are ultimately less likely to cause substantial harm or inconvenience.[476] A large number of such notices could undermine the effectiveness of the notice regime.

The broader minimum standard for notification is likely to result in higher compliance costs for covered institutions. In particular, it is possible the covered institutions have developed processes and systems designed to provide enhanced information safeguards for the specific types of information enumerated in the various state laws. For example, it is likely that IT systems deployed by financial institutions only retain information such as passwords or answers to security questions in hashed form, reducing the potential for such information to be compromised. Similarly, it is likely that such systems limit access to information such as Social Security numbers to a limited set of employees.

It may be costly for covered institutions to upgrade these systems to expand the scope of enhanced information safeguards. In some cases, it may be impractical to expand the scope of such systems. For example, while it may be feasible for covered institutions to strictly limit access to Social Security numbers, passwords, or answers to secret questions, it may not be feasible to apply such limits to account numbers, transaction histories, account balances, related accounts, or other potentially sensitive customer information. In these cases, the proposed

---

[476] This may be the case even though the proposal includes an exception from notification when the covered institution determines, after investigation, 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. For example, the covered institution could decide to forgo investigations and always report, or could investigate but not reach a conclusion that satisfied the terms of the exception.

minimum standard may not have a significant prophylactic effect, and may lead to an increase in reputation and litigation costs for covered institutions resulting from more frequent breach notifications as well as increased administrative costs related to sending out additional notice.[477] In addition, because the proposed notice trigger is based on a determination that there is a reasonably likely risk of substantial harm or inconvenience, it could increase costs related to incident evaluation, legal consultation, and litigation risk. This subjectivity could reduce consistency in the propensity of covered institutions to provide notice to customers, reducing the utility of such notices in customer's inferences about covered institutions' safeguarding efforts.

v. Notification Trigger

Under the proposal, the access or use without authorization of an individual's sensitive customer information (or the reasonable likelihood thereof) triggers the customer notice requirement unless the covered institution is able to determine 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.[478] Moreover, if the covered institution is unable to determine which customers are affected by a data breach, a notice to all potentially affected customers would be required.[479] The resulting presumptions for notification are important because although it is usually possible to determine what information could have been compromised in a data breach, it is often not possible to determine what information was compromised[480] or to estimate the potential for such information to be used in a way that is likely to cause harm. Because of this, it may not be feasible to establish the likelihood of sensitive customer information being accessed or used in a way that creates a risk of substantial harm or inconvenience.

---

477 *See supra* note 471.

478 Proposed rule 248.30(b)(4)(i).

479 Proposed rule 248.30(b)(4)(ii).

480 Many covered institutions, especially smaller investment advisers and broker-dealers, are unlikely to have elaborate software for logging and auditing data access. For such entities, it may be impossible to determine what specific information was exfiltrated during a data breach.

Consequently, in the absence of the presumption for notification, it may be possible for covered institutions to avoid notifying customers in cases where it is unclear whether customer information was accessed or used in this way. Currently, 21 states' notification laws do not include a presumption for notification.

We do not have data with which to estimate reliably the effect of this presumption on the propensity of covered institutions to issue customer notifications. However, we expect that for the estimated 15 million customers residing in states without the presumption of notification, some notifications that would be required under the proposed amendments are not currently occurring. Thus, we anticipate that the proposed amendments will improve these customers ability to take actions to mitigate the effects of data breaches.

The increased sensitivity of the notification trigger resulting from the presumption for notification would result in additional costs for covered institutions, who would bear higher reputational costs as well as some additional direct compliance costs (*e.g.*, mailing notices, responding to customer questions, etc.) due to more breaches requiring customer notification. We are unable to quantify these additional costs.

2. Extend Scope of Customer Safeguards to Transfer Agents

The proposed amendments would bring transfer agents within the scope of the safeguards rule.[481] In addition to the costs and benefits arising from the proposed response program discussed separately in section III.D.1 this would create an additional obligation on transfer agents to develop, implement, and maintain written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information more generally.[482]

---

481 *See infra* note 173 and accompanying text.

482 Proposed rule 248.30(b).

As discussed in sections II.C.3 and III.C.3.d, in the U.S., transfer agents provide the infrastructure for tracking ownership of securities. Maintaining such ownership records necessarily entails holding or accessing non-public information about a large swath of the U.S. investing public. Given the highly-concentrated nature of the transfer agent market,[483] a general failure of customer information safeguards at a transfer agent could negatively impact large numbers of customers.[484] In general, transfer agents with written policies and procedures to safeguard this information would be at reduced risk of experiencing such safeguard failures.[485] Further, , because the core of the transfer agent business is maintaining customer records, and transfer agents are likely to handle large numbers of customers, transfer agents are likely to have written policies and procedures in place to address safeguarding of customer information.[486] In addition, transfer agents are currently subject to the notification requirements in state law, which would require customer notification in many of the same cases as under the proposed amendments.[487] Thus, we do not expect substantial costs or benefits to arise from extending the scope of the safeguards rule to transfer agents in the aggregate. We anticipate that most transfer agents have policies and procedures in place already, and that the compliance costs of the proposal would thus be limited to the review of those existing policies and procedures for consistency with the safeguards rule. We discuss these costs in section IV.[488]

3. Recordkeeping

Under the new recordkeeping requirements, covered institutions would be required to make and maintain written records documenting compliance with the requirements of the

---

483 *See supra* section III.C.3.

484 Half of the registered transfer agents maintain records for more than 10,000 individual accounts. *See supra* Figure 5.

485 *See supra* section III.D.1.a for a discussion of the benefits of written policies and procedures generally.

486 *See supra* text accompanying notes 420-424.

487 *See supra* section III.D.1.c.

488 *See supra* note 435.

safeguards rule and of the disposal rule.[489] A covered institution would be required to make and maintain written records documenting its compliance with, among other things: its written policies and procedures required under the proposed rules, including those relating to its service providers and its consumer information and customer information disposal practices; its assessments of the nature and scope of any incidents involving unauthorized access to or use of customer information; any notifications of such incidents received from service providers; steps taken to contain and control such incidents; and, where applicable, any investigations into the facts and circumstances of an incident involving sensitive customer information, and the basis for determining 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.[490]

These proposed recordkeeping requirements would help facilitate the Commission's inspection and enforcement capabilities. As a result, the Commission would be better able to detect deficiencies in a covered institution's response program so that such deficiencies could be remedied. Insofar as correcting deficiencies results in material improvement in the response capabilities of covered institutions and mitigates potential harm resulting from the lack of an adequate response program, the proposed amendments would benefit customers through channels described in section III.D.1.

We do not expect the proposed recordkeeping requirements to impose substantial compliance costs. As covered institutions are currently subject to similar recordkeeping requirements applicable to other required policies and procedures, we do not anticipate covered institutions will need to invest in new recordkeeping staff, systems, or procedures to satisfy the new recordkeeping requirements.[491] The incremental administrative costs arising from

---

489 *See* proposed rule 248.30(d).

490 *See* the various provisions of proposed rule 248.30(b) and 248.30(c)(2).

491 *See, e.g.,* 17 CFR 240.17a-3; 17 CFR 275.204-2; 17 CFR 270.31a-1; and 17 CFR 240.17Ad-7. Where permitted, entities may choose to use third-party providers in meeting their recordkeeping obligations under the proposed rule, *see supra* note 217.

maintaining additional records related to these provisions using existing systems are covered in the Paperwork Reduction Act analysis in section IV and estimated to be $381/year.

