SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 240, 248, 270, and 275

[Release Nos. 34-100155; IA-6604; IC-35193; 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: Final rule.

SUMMARY: The Securities and Exchange Commission ("Commission" or "SEC") is adopting rule amendments that will require brokers and dealers (or "broker-dealers"), investment companies, investment advisers registered with the Commission ("registered investment advisers"), funding portals, and transfer agents registered with the Commission or another appropriate regulatory agency ("ARA") as defined in the Securities Exchange Act of 1934 ("transfer agents") to adopt written policies and procedures for incident response programs to address unauthorized access to or use of customer information, including procedures for providing timely notification to individuals affected by an incident involving sensitive customer information with details about the incident and information designed to help affected individuals respond appropriately. In addition, the amendments extend the application of requirements to safeguard customer records and information to transfer agents; broaden the scope of information covered by the requirements for safeguarding customer records and information and for properly disposing of consumer report information; impose requirements to maintain written records documenting compliance with the amended rules; and conform annual privacy notice delivery

provisions to the terms of an exception provided by a statutory amendment to the Gramm-Leach-Bliley Act ("GLBA").

DATES: *Effective date*: This rule is effective [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

Compliance date: The applicable compliance dates are discussed in section II.F of this rule.

FOR FURTHER INFORMATION CONTACT: Emily Hellman, 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; Kevin Schopp, Senior Special Counsel; Moshe Rothman, Assistant Director; Office of Clearance and Settlement, Division of Trading and Markets, (202) 551-5550, Susan Ali and Andrew Deglin, Counsels; Michael Khalil and Y. Rachel Kuo, Senior Counsels; Blair Burnett and Bradley Gude, Branch Chiefs; or Brian McLaughlin Johnson, Assistant Director, Investment Company Regulation Office, Division of Investment Management, (202) 551-6792, Securities and Exchange Commission, 100 F Street NE, Washington, DC, 20549.

SUPPLEMENTARY INFORMATION: The Commission is adopting amendments to 17 CFR 248.1 through 248.100 ("Regulation S-P") under Title V of the GLBA [15 U.S.C. 6801 through 6827], the Fair Credit Reporting Act ("FCRA") [15 U.S.C. 1681 through 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*.].

TABLE OF CONTENTS

I. INTRODUCTION AND BACKGROUND 5
II. DISCUSSION 15
A. Incident Response Program Including Customer Notification 16
1. Assessment 21
2. Containment and Control 22
3. Notice to Affected Individuals 23
4. Service Providers 69
B. Scope of Safeguards Rule and Disposal Rule 92
1. Scope of Information Protected 92
2. Extending the Scope of the Safeguards Rule and the Disposal Rule to Cover All Transfer Agents 100
3. Maintaining the Current Regulatory Framework for Notice-Registered Broker-Dealers 119
C. Recordkeeping 121
D. Exception from Requirement to Deliver Annual Privacy Notice 126
E. Existing Staff No-Action Letters and Other Staff Statements 128
F. Compliance Period 129
III. OTHER MATTERS 132
IV. ECONOMIC ANALYSIS 133
A. Introduction 133
B. Broad Economic Considerations 140
C. Baseline 150
1. Safeguarding Customer Information: Risks and Practices 155
2. Regulations and Guidelines 160
3. Market Structure 185
D. Benefits and Costs of the Final Rule Amendments 199
1. Written Policies and Procedures 203
2. Extending the Scope of the Safeguards Rule and the Disposal Rule 268
3. Recordkeeping 282
4. Exception from Annual Notice Delivery Requirement 284
E. Effects on Efficiency, Competition, and Capital Formation 285
F. Reasonable Alternatives Considered 296
1. Reasonable Assurances from Service Providers 296
2. Lower Threshold for Customer Notice 299
3. Encryption Safe Harbor 300
4. Longer Customer Notification Deadlines 302
5. Broader National Security and Public Safety Delay in Customer Notification 303
V. PAPERWORK REDUCTION ACT 305
A. Introduction 305
B. Amendments to the Safeguards Rule and Disposal Rule 308
VI. FINAL REGULATORY FLEXIBILITY ACT ANALYSIS 314