4. Exception from Annual Notice Delivery Requirement

The proposed amendments would incorporate into the regulation an existing statutory exception to the requirement that a broker-dealer, investment company, or registered investment adviser deliver an annual privacy notice to its customers.[492] An institution may only rely on the exception if it has not changed its policies and practices with regard to disclosing nonpublic personal information from those it most recently provided to the customer via privacy notice.[493] Reliance on the exception is further limited to cases where the institution provides information to a third party to perform services for, or functions on behalf of, the institution[494] in accordance with one of a number of existing exemptions that contain notice provisions.[495]

The effect of the exception would be to eliminate the requirement to send the same privacy policy notice to customers on multiple occasions. As such notices would provide no new information, we do not believe that receiving multiple copies of such notices provides any significant benefit to customers. Moreover, we expect that widespread reliance on the proposed exception is more likely to benefit customers, by providing clearer signals of when privacy policies have changed.[496] At the same time, reliance on the exception would reduce costs for covered entities. However, we expect these cost savings to be limited to the administrative burdens discussed in section IV.

---

492 *See supra* note 220.

493 *See* proposed rule 248.5(e)(1)(ii).

494 *See id; see also* 15 U.S.C. 6802(b)(2) (providing the statutory basis to this exception).

495 *See* proposed rule 248.5(e)(1)(i). These existing exemptions address a number of cases, such as information sharing necessary to perform transactions on behalf of the customer, information sharing directed by the customer, reporting to credit reporting agencies, information sharing resulting from business combination transactions (mergers, sales, etc.). *See* 15 U.S.C. 6802(e) (providing the statutory basis to these additional criteria).

496 In other words, reducing the number of privacy notices with no new content allows customers to devote more attention to parsing notices that do contain new content.

Because the exception became effective when the statute was enacted, we believe that the aforementioned benefits have already been realized. Consequently, we do not believe that its inclusion would have any economic effects relative to the current status quo.[497]

E. Effects on Efficiency, Competition, and Capital Formation

As discussed in the foregoing sections, market imperfections could lead to underinvestment in customer information safeguards, and to information asymmetry about cybersecurity incidents.[498] Various elements of the proposed amendments aim to mitigate the inefficiency resulting from these imperfections by imposing mandates for policies and procedures. Specifically, the proposal would require covered entities to include a response program for incidents involving unauthorized access to or use of customer information, which would address assessment and containment of such incidents, and could thereby reduce potential underinvestment in these areas, and thereby improve customer information safeguards.[499] In addition, by requiring notification to customers about certain safeguard failures, the proposal could reduce the aforementioned information asymmetry.

While the proposed amendments have the potential to mitigate these inefficiencies, the scale of the overall effect is likely to be limited due to the presence of state notification laws, and existing security practices, as well as existing regulations.[500] Moreover, insofar as the proposed amendments alter covered institutions' practices, the improvement—in terms of the effectiveness of covered institutions' response to incidents, customers' ability to respond to breaches of their sensitive customer information, and in reduced information asymmetry about covered institutions' efforts to safeguard this information—is generally impracticable to quantify due to

---

497 We distinguish here between the theoretical "baseline" in which the self-effectuating provisions of the statute have not come into effect and the current "status quo" (in which they have). *See supra* note 221 and accompanying text.

498 *See supra* section III.B.

499 *See supra* section III.D (discussing benefits and costs of response program requirement).

500 *See supra* sections III.C.1 and III.C.2.

data limitations discussed previously.[501] The proposed provisions would not have first order effects on channels typically associated with capital formation (*e.g.*, taxation policy, financial innovation, capital controls, investor disclosure, market integrity, intellectual property, rule-of-law, and diversification). Thus, the proposed amendments are unlikely to lead to significant effects on capital formation.

Because the proposed amendments are likely to impose proportionately larger costs on smaller and more geographically-limited covered institutions, this may affect their competitiveness vis-à-vis their larger peers. Such covered institutions— which may be less likely to have written policies and procedures for incident response programs already in place— would face disproportionately higher costs resulting from the proposed amendments.[502] Thus, the proposed amendments could tilt the competitive playing field in favor of larger covered institutions. On the other hand, if clients and investors believe that the proposed amendments effectively induce the appropriate level of effort, smaller covered institutions would likely reap disproportionately large benefits from these improved perceptions.[503]

With respect to competition among covered institutions' service providers, the overall effect of the proposed amendments is similarly ambiguous. The standardized terms of service used by some service providers may already contain appropriate measures designed to protect against unauthorized access to or use of customer information. If they do not, however, it is likely that some service providers would decline to negotiate contractual terms with respect to customer information safeguards, effectively causing these service providers to cease offering

---

501 *See, e.g., supra* sections III.A., III.D.1.a. and III.D.1.c.

502 The development of policies and procedures entails a fixed cost component that imposes a proportionately larger burden on smaller firms. We expect smaller investment advisers and broker dealers would be most affected. *See supra* sections III.C.3.a and III.C.3.b.

503 Given the aforementioned disproportionately large costs faced by smaller institutions, it is reasonable for potential customers to suspect that smaller entities would be more inclined to avoid such costs than their larger peers; such suspicions would be mitigated by a regulatory requirement.

services to affected covered institutions.[504] This would reduce competition. On the other hand, service providers with fewer customer information safeguards (*i.e.,* those unwilling to provide said assurances) would be unable to undercut service providers with greater information safeguards. This would improve the competitive position of this latter group.

Finally, we anticipate that neither the proposed recordkeeping provisions,[505] nor the proposed exception from annual privacy notice delivery requirements[506] will have a notable impact on efficiency, competition, or capital formation due to their limited economic effects.[507] As discussed elsewhere in this proposal, we do not expect the proposed recordkeeping requirements to impose material compliance costs, and we expect the economic effects of the proposed exception to be limited.

F. Reasonable Alternatives Considered

In formulating our proposal, we have considered various reasonable alternatives. These alternatives are discussed below.

1. Reasonable Assurances from Service Providers

Rather than requiring policies and procedures that require covered institutions to enter into a written contract with each service provider requiring that it take appropriate measures designed to protect against unauthorized access to or use of customer information,[508] the Commission considered requiring covered institutions to obtain "reasonable assurances" from service providers instead. This would be a lower threshold than the proposed provision requiring a written contract, and as such would be less costly to reach but also less protective.

---

504 *See supra* section III.C.3.e.

505 Proposed rule 248.30(d).

506 Proposed rule 248.5.

507 *See supra* sections III.D.3 and III.D.4.

508 *See supra* section III.D.1.b.

Under this alternative we would use the proposal's definition of "service provider," which is "any person or entity that is a third party and receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution."[509] Thus, similar to the proposal, this alternative could affect a broad range of service providers including, potentially: email providers, customer relationship management systems, cloud applications, and other technology vendors. Depending on the states where they operate, these service providers may already be subject to state laws applicable to businesses that "maintain" computerized data containing private information.[510] Additionally, it is likely that any service provider that offers a service involving the maintenance of customer information to U.S. financial firms generally, or to any specific financial firm with a national presence, has processes in place to ensure compliance with these state laws; we request public comment on this assumption.

For service providers that provide specialized services aimed at covered institutions, this alternative would, like the proposal, create market pressure to enhance service offerings so as to provide the requisite assurances and facilitate covered institutions' compliance with the proposed requirements.[511] These service providers would have little choice other than to adapt their services to provide the required assurances, which would result in additional costs for the service providers related to adapting business processes to accommodate the requirements. In general, we expect these costs would be limited in scale in the same ways the costs of the proposal are limited in scale: specialized service providers are adapted to operating in a highly-regulated industry, and are likely to have policies and procedures in place to facilitate compliance with state data breach laws. And, as with the proposal, we generally anticipate that such costs would

---

509 Proposed rule 248.30(e)(10).

510 *See, e.g.,* Cal. Civil Code sec. 1798.82(b), N.Y. Gen. Bus. Law sec. 899-AA(3).