A. Need for, and Objectives of, the Final Amendments 314
B. Significant Issues Raised by Public Comments 315
C. Small Entities Subject to Final Amendments 319
D. Projected Reporting, Recordkeeping, and Other Compliance Requirements 321
E. Agency Action to Minimize Effect on Small Entities 326
STATUTORY AUTHORITY 328

I. INTRODUCTION AND BACKGROUND

Regulation S-P is a set of privacy rules adopted pursuant to the GLBA and the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") that govern the treatment of nonpublic personal information about consumers by certain financial institutions.[1] The Commission is adopting rule amendments that are designed to modernize and enhance the protections that Regulation S-P provides by addressing the expanded use of technology and corresponding risks that have emerged since the Commission originally adopted Regulation S-P in 2000. The amendments in particular update the requirements of the "safeguards" and "disposal" rules. The safeguards rule requires brokers, dealers, investment companies,[2] and registered investment advisers to adopt written policies and procedures that address administrative, technical, and physical safeguards to protect customer records and information.[3] The disposal rule, which applies to transfer agents registered with the Commission in addition to the institutions covered by the safeguards rule, requires proper disposal of consumer report information.[4] In addition, under Regulation Crowdfunding, funding portals must comply with the requirements of Regulation S-P as they apply to brokers.[5] Thus, funding portals will also be required to comply with the applicable amendments to Regulation S-P adopted in this release.

---

1 *See* 17 CFR 248.1.

2 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 – are not subject to Regulation S-P.

3 17 CFR 248.30(a). References in this release to "rule 248.30" are to 17 CFR 248.30.

4 Rule 248.30(b).

5 *See* 17 CFR 227.403(b). Accordingly, unless otherwise stated (for example, *see infra* sections IV and V), references in this release to "brokers" or "broker-dealers" include funding portals.

The final Regulation S-P amendments are needed to provide enhanced protection of customer or consumer information and help ensure that customers of covered institutions receive timely and consistent notifications in the event of unauthorized access to or use of their information.[6] In evaluating amendments to Regulation S-P, we have considered developments in how firms obtain, share, and maintain individuals' personal information since the Commission originally adopted Regulation S-P, which correspond with an increasing risk of harm to individuals.[7] This environment of expanded risks and the importance of reducing or mitigating the potential for harm also supports our amendments to Regulation S-P.

In March 2023, the Commission proposed amendments to Regulation S-P.[8] In particular, the proposed amendments would amend the safeguards rule to require any broker or dealer, investment company, registered investment adviser, or transfer agent (collectively, "covered

---

6 *See* Proposing Release at section II.A.4.

7 *See*, *e.g.*, Federal Bureau of Investigation, 2022 Internet Crime Report (Mar. 27, 2023), at 7-8, *available at*: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (stating that the FBI's Internet Crime Complaint Center received 800,944 complaints in 2022 (an increase from 351,937 complaints in 2018). The complaints included 58,859 related to personal data breaches (an increase from 50,642 breaches in 2018)); the Financial Industry Regulatory Authority ("FINRA"), *2022 Report on FINRA's Examination and Risk Monitoring Program: Cybersecurity and Technology Governance* (Feb. 2022), *available at:* https://www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program (noting increased number and sophistication of cybersecurity attacks and reminding firms of their obligations to oversee, monitor, and supervise cybersecurity programs and controls of third-party vendors); 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* Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, Securities Exchange Act Release No. 97141 (Mar. 15, 2023) [88 FR 20616 (Apr. 6, 2023)] ("Proposing Release" or "proposal"). The Commission voted to issue the Proposing Release on Mar. 15, 2023. The release was posted on the Commission website that day, and comment letters were received beginning the same day. The comment period closed on June 5, 2023. We have considered all comments received since Mar. 15, 2023.

institutions") to develop, implement, and maintain written policies and procedures for an incident response program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. The proposal included a further requirement that, as part of this incident response program, covered institutions would provide notices to individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization as soon as practicable, but not later than 30 days, after becoming aware that the incident occurred or is reasonably likely to have occurred. The proposed notice requirement included provisions that addressed the use of service providers by covered institutions and included a provision that would permit covered institutions to delay providing notice after receiving a written request from the United States Attorney General ("Attorney General") that this notice poses a substantial risk to national security.

The Commission also proposed other amendments to Regulation S-P to enhance the protection of customers' nonpublic personal information. The proposed amendments included provisions to expand the scope of the protections of the safeguards and disposal rules, including extending the safeguards rule to transfer agents. The proposed amendments also included requirements for covered institutions to maintain written records documenting compliance with the proposed amended rules. Finally, the Commission proposed amendments to conform annual privacy notice delivery provisions to the terms of an exception provided by a statutory amendment to the GLBA.

The Commission received comment letters on the proposal from a variety of commenters, including financial services firms and their service providers, law firms, investor advocacy groups, professional and trade associations, public policy research institutes, academics, and

interested individuals.[9] Most individual and public interest group commenters and some industry groups generally supported the proposed amendments.[10] A few commenters urged the Commission to consider taking additional steps to strengthen the proposed requirements, for example, by shortening the period for customer notification.[11] Many industry commenters expressed concern with specific elements of the proposed amendments, however, suggesting that these amendments would pose operational difficulties.[12]

Comments on specific aspects of the proposed amendments focused on a few key themes. First, commenters urged the Commission to take a more holistic regulatory approach to harmonize the proposed amendments with other Commission rules and proposals to avoid

---

9 The comment letters on the proposal are available at https://www.sec.gov/comments/s7-05-23/s70523.htm.

10 *See, e.g.,* Comment Letter of the Investment Adviser Association (June 5, 2023) ("IAA Comment Letter 1"); Comment Letter of the Investment Company Institute (May 23, 2023) ("ICI Comment Letter 1"); Comment Letter of Better Markets (June 5, 2023) ("Better Markets Comment Letter"); Comment Letter of North American Securities Administrators Association (May 22, 2023) ("NASAA Comment Letter"). Some commenters suggested more tailored requirements for smaller covered institutions. *See, e.g.*, IAA Comment Letter 1; Comment Letter of the Securities Transfer Association (June 2, 2023) ("STA Comment Letter 2"); Comment Letter of the Committee of Annuity Insurers (June 5, 2023) ("CAI Comment Letter"). As discussed in more detail below, the final amendments apply to all covered institutions because entities of all sizes are vulnerable to the types of data security breach incidents we are trying to address. *See infra* section VI.

11 *See, e.g.,* Better Markets Comment Letter.

12 *See, e.g.,* Comment Letter of the Securities Industry and Financial Markets Association, et al. (June 5, 2023) ("SIFMA Comment Letter 2"); Comment Letter of the Financial Services Institute (May 22, 2023) ("FSI Comment Letter"); Comment Letter of Federated Hermes, Inc. (June 6, 2023) ("Federated Comment Letter").

creating redundant, overlapping, or conflicting obligations for covered institutions.[13] We have modified the rule from the proposal to address comments.[14]

For example, covered institutions may be required to adopt written policies and procedures on similar issues under other provisions of the Federal securities laws.[15] A covered institution can, however, adopt a single set of policies and procedures covering Regulation S-P and other rules, provided that the policies and procedures meet the requirements of each rule.[16] Additionally, we have changed the proposed requirement to delay providing customer notices

---

13 *See, e.g.,* IAA Comment Letter 1; ICI Comment Letter 1; Comment Letter of Nasdaq Stock Market LLC (June 2, 2023) ("Nasdaq Comment Letter"). Commenters also raised these concerns about other proposed rulemakings that the Commission has not adopted. *See*, *e.g.*, Comment Letter of the Investment Adviser Association (June 17, 2023) ("IAA Comment Letter 2"); ICI Comment Letter 1. Other commenters requested more specific guidance regarding how the various policies and procedure requirements in other Commission proposals would interact with each other. *See, e.g.*, CAI Comment Letter; SIFMA Comment Letter 2; IAA Comment Letter 2. To the extent that those proposals are adopted, the baseline in those subsequent rulemakings will reflect the existing regulatory requirements at that time.

14 Since the publication of the proposing release, the Commission adopted new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934 ("Public Company Cybersecurity Rules"). *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Securities Act Release No. 11216 (July 26, 2023) [88 FR 51896 (Aug. 4, 2023)].

15 *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); and 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).