511 A service provider involved in any business-critical function likely "receives, maintains, processes, or otherwise is permitted access to customer information". *See* proposed rule 248.30(e)(10).

largely be passed on to covered institutions and ultimately their customers. As compared to the proposal's requirement for written contracts, we expect that "reasonable assurances" would require fewer changes to business processes and, accordingly, lower costs. Assuming the covered institution did not use written contracts to document the "reasonable assurances," however, this alternative would also be less protective than the proposed requirement for contractual language. As compared to "reasonable assurances," a written contract is clearer, more easily enforced as between the covered institution and the service provider, and more likely to ensure customer notification in the event of a data breach.

With respect to more generic service providers (*e.g.*, email, or customer-relationship management), the situation could be quite different. For these providers, covered institutions are likely to represent a small fraction of their customer base. As under the proposed service provider provisions, generic service providers may again be unwilling to adapt their business processes to the regulatory requirements of a small subset of their customers under this alternative.[512] Some generic service providers may be unwilling to make the assurances needed, although we anticipate that they would be generally more willing to make assurances than to provide contractual guarantees.[513] If the covered institution could not obtain the reasonable assurances required under this alternative, the covered institution would need to switch service providers and bear the associated switching costs, while the service providers would suffer loss of customers. Although the costs of obtaining reasonable assurances would likely be lower than under the proposed service provider provisions, and the need to switch providers less frequent, these costs could nonetheless be particularly acute for smaller covered institutions who lack bargaining power with generic service providers. And, as outlined above, this alternative would be less protective than contractual language.

---

512 *See supra* section III.D.1.b (discussing the proposed requirement for covered institutions to enter into written contracts with their service providers).

513 *See id.* Additionally, the service provider's standard terms and conditions might in some situations provide reasonable assurances adequate to meet the requirement.

2. Lower Threshold for Customer Notice

The Commission considered lowering the threshold for customer notice, such as one based on the "possible misuse" of sensitive customer information (rather than the proposed threshold requiring notice when sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization), or even requiring notification of any breach without exception. A lower threshold would increase the number of notices customers receive. Although more frequent notices could potentially reveal incidents that warrant customers' attention and thereby potentially increase the benefits accruing to customers from the notice requirement discussed in section III.D.1.c, they would also increase the number of false alarms. As discussed in section III.D.1.c.iv, such false alarms could be problematic if they reduce customers' ability to discern which notices require action.

Although a lower threshold could impose some additional compliance costs on covered institutions (due to additional notices being sent), we would not anticipate the additional direct compliance costs to be significant.[514] Of more economic significance to covered institutions would be the resulting reputational effects.[515] However, the direction of these effects is ambiguous. On the one hand, increased notices resulting from a lower threshold can be expected to lead to additional reputation costs for firms required to issue more of such notices. On the other hand, lower thresholds could inundate customers with notices, such that notices are no longer notable, likely leading the negative reputation effects associated with such notices to be reduced.

3. Encryption Safe Harbor

The Commission considered including a safe harbor to the notification requirement for breaches in which only cipher text was compromised. Assuming that such an alternative safe harbor would be sufficiently circumscribed to prevent its application to insecure encryption

---

514 The direct compliance costs of notices are discussed in section IV.

515 *See supra* section III.B.

algorithms, or to secure algorithms used in a manner as to render them insecure, we believe that the economic effects of its inclusion would be largely indistinguishable from the proposal. This is because, as proposed, notification is triggered by the "reasonable likelihood" that sensitive customer information was accessed or used without authorization.[516] Given the computational complexity involved in cracking the cipher texts of modern encryption algorithms generally viewed as secure, the compromise of cipher text produced by such algorithms in accordance with secure procedures[517] would generally not give rise to "a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information."[518] It would thus not constitute "sensitive customer information," meaning that the threshold for providing notice would not be met and thereby rendering an explicit encryption safe harbor superfluous in such cases. In certain other cases, however, an express safe harbor may not be as protective as the proposal's minimum nationwide standard for determining whether the compromise of customer information could create "a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information."[519] It may also become outdated as technologies and security practices evolve. Thus, while an explicit (and appropriately circumscribed) safe harbor could provide some procedural efficiencies from streamlined application, it could also be misapplied.

---

516 Proposed rule 248.30(b)(3)(iii).

517 Here, "secure procedures" refers to the secure implementation of encryption algorithms and encompasses proper key generation and management, timely patching, user access controls, etc.

518 Proposed rule 248.30(e)(9); *see also supra* note 112 and accompanying text.

519 *See* proposed rule 248.30(e)(9). The August 2022 breach of the LastPass cloud-based password manager provides an illustrative example. In this data breach a large database of website credentials belonging to LastPass' customers was exfiltrated. The customer credentials in this database were encrypted using a secure algorithm and the encryption keys could not have been exfiltrated in the breach, so an encryption safe harbor could be expected to apply in such a case. Nonetheless, customers whose encrypted passwords were divulged in the breach became potential targets for brute force attacks (*i.e.,* attempts to decrypt the passwords by guessing a customer's master password) and to phishing attacks (*i.e.,* attempts to induce an affected customer to divulge the master password). *See* Karim Toubba, *Notice of Recent Security Incident*, LASTPASS (Dec. 22, 2022), *available at* https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/; *see also* Craig Clough, *LastPass Security Breach Drained Bitcoin Wallet, User Says*, PORTFOLIO MEDIA (Jan. 4, 2023), *available at* https://www.law360.com/articles/1562534/lastpass-security-breach-drained-bitcoin-wallet-user-says.

4. Longer Customer Notification Deadlines

The Commission considered incorporating longer customer notification deadlines, such as 60 or 90 days, as well as providing no fixed customer notification deadline. Although longer notification deadlines would provide more time for covered institutions to rebut the presumption in favor of notification discussed in section II.A.4.a, we expect that longer investigations would, in general, correlate with more serious or complicated incidents and would therefore be unlikely to end in a determination 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. We therefore do not believe that longer notification deadlines would ultimately lead to significantly fewer required notifications. Compliance costs conditional on notices being required (*i.e.*, the actual furnishing of notices to customers) would be largely unchanged under alternative notice deadlines. That said, costs related to incident assessment would likely be somewhat lower due to the reduced urgency of determining the scope of an incident and a reduced likelihood that notifications would need to be made before an incident has been contained.[520] Arguably, longer notification deadlines may increase reputation costs borne by covered institutions that choose to take advantage of the longer deadlines. Overall, however, we do not expect that longer notification deadlines would lead to costs for covered institutions that differ significantly from the costs of the proposed 30-day deadline.

Providing for longer notifications deadlines would likely reduce the promptness with which some covered institutions issue notifications to customers, potentially reducing their customers' ability to take effective mitigating actions. In particular, as discussed in section III.D.1.c.iii, some breaches are discovered very quickly. For customers whose sensitive customer information is compromised in such breaches, a longer notification deadline could significantly

---

[520] *See supra* section III.D.1.c.iii.

reduce the timeliness—and value—of the notice.[521] On the other hand, where a public announcement could hinder containment efforts, a longer notification timeframe could yield benefits to the broader public (and/or to the affected investors).[522]

5. Broader Law Enforcement Exception from Notification Requirements

The Commission considered providing for a broader exception to the 30-day notification deadline, for example by extending its applicability to cases where any appropriate law enforcement agency requests the delay, and not limiting the length of the delay. This alternative law enforcement exception would more closely align with the law enforcement exceptions adopted by the Banking Agencies[523] and many states.[524]

The principal function of a law enforcement exception would be to allow a law enforcement or national security agency to keep cybercriminals unaware of their detection. Observing a cyberattack that is in progress can allow investigators to take actions that can assist in revealing the attacker's location, identity, or methods.[525] Notifying affected customers has the potential to alert attackers that their intrusion has been detected, hindering these efforts.[526] Thus, a broader law enforcement exception could generally be expected to enhance law enforcement's efficacy in cybercrime investigations, which would potentially benefit affected customers through damage mitigation and benefit the general public through improved deterrence and increased recoveries, and by enhancing law enforcement's knowledge of attackers' methods.

---

521 *See supra* note 462 and accompanying text.

522 *See supra* section II.A.4.e

523 *See* Banking Agencies' Incident Response Guidance*, supra* note 47.

524 *See, e.g.,* RCW 19.255.010(8); Fla. Stat. sec. 501.171(4)(b).

525 *Cybersecurity Advisory: Technical Approaches to Uncovering and Remediating Malicious Activity*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Sept. 24, 2020), *available at* https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a (explaining how and why investigators may "avoid tipping off the adversary that their presence in the network has been discovered").

526 *Id*.

That said, use of the exception would necessarily delay notice to customers affected by a cyber-attack, reducing the value to customers of such notices.[527] Incidents where law enforcement would like to delay customer notifications are likely to involve numerous customers, who—without timely notice—may be unable to take timely mitigating actions that could prevent additional harm.[528] Law enforcement investigations can also take time to resolve and, even when successful, their benefits to affected customers (e.g., recovery of criminals' ill-gotten gains) may be limited.

Information about cybercrime investigations is often confidential. The Commission does not have data on the prevalence of covert cybercrime investigations, their success or lack of success, their deterrent effect if any, or the impact of customer notification on investigations. Thus, we are unable to quantify the costs and benefits of this alternative. We invite public comment on these topics.

G. Request for Comment on Economic Analysis

To assist the Commission in better assessing the economic effects of the proposal, we request comment on the following questions:

107. What additional qualitative or quantitative information should be considered as part of the baseline for the economic analysis of the proposals?
108. Are the effects on competition, efficiency, and capital formation arising from the proposed amendments accurately characterized? If not, why not?
109. Are the economic effects of the alternatives accurately characterized? If not, why not?
110. Are the costs and benefits of the proposals accurately characterized? If not, why not? What, if any, other costs or benefits should be taken into account? Please

---

527 *See supra* note 462 and accompanying text.

528 *See supra section* III.D.1.c.iii.

provide data that could help us quantify any of the aforementioned costs and benefits that we have been unable to quantify.

111. Do institutions that would be covered by this proposal already comply with one or more state data breach notification requirements? If so, how similar or different are the compliance obligations under the state data breach notification laws and our proposal?

112. Do existing contracts between covered institutions and service providers address notification in the event of a data breach? If so, in what circumstances does the service provider notify either the covered institution or the customer whose data was compromised?

113. Do you believe the Commission has accurately characterized the cost of service providers adapting business practices to accommodate the proposed requirements? Please state why or why not, in as much detail as possible.

114. Do policies and procedures implemented to comply with Regulation S-ID incorporate red flags related to potential compromise of customer information?

115. Have potentially covered institutions developed and implemented written policies and procedures for response to data breach incidents?

    a. If so, please indicate whether these policies and procedures are written to comply with state data breach notification laws, international law, contracts, and/or other law or guidance.

    b. If so, please indicate which elements (*e.g.,* detection, assessment, containment, lessons learned, notification) such policies contain.

    c. Please indicate what kind of institution (*e.g.*, broker, transfer agent, etc.) your experience reflects.

116. Have service providers to potentially covered institutions developed and implemented written policies and procedures for response to data breach incidents?

a. If so, please indicate whether these policies and procedures are written to comply with state data breach notification laws, international law, contracts, and/or other law or guidance.

b. If so, please indicate which elements (*e.g.,* detection, assessment, containment, lessons learned, notification) such policies contain.

c. Please indicate what kind of service provider your experience reflects.

117. Do you believe that written policies and procedures to safeguard information lead to reduced risk of safeguard failures? Please share your experience or the basis for your belief.

118. Do you believe that safeguarding the customer information of customers of other financial institutions, or notifying these individuals in the event their sensitive customer information is compromised would entail additional costs?

a. If so, please indicate the nature and scale of the costs.

b. If so, please characterize the population of individuals whose sensitive customer information would entail these significant additional costs.

119. Do you believe a broader law enforcement exception would provide benefits?

a. If so, please indicate the nature and scale of these benefits.

b. If so, to the extent possible, please provide data or case studies that could help establish the scale of these benefits.

120. Do you believe that use of a broader law enforcement exception would entail significant costs to individuals whose sensitive customer information is compromised?

a. If so, please indicate the nature and scale of these costs.

b. If so, to the extent possible, please provide data or case studies that could help establish the scale of these costs.

IV. PAPERWORK REDUCTION ACT

A. Introduction

Certain provisions of the proposed amendments contain "collection of information" requirements within the meaning of the Paperwork Reduction Act of 1995 ("PRA").[529] We are submitting the proposed collection of information to the Office of Management and Budget ("OMB") for review in accordance with the PRA.[530] The safeguards rule and the disposal rule we propose to amend would have an effect on the currently approved existing collection of information under OMB Control No. 3235-0610, the title of which is, "Rule 248.30, Procedures to safeguard customer records and information; disposal of consumer report information."[531]

An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. The proposed requirement to adopt policies and procedures constitutes a collection of information requirement under the PRA. The collection of information associated with the proposed amendments would be mandatory, and responses provided to the Commission in the context of its examination and oversight program concerning the proposed amendments would be kept

---

529 44 U.S.C. 3501 through 3521.

530 44 U.S.C. 3507(d); 5 CFR 1320.11.

531 The paperwork burden imposed by Regulation S-P's notice and opt-out requirements, 17 CFR 248.1 to 248.18, is currently approved under a separate OMB control number, OMB Control No. 3235-0537. The proposed amendments would implement a statutory exception that has been in effect since late 2015. We do not believe that the proposed amendment to implement the statutory exception makes any substantive modifications to this existing collection of information requirement or imposes any new substantive recordkeeping or information collection requirements within the meaning of the PRA. Similarly, we do not believe that the proposed amendments to: (i) Investment Company Act rules 31a-1(b) (OMB control number 3235-0178) and 31a-2(a) (OMB control number 3235-0179) for investment companies that are registered under the Investment Company Act, (ii) Investment Advisers Act rule 204-2 (OMB control number 3235-0278) for investment advisers, (iii) Exchange Act rule 17a-4 (OMB control number 3235-0279) for broker-dealers, and (iv) Exchange Act rule 17Ad-7 (OMB control number 3235-0291) for transfer agents, makes any modifications to this existing collection of information requirement or imposes any new recordkeeping or information collection requirements. Accordingly, we believe that the current burden and cost estimates for the existing collection of information requirements remain appropriate, and we believe that the proposed amendments should not impose substantive new burdens on the overall population of respondents or affect the current overall burden estimates for this collection of information. We are, therefore, not revising any burden and cost estimates in connection with these amendments.

confidential subject to the provisions of applicable law. A description of the proposed amendments, including the need for the information and its use, as well as a description of the types of respondents, can be found in section II above, and a discussion of the expected economic effects of the proposed amendments can be found in section III above.