16 Two commenters addressed the proposal's application to dually-registered investment advisers and broker-dealers or firms operating both business models (collectively, "dual registrants"). One of these commenters stated that the proposed amendments to Regulation S-P allow for streamlining of process because they would apply uniformly to broker-dealers and investment advisers. FSI Comment Letter. The other commenter addressed collectively other Commission cyber proposals and the proposed amendments to Regulation S-P. The commenter stated that these proposals collectively would involve significant burden for a dual registrant to bring both broker-dealer and investment adviser entities into compliance, urging the Commission to provide an extended compliance period for all of the proposed rules to provide time for dual registrants to come into compliance and "identify some synergies that might make compliance more effective and economical." Cambridge Comment Letter. As one of these commenters stated, Regulation S-P's requirements apply uniformly to broker-dealers and advisers, although each covered institution—including a dual registrant—will have to tailor its policies and procedures to its business.

when that notice poses a substantial risk to national security or public safety in order to align with a similar provision contained in the Public Company Cybersecurity Rules.[17]

Commenters also questioned the need for the proposed amendments in light of existing state laws that also address data breaches and raised concerns about differences between the proposed amendments and state regulatory requirements. One commenter stated that the proposed amendments were not needed because existing state laws already require firms to provide notice to individuals in the event of a data breach.[18] Some commenters stated that parts of the proposed amendments would conflict with certain provisions of state laws,[19] while other commenters stated that parts of the proposed amendments would duplicate existing state laws.[20]

As discussed more fully later in this section, while we recognize that existing state laws require covered institutions to notify state residents of data breaches in some cases, state laws are not consistent on this point and exclude some entities from certain requirements.[21] The final amendments will require notification to all customers of a covered institution affected by a data breach (regardless of state residency), in order to provide timely and consistent disclosure of important information to help affected customers respond to a data breach.[22] To that end, the final amendments will enhance investor protection in a number of ways, including by covering a

---

17 *See infra* section II.A.3.d(2).

18 *See* CAI Comment Letter.

19 *See*, *e.g.*, IAA Comment Letter 1; Letter from Computershare (June 5, 2023) ("Computershare Comment Letter"); SIFMA Comment Letter 2.

20 *See, e.g.,* CAI Comment Letter.

21 *See infra* section IV.C.2.

22 With respect to the interaction of the final rule with state law, Section 15(i)(1) of the Exchange Act (15 U.S.C. 78o(i)(1)) provides that no law, rule, regulation, or order, or other administrative action of any state or political subdivision thereof shall establish capital, custody, margin, financial responsibility, making and keeping records, bonding, or financial or operational reporting requirements for brokers, dealers, municipal securities dealers, government securities brokers, or government securities dealers that differ from, or are in addition to, the requirements in those areas established under the Exchange Act.

broader scope of customer information than many states;[23] providing for a 30-day notification deadline that is shorter than the timing currently mandated by many states (including states that have no deadline or those allowing for various notification delays);[24] and providing for a more robust notification trigger than in many states.[25]

Commenters also raised concerns with differences between the proposed amendments and other Federal regulators' safeguarding standards that also include a requirement for a data breach response plan or program.[26] 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, the Consumer Financial Protection Bureau ("CFPB"), and the FTC.[27] Accordingly, the Commission has also been mindful of the need to set standards for safeguarding customer records and information that are consistent and comparable with the corresponding standards set

---

23 *See infra* section IV.D.1.b(3).

24 *See infra* section IV.D.1.b(2).

25 *See infra* section IV.D.1.b(4).

26 The Federal Trade Commission ("FTC") in 2021 amended its Safeguards Rule (16 CFR part 314 ("FTC 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). 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 id.* at n.295. 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. In 2005, 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 (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 information has occurred or is reasonably possible, it should notify affected customers as soon as possible.

27 *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).

by these agencies in developing the amendments.[28] To this end, we have modified the final amendments from the proposal to promote greater consistency with other applicable Federal safeguard standards to the extent they do not affect the investor protection purposes of this rulemaking, as discussed in more detail below. For example, the final amendments require covered institutions to ensure that their service providers provide notification as soon as possible, but no later than 72 hours after becoming aware that an applicable breach has occurred, which is informed by the 72-hour deadline that is required under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA").[29]

We recognize, however, that there are some areas of divergence between the final amendments and other Federal regulators' GLBA safeguarding standards, and we discuss the basis for each provision of the final rules below, including cases where the amendments differ from analogous requirements under state law or other federal regulations.[30]

Many commenters also urged the Commission to coordinate with other Federal agencies, particularly on reporting deadlines.[31] For example, a number of commenters suggested that the Commission coordinate with CISA as it develops regulations pursuant to CIRCIA.[32] We have

---

28 *See* Proposing Release at the text following n.37.