B. Amendments to the Safeguards Rule and Disposal Rule

As discussed above, the proposed amendments to the safeguards rule would require covered institutions to develop, implement, and maintain written policies and procedures that include incident response programs reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures. The response program must include procedures to assess the nature and scope of any incident involving unauthorized access to or use of customer information; take appropriate steps to contain and control the incident; and provide notice to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization (unless the covered institution makes certain determinations as specified in the proposed rule).

The proposed amendments to the disposal rule would require covered institutions that maintain or otherwise possess customer information or consumer information for a business purpose to adopt and implement written policies and procedures that address proper disposal of such information, which would include taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

Finally, the proposed amendments would require covered institutions to make and maintain written records documenting compliance with the requirements of the safeguards rule and the disposal rule. Under the proposed rules, the time periods for preserving records would vary by covered institution to be consistent with existing recordkeeping rules. [532]

---

[532] The proposed amendments would also broaden the scope of information covered by the safeguards rule and the disposal rule (to include *all* customer information in the possession of a

Based on FOCUS Filing and Form BD-N data, as of December 2021, there were 3,401 brokers or dealers other than notice-registered brokers or dealers. Based on Investment Adviser Registration Depository data, as of June 2022, there were 15,129 investment advisers registered with the Commission. As of December 2021, there were 13,965 investment companies.[533] Based on Form TA-1, as of December, 2021, there were 335 transfer agents registered with the Commission and 67 transfer agents registered with the Banking Agencies.

Table 2 below summarizes our PRA initial and ongoing annual burden estimates associated with the proposed amendments to the safeguards rule and the disposal rule.

Table 2: Proposed Amendments to Safeguards Rule and Disposal Rule - PRA

	Internal initial burden hours	Internal annual burden hours[1]		Wage rate[2]	Internal time cost	Annual external cost burden
PROPOSED ESTIMATES						
Adopting and implementing policies and procedures	60 hours	25 hours[3]		$455 (blended rate for compliance attorney and assistant general counsel)	$11,375 (equal to the internal annual burden X the wage rate)	$2,655[4]
Preparation and distribution of notices	9 hours	8 hours[5]		$300 (blended rate for senior compliance examiner and compliance manager)	$2,400 (equal to the internal annual burden X the wage rate)	$2,018[6]
Recordkeeping	1 hour	1 hour		$381 (blended rate for compliance attorney and	$381	$0

covered institution, and all consumer information that a covered institution maintains or otherwise possesses for a business purpose) and extend the application of the safeguards provisions to transfer agents registered with the Commission or another appropriate regulatory agency. These amendments do not contain collections of information beyond those related to the incident response program analyzed above.

533 Data on investment companies registered with the Commission comes from Form N-CEN filings; data on BDCs comes from Forms 10-K and 10-Q; and data on employees' securities companies comes from Form 40-APP. *See supra* Table 1.

				senior programmer)		
Total new annual burden per covered institution		34 hours (equal to the sum of the above three boxes)			$14,156 (equal to the sum of the above three boxes)	$4,673 (equal to the sum of the above two boxes)
Number of covered institutions		x 32,897 covered institutions[7]			x 32,897 covered institutions	16,449[8]
Total new annual aggregate burden		1,118,498 hours			$465,689,932	$76,866,177
TOTAL ESTIMATED BURDENS INCLUDING AMENDMENTS						
Current aggregate annual burden estimates		+ 47,565 hours				+ $0
Revised aggregate annual burden estimates		1,166,063 hours				$76,866,177

Notes:

1. Includes initial burden estimates annualized over a 3-year period.
2. The Commission's estimates of the relevant wage rates are based on the SIFMA Wage Report. The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.
3. Includes initial burden estimates annualized over a three-year period, plus 5 hours of ongoing annual burden hours. The estimate of 2560 hours is based on the following calculation: ((60 initial hours/3) + 5 hours of additional ongoing burden hours) = 25 hours.
4. This estimated burden is based on the estimated wage rate of $531/hour, for 5 hours, for outside legal services. The Commission's estimates of the relevant wage rates for external time costs, such as outside legal services, takes into account staff experience, a variety of sources including general information websites, and adjustments for inflation.
5. Includes initial burden estimate annualized over a three-year period, plus 5 hours of ongoing annual burden hours. The estimate of 8 hours is based on the following calculation: ((9 initial hours / 3 years) + 5 hours of additional ongoing burden hours) = 8 hours.
6. This estimated burden is based on the estimated wage rate of $531/hour, for 3 hours, for outside legal services and $85/hour, for 5 hours, for a senior general clerk.
7. Total number of covered institutions is calculated as follows: 3,401 broker-dealers other than notice-registered broker-dealers + 15,129 investment advisers registered with the Commission + 13,965 investment companies + 335 transfer agents registered with the Commission + 67 transfer agents registered with the Banking Agencies = 32,897 covered institutions.
8. We estimate that 50% of covered institutions will use outside legal services for these collections of information. This estimate takes into account that covered institutions may elect to use outside legal services (along with in-house counsel), based on factors such as budget and the covered institution's standard practices for using outside legal services, as well as personnel availability and expertise.

C. Request for Comment

We request comment on whether these estimates are reasonable. Pursuant to 44 U.S.C. 3506(c)(2)(B), the Commission solicits comments in order to: (1) evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information will have practical utility; (2) evaluate the accuracy of the Commission's estimate of the burden of the proposed collection of information; (3) determine whether there are ways to enhance the quality, utility, and clarity of the information to be collected; and (4) determine whether there are ways to minimize the burden of the collection of information on those who are to respond, including through the use of automated collection techniques or other forms of information technology.

Persons wishing to submit comments on the collection of information requirements of the proposed amendments should direct them to the OMB Desk Officer for the Securities and Exchange Commission, MBX.OMB.OIRA.SEC_desk_officer@omb.eop.gov, and should send a copy to Vanessa A. Countryman, Secretary, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-1090, with reference to File No. S7-05-23. OMB is required to make a decision concerning the collections of information between 30 and 60 days after publication of this release; therefore, a comment to OMB is best assured of having its full effect if OMB receives it within 30 days after publication of this release. Requests for materials submitted to OMB by the Commission with regard to these collections of information should be in writing, refer to File No. S7-05-23, and be submitted to the Securities and Exchange Commission, Office of FOIA Services, 100 F Street NE, Washington, DC, 20549-2736.

V. INITIAL REGULATORY FLEXIBILITY ACT ANALYSIS

The Regulatory Flexibility Act[534] ("RFA") requires an agency, when issuing a rulemaking proposal, to prepare and make available for public comment an Initial Regulatory Flexibility Analysis ("IRFA") that describes the impact of the proposed rule on small entities,

---

534 *See* 5 U.S.C. 601 *et seq*.

unless the Commission certifies that the rule, if adopted, would not have a significant economic impact on a substantial number of small entities.[535] This IRFA has been prepared in accordance with the RFA. It relates to the proposed new rules and amendments described in sections II through IV above.

A. Reason For and Objectives of the Proposed Action

The objectives of the proposed amendments are to: (i) establish a Federal minimum standard for providing notification to all customers of a covered institution affected by a data breach (regardless of state residency) and providing consistent disclosure of important information to help affected customers respond to a data breach; (ii) 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; (iii) enhance the protection of customers' nonpublic personal information by aligning the information protected under the safeguards rule and the disposal rule by applying the protections of both rules to "customer information," while also broadening the group of customers whose information is protected under both rules; and (iv) bring all transfer agents within the scope of the safeguards rule and the disposal rule. The proposed amendments also would update applicable recordkeeping requirements and conform Regulation S-P's annual privacy notice delivery provisions to the terms of a statutory exception. The proposed amendments are intended to:

A. Prevent and mitigate the unauthorized access to or use of customer information;

B. Improve covered institutions' preparedness to respond to data breaches involving customer information, and the effectiveness of their response programs to such data breaches when they do occur;

---

535 *See* 5 U.S.C. 603(a); 5 U.S.C. 605(b).

C. Ensure that firms consistently monitor their systems to identify, contain, and control data breach incidents involving customer information quickly;

D. Help affected individuals through the adoption of a minimum standard for notification in response to unauthorized access or use of sensitive customer information that leverages some of the more protective state law practices already in existence;

E. Expand the coverage of the safeguards rule to provide for greater protection of customer information that is maintained by transfer agents;

F. Extend the protections of Regulation S-P to cover customer information that covered institutions receive from another financial institution in the process of conducting business;

G. Create more consistent standards across the safeguards rule and the disposal rule for the handling of the same types of nonpublic personal information; and

H. Require that a covered institution's response program include policies and procedures that require a covered institution, by contract, to require that its service providers take appropriate measures that are designed to protect against unauthorized access to or use of customer information.

B. Legal Basis

We are proposing the new rules and rule amendments described above under the 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].

C. Small Entities Subject to Proposed Rule Amendments

The proposed amendments to Regulation S-P would affect brokers, dealers, registered investment advisers, investment companies, and transfer agents, including entities that are considered to be a small business or small organization (collectively, "small entity") for purposes of the RFA. For purposes of the RFA, under the Exchange Act 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.[536] 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.[537] Under the Investment Company Act, investment companies are considered small entities if they, together with other funds in the same group of related funds, have net assets of $50 million or less as of the end of its most recent fiscal year.[538] Under the Investment Advisers Act, a small entity is an investment adviser that: (i) manages less than $25 million in assets; (ii) has total assets of less than $5 million on the last day of its most recent fiscal year; and (iii) does not control, is not controlled by, and is not under common control with another investment adviser that manages $25 million or more in assets, or any person that has had total assets of $5 million or more on the last day of the most recent fiscal year.[539]

---

536 17 CFR 240.0-10.

537 *Id.*

538 17 CFR 270.0-10.

539 17 CFR 275.0-7.

Based on Commission filings, we estimate that approximately 764 broker-dealers,[540] 158 transfer agents,[541] 85 investment companies,[542] and 522 registered investment advisers[543] may be considered small entities.

D. Projected Reporting, Recordkeeping, and Other Compliance Requirements

The proposed amendments to Regulation S-P would require covered institutions to develop incident response programs for unauthorized access to or use of customer information, as well as imposing a customer notification obligation in instances where sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. The proposed amendments also would include new mandatory recordkeeping requirements and language conforming Regulation S-P's annual privacy notice delivery provisions to the terms of a statutory exception.

Under the proposed amendments, covered institutions would have to develop, implement, and maintain, within their written policies and procedures designed to comply with Regulation S-P, a program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures. Such policies and procedures would also need to require that covered institutions, pursuant to a written contract between the covered institution and its service providers, require the service providers to take appropriate measures designed to protect against unauthorized access to or use of customer information, including by notifying the covered institution as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security that results in

---

540 Estimate based on FOCUS Report data collected by the Commission as of September 30, 2022.

541 Estimate based on the number of transfer agents that reported a value of fewer than 1,000 for items 4(a) and 5(a) on Form TA-2 for the 2021 annual reporting period (which, was required to be filed by March 31, 2022).

542 Based on Commission staff approximation that as of June 2022, approximately 43 open-end funds (including 11 exchange-traded funds), 31 closed-end funds, and 11 business development companies are small entities. *See* Tailored Shareholder Reports for Mutual Funds and Exchange-Traded Funds; Fee Information in Investment Company Advertisements, Securities Act Release No. 11125 (Oct. 26, 2022) [87 FR 72758-01 (Nov. 25, 2022)].

543 Estimate based on IARD data as of June 30, 2022.

unauthorized access to a customer information system maintained by the service provider, in order to enable the covered institution to implement its response program. If an incident were to occur, 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 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 to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. As part of its incident response program, a covered institution may also enter into a written agreement with its service provider to have the service provider notify affected individuals on its behalf.

In addition, covered institutions would be required to make and maintain specified written records designed to evidence compliance with these requirements. Such records would be required to be maintained starting from when the record was made, or from when the covered institution terminated the use of the written policy or procedure, for the time periods stated in the amended recordkeeping regulations for each type of covered institution.[544]

Some covered institutions, including covered institutions that are small entities, would incur increased costs involved in reviewing and revising their current safeguarding policies and procedures to comply with these obligations, including their cybersecurity policies and procedures. Initially, this would require covered institutions to develop as part of their written policies and procedures under the safeguards rule, a program reasonably designed to detect, respond to, and recover from any unauthorized access to or use of customer information,

---

[544] Specifically, the proposal would amend (i) Investment Company Act rules 31a-1(b) and 31a-2(a) for investment companies that are registered under the Investment Company Act, (ii) proposed rule 248.30(d) under Regulation S-P for unregistered investment companies, (iii) Investment Advisers Act rule 204-2 for investment advisers, (iv) Exchange Act rule 17a-4 for broker-dealers, and (v) Exchange Act rule 17Ad-7 for transfer agents.

including customer notification procedures, in a manner that provides clarity for firm personnel. Further, in developing these policies and procedures, covered institutions would need to include policies and procedures requiring the covered institution, pursuant to a written contract, to require its service providers to take appropriate measures that are designed to protect against unauthorized access to or use of customer information, including notifying the covered institution as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security resulting in unauthorized access to a customer information system maintained by the service provider, in order to enable the covered institution to implement its response program. However, as the Commission recognizes the number and varying characteristics (*e.g.*, size, business, and sophistication) of covered institutions, these proposed amendments would help covered institutions to tailor these policies and procedures and related incident response program based on the individual facts and circumstances of the firm, and provide flexibility in addressing the general elements of the response program requirements based on the size and complexity of the covered institution and the nature and scope of its activities.

In addition, the Commission acknowledges that the proposed rule would impose greater costs on those transfer agents that are registered with another appropriate regulatory agency, if they are not currently subject to Regulation S-P, as well as those transfer agents registered with the Commission who are not currently subject to the safeguards rule. As discussed above, such costs would include the development and implementation of necessary policies and procedures, the ongoing costs of required recordkeeping and maintenance requirements, and, where necessary, the costs to comply with the customer notification requirements of the proposed rule. Such costs would also include the same minimal costs for employee training or establishing clear procedures for consumer report information disposal that are imposed on all covered institutions. To the extent that such costs are being applied to a transfer agent for the first time as a result of new obligations being imposed, the proposed rule would incur higher present costs on those

transfer agents than those covered institutions that are already subject to the safeguards rule and the disposal rule.

To comply with these amendments on an ongoing basis, covered institutions would need to respond appropriately to incidents that entail the unauthorized access to or use of customer information. This would entail carrying out the established response program procedures 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; (ii) take appropriate steps to contain and control 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, 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, 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.

Where the covered institution determines notice is required, the covered institution would need to provide a clear and conspicuous notice to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. This notice would need to be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing. Further, the covered institution would need to satisfy the specified content requirements of that notice,[545] the preparation of which would incur some incremental additional costs on covered institutions.

---

[545] *See* proposed rule 248.30(b)(4)(iv). In particular, the covered institution would need to: (i) 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; (ii) describe what has been done to protect the sensitive customer information from further unauthorized access or use; (iii) 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

Finally, covered institutions would also face costs in complying with the new recordkeeping requirements imposed by these amendments that are incrementally more than those costs covered institutions already incur from their existing regulatory recordkeeping obligations, in light of their already existing record retention systems. However, the Commission has proposed such record maintenance provisions to align with those most frequently employed as to each covered institution subject to this rulemaking, partially in an effort to minimize these costs to firms.

Overall, incremental costs would be associated with the proposed amendments to Regulation S-P.[546] Some proportion of large or small institutions would be likely to experience some increase in costs to comply with the proposed amendments if they are adopted.

More specifically, we estimate that many covered institutions would incur one-time costs related to reviewing and revising their current safeguarding policies and procedures to comply with these obligations, including their cybersecurity policies and procedures. Additionally, some covered institutions, including transfer agents, may incur costs associated with establishing such policies and procedures as these amendments require if those covered institutions do not already

---

date range within which the incident occurred; (iv) 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; (v) 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; (vi) 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; (vii) recommend that the individual periodically obtain credit reports from each nationwide credit reporting company and have information relating to fraudulent transactions deleted; (viii) explain how the individual may obtain a credit report free of charge; and (ix) 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.

546 Covered institutions are currently subject to similar recordkeeping requirements applicable to other required policies and procedures. Therefore, covered institutions will generally not need to invest in new recordkeeping staff, systems, or procedures to satisfy the new recordkeeping requirements; *see supra* note 491 and accompanying text.

have such policies and procedures. We also estimate that the ongoing, long-term costs associated with the proposed amendments could include costs of responding appropriately to incidents that entail the unauthorized access to or use of customer information.

We encourage written comments regarding this analysis. We solicit comments as to whether the proposed amendments could have an effect that we have not considered. We also request that commenters describe the nature of any impact on small entities and provide empirical data to support the extent of the impact. In addition, we solicit comments regarding our proposal to amend Regulation S-P's annual privacy notice delivery provisions to conform to the terms of a statutory exception.

E. Duplicative, Overlapping, or Conflicting Federal Rules

As discussed above, the proposed amendments would impose requirements that covered institutions develop response programs for unauthorized access to or use of customer information in the form of written policies and procedures designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures. Covered institutions are subject to requirements elsewhere under the Federal securities laws and rules of the self-regulatory organizations that require them to adopt written policies and procedures that may relate to some similar issues.[547] The proposed amendments to Regulation S-P, however, would not require covered institutions to maintain duplicate copies of

---

[547] *See, e.g.*, 15 U.S.C. 80b-4a (requiring each adviser registered with the Commission to have written policies and procedures reasonably designed to prevent misuse of material non-public information by the adviser or persons associated with the adviser); 17 CFR 270.38a-1(a)(1) (requiring investment companies to adopt compliance policies and procedures); 275.206(4)-7(a) (requiring investment advisers to adopt compliance policies and procedures); Regulation S-ID, 17 CFR part 248, subpart C, (requiring financial institutions subject to the Commission's jurisdiction with covered accounts to develop and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with covered accounts, which must include, among other things, policies and procedures to respond appropriately to any red flags that are detected pursuant to the program); and FINRA Rule 3110 (requiring each broker-dealer to establish and maintain written procedures to supervise the types of business it is engaged in and to supervise the activities of registered representatives and associated persons, which could include registered investment advisers).

records covered by the rule, and an institution's incident response program for unauthorized access to or use of customer information would not have to be maintained in a single location. We preliminarily believe, therefore, that any duplication of regulatory requirements would be limited and would not impose significant additional costs on covered institutions including small entities.[548] With the exception of the Banking Agencies' Incident Response Guidance and their requirements for safeguarding customer information and disposing of consumer financial report information as they apply to transfer agents that are registered with another appropriate regulatory agency, we believe there are no other Federal rules that duplicate, overlap, or conflict with the proposed reporting requirements.

In the case of transfer agents that are registered with another appropriate regulatory agency, the proposed rule might be considered duplicative of or overlapping with the Banking Agencies' Incident Response Guidance. Specifically, the proposed rule might be considered to overlap or conflict with the Banking Agencies' Incident Response Guidance regarding the safeguarding of customer information, disposal of consumer financial report information, and as to procedures for customer notification in connection with an incident response program.

In general, however, the similarities between the proposed reporting requirements and existing reporting requirements under rules of the Banking Agencies and the FTC are the result of our statutory mandate to set standards for safeguarding customer records and information that are consistent and comparable with the corresponding standards set by the other agencies.

F. Significant Alternatives

The Regulatory Flexibility Act directs us to consider significant alternatives that would accomplish the stated objectives, while minimizing any significant adverse impact on small entities. In connection with the proposed amendments, we considered the following alternatives:

---

548 *See supra* section II.G.

1. establishing different compliance or reporting standards that take into account the resources available to small entities;
2. the clarification, consolidation, or simplification of the reporting and compliance requirements under the rule for small entities;
3. use of performance rather than design standards; and
4. exempting small entities from coverage of the rule, or any part of the rule.

With regard to the first alternative, we have proposed amendments to Regulation S-P that would continue to permit institutions substantial flexibility to design safeguarding policies and procedures appropriate for their size and complexity, the nature and scope of their activities, and the sensitivity of the personal information at issue. We nevertheless believe it necessary to propose to require that covered institutions, regardless of their size, adopt a response program for incidents of unauthorized access to or use of customer information, which would include customer notification procedures.[549] The proposed amendments to Regulation S-P arise from our concern with the increasing number of information security breaches that have come to light in recent years, particularly those involving institutions regulated by the Commission. Establishing different compliance or reporting requirements for small entities could lead to less favorable protections for these entities' customers and compromise the effectiveness of the proposed amendments.

With regard to the second alternative, the proposed amendments should, by their operation, simplify reporting and compliance requirements for small entities. Small covered institutions are likely to maintain personal information on fewer individuals than large covered institutions, and they are likely to have relatively simple personal information systems. The proposed amendments would not prescribe specific steps a covered institution must take in response to a data breach, but instead would give the institution flexibility to tailor its policies

---

[549] *See* proposed rule 248.30(b)(3).

and procedures to its individual facts and circumstances. The proposed amendments therefore are intended to give covered institutions the flexibility to address the general elements in the response program based on the size and complexity of the institution and the nature and scope of its activities. Accordingly, the requirements of the proposed amendment already would be simplified for small entities. In addition, the requirements of the proposed amendments could not be further simplified, or clarified or consolidated, without compromising the investor protection objectives the proposed amendments are designed to achieve.

With regard to the third alternative, the proposed amendments are design based. Rather than specifying the types of policies and procedures that an institution would be required to include in its response program, the proposed amendments would require a response program that is reasonably designed to detect, respond to, and recover from both unauthorized access to and unauthorized use of customer information. With respect to the specific requirements regarding notifications in the event of a data breach, we have proposed that institutions provide only the information that seems most relevant for an affected customer to know in order to assess adequately the potential damage that could result from the breach and to develop an appropriate response.

Finally, with regard to alternative four, we preliminarily believe that an exemption for small entities would not be appropriate. Small entities are as vulnerable as large ones to the types of data security breach incidents we are trying to address. In this regard, the specific elements we have proposed must be considered and incorporated into the policies and procedures of all covered institutions, regardless of their size, to mitigate the potential for fraud or other substantial harm or inconvenience to investors. Exempting small entities from coverage of the proposed amendments or any part of the proposed amendments could compromise the effectiveness of the proposed amendments and harm investors by lowering standards for safeguarding investor information maintained by small covered institutions. Excluding small entities from requirements that would be applicable to larger covered institutions also could

create competitive disparities between large and small entities, for example by undermining investor confidence in the security of information maintained by small covered institutions.

We request comment on whether it is feasible or necessary for small entities to have special requirements or timetables for, or exemptions from, compliance with the proposed amendments. In particular, could any of the proposed amendments be altered in order to ease the regulatory burden on small entities, without sacrificing the effectiveness of the proposed amendments?

G. Request for Comment

We encourage the submission of comments with respect to any aspect of this IRFA. In particular, we request comments regarding:

121. The number of small entities that may be affected by the proposed rules and amendments;
122. The existence or nature of the potential impact of the proposed rules and amendments on small entities discussed in the analysis;
123. How the proposed amendments could further lower the burden on small entities; and
124. How to quantify the impact of the proposed rules and amendments.

Commenters are asked to describe the nature of any impact and provide empirical data supporting the extent of the impact. Comments will be considered in the preparation of the Final Regulatory Flexibility Analysis, if the proposed rules and amendments are adopted, and will be placed in the same public file as comments on the proposed rules and amendments themselves.

VI. CONSIDERATION OF IMPACT ON THE ECONOMY

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996 ("SBREFA"), the Commission must advise OMB whether a proposed regulation constitutes a "major" rule. Under SBREFA, a rule is considered "major" where, if adopted, it results in or is likely to result in:

A. An annual effect on the economy of $100 million or more;
B. A major increase in costs or prices for consumers or individual industries; or
C. Significant adverse effects on competition, investment, or innovation.

We request comment on whether our proposal would be a "major rule" for purposes of SBREFA. We solicit comment and empirical data on:

- The potential effect on the U.S. economy on an annual basis;
- Any potential increase in costs or prices for consumers or individual industries; and
- Any potential effect on competition, investment, or innovation.

Commenters are requested to provide empirical data and other factual support for their views to the extent possible.

STATUTORY AUTHORITY

The Commission is proposing to amend 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

in 17 CFR Parts 240, 270, and 275

Reporting and recordkeeping requirements; Securities.

in 17 CFR Part 248

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

Text of Proposed Amendments

For the reasons set out in the preamble, the Securities and Exchange Commission proposes to amend 17 CFR chapter II as follows:

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

1. The authority citation for part 240 continues to read, in part, 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, 78*l*, 78m, 78n, 78n-1, 78*o*, 78*o*-4, 78*o*-10, 78p, 78q, 78q-1, 78s, 78u-5, 78w, 78x, 78dd, 78*ll*, 78mm, 80a-20, 80a-23, 80a-29, 80a-37, 80b-3, 80b-4, 80b-11, and 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 paragraphs (e)(13) and (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(b)(1) 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(b)(3) 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(b)(4), including the basis for any determination made, 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(b)(5)(i) 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(b)(5) 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(c)(2) until three years after the termination of the use of the policies and procedures;

* * * * *

3. Amend §240.17Ad-7 by revising the section heading and adding paragraphs (j) and (k) to 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(b)(1) 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(b)(3) 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(b)(4), including the basis for any determination made, 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(b)(5)(i) 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(b)(5) 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(c)(2) 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, in part, as follows:

Authority: 15 U.S.C. 78q, 78q–1, 78*o*–4, 78*o*–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 § 248.2 by revising paragraph (c) to read as follows:

§ 248.2 Model privacy form: rule of construction.

* * * * *

(c) *Substituted compliance with CFTC financial privacy rules by futures commission merchants and introducing brokers.* Except with respect to § 248.30(c), any futures commission merchant or introducing broker (as those terms are defined in the Commodity Exchange Act (7 U.S.C. 1, et seq.)) registered by notice with the Commission for the purpose of conducting business in security futures products pursuant to section 15(b)(11)(A) of the Securities Exchange Act of

1934 (15 U.S.C. 78o(b)(11)(A)) that is subject to and in compliance with the financial privacy rules of the Commodity Futures Trading Commission (17 CFR part 160) will be deemed to be in compliance with this part.

6. Amend §248.5 by revising the first sentence of paragraph (a)(1), and adding paragraph (e).

The revision and addition 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:

(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 notic*e. 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 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.

7. 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."

8. 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) *Scope of information covered by this section*. The provisions of this section apply to all customer information in the possession of a covered institution, and all consumer information that a covered institution maintains or otherwise possesses for a business purpose, as applicable, regardless of whether such information pertains to individuals with whom the covered institution has a customer relationship, or pertains to the customers of other financial institutions and has been provided to the covered institution.

(b) *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 (b)(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;

(ii) Take appropriate steps to contain and control 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 (b)(4) of this section 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, 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.

(4) *Notifying affected individuals of unauthorized access or use*. (i) *Notification obligation*. 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 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 to each affected individual whose sensitive 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.

(iii) *Timing*. 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 unless the Attorney General of the United States informs the covered institution, in writing, that the notice required under this rule poses a substantial risk to national security, in which case the covered institution may delay such a notice for a time period specified by the Attorney General of the United States, but not for longer than 15 days. The notice may be delayed for an additional period of up to 15 days if the Attorney General of the United States determines that the notice continues to pose a substantial risk to national security.

(iv) *Notice contents*. The 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) Describe what has been done to protect the sensitive customer information from further unauthorized access or use;

(C) 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;

(D) 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;

(E) 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;

(F) 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;

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

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

(I) 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 (b)(3) of this section must include written policies and procedures requiring the institution, pursuant to a written contract between the covered institution and its service providers, to require the service providers to take appropriate measures that are designed to protect against unauthorized access to or use of customer information, including notification to the covered institution as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security resulting in unauthorized access to a customer information system maintained by the service provider to enable the covered institution to implement its response program.

(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 its behalf in accordance with paragraph (b)(4) of this section.

(c) *Disposal of consumer information and customer information*. (1) *Standard*. Every covered institution, other than notice-registered broker-dealers, that maintains or otherwise possesses customer information or consumer information for a business purpose must properly dispose of the 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 (c)(1) of this section.

(3) *Relation to other laws*. Nothing in this paragraph (c) 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.

(d) *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 written records documenting its compliance with the requirements of paragraphs (b) and (c)(2) of this section.

(2) In the case of covered institutions described in paragraph (d)(1) of this section, the records required under paragraphs (b) and (c)(2) of this section, apart from any policies and procedures thereunder, 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 (b) and (c)(2) of this section, covered institutions described in paragraph (d)(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.

(e) *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. Consumer information also means a compilation of such records. 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, *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* 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 handled or maintained by the covered institution or on its behalf.

(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 handled or maintained by the transfer agent or on its behalf.

(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.

(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 (e)(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 is a third party and receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution.

(11) *Substantial harm or inconvenience* means personal injury, or financial loss, expenditure of effort or loss of time that is more than trivial, including 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.

(12) *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

9. The authority citation for part 270 continues to read, in part, as follows:

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

* * * * *

10. 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) Any written records documenting compliance with the requirements set forth in 248.30(b) and (c)(2).

* * * * *

11. Amend § 270.31a-2 by:

a. In paragraph (a)(7), removing the period at the end of 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

12. The authority citation for part 275 continues to read, in part, 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, and 80b-11, unless otherwise noted.

* * * * *

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

* * * * *

13. Amend § 275.204-2 by adding paragraph (a)(20) to read as follows:

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

* * * * *

(a) * * *

(20) A copy of the written records documenting compliance with the requirements set forth in §248.30(b) and (c)(2).

* * * * *

By the Commission.

Dated: March 15, 2023.

Vanessa A. Countryman,
Secretary.

[FR Doc. 2023-05774 Filed: 4/5/2023 8:45 am; Publication Date: 4/6/2023]