29 *See* final rule 248.30(a)(5)(i); *see also infra* footnote 245 and accompanying text (discussing how a 72-hour reporting deadline would align with other regulatory standards). Under CIRCIA, the 72-hour reporting deadline is for entities to report cyber incidents to the Cybersecurity and Infrastructure Security Agency ("CISA").

30 Among the changes being adopted, we are revising as proposed the requirements of 17 CFR 248.17 ("rule 248.17") to refer to determinations made by the CFPB rather than the FTC, 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). Upon its adoption, rule 248.17 essentially restated the then-current text of section 507 of the GLBA, and as such, referenced determinations made by the FTC. *See* Privacy of Consumer Financial Information (Regulation S-P), Exchange Act Release No. 42974 (June 22, 2000) [65 FR 40334 (June 29, 2000)].

31 *See*, *e.g.*, Comment Letter of Amazon Web Services (June 5, 2023) ("AWS Comment Letter"); Comment Letter of Google Cloud (June 5, 2023) ("Google Comment Letter"); and Nasdaq Comment Letter.

32 *See*, *e.g.*, SIFMA Comment Letter 2; Cambridge Comment Letter; Google Comment Letter. CISA has

consulted and coordinated with CISA and, consistent with the requirements of the GLBA and other statutory requirements,[33] other relevant agencies and their representatives for the purpose of ensuring, to the extent possible, that the amendments are consistent and comparable with the regulations prescribed by other relevant agencies.[34]

We are adopting amendments to Regulation S-P substantially as proposed, with some changes in response to comments. The principal elements of the final amendments, as discussed in more detail below, are as follows:

- *Incident Response Program.* The final safeguards rule requires 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. The final amendments will require that a response program include procedures to assess the nature and scope of any incident and to take appropriate steps to contain and control the incident to prevent further unauthorized access or use.
- *Notification Requirement.* The response program procedures in the final amendments also includes a requirement that covered institutions provide a notification to individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. Notice

provided a notice of proposed rulemaking that would implement the CIRCIA requirements but they have not yet been adopted. *See also* Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 FR 23644 (Apr. 4, 2024).

33 *See* Exchange Act Section 17A(d)(3)(A), 15 U.S.C 78q-1(d)(3)(A) (providing that "[w]ith respect to any clearing agency or transfer agent for which the Commission is not the appropriate regulatory agency, the Commission and the appropriate regulatory agency for such clearing agency or transfer agent shall consult and cooperate with each other...").

34 *See* 15 U.S.C. 6804(a)(2). The relevant agencies include the OCC, FRB, FDIC, CFPB, FTC, CISA, Commodity Futures Trading Commission ("CFTC"), Department of Justice ("DOJ"), and the National Association of Insurance Commissioners.

will not be required if a covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, that the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. Under the final amendments, a customer notice must be clear and conspicuous and provided by a means designed to ensure that each affected individual can reasonably be expected to receive it. This notice must be provided as soon as reasonably practicable, but not later than 30 days, after the covered institution becomes aware that unauthorized access to or use of customer information has, or is reasonably likely to have, occurred. As discussed in more detail below, the final amendments will permit covered institutions to delay providing notice after the Commission receives a written request from the Attorney General that this notice poses a substantial risk to national security or public safety.[35]

- *Service Providers.* The final amendments to the safeguards rule include new provisions that address the use of service providers by covered institutions. Under these provisions, covered institutions will be required to establish, maintain, and enforce written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring of service providers, including to ensure that affected individuals receive any required notices. The final amendments make clear that while covered institutions may use service providers to provide any required notice, covered institutions will retain the obligation to

[35] *See infra* section II.A.3.d(2).

ensure that affected individuals are notified in accordance with the notice requirements.

- *Scope.* The final amendments will 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. The final amendments will also broaden the group of customers whose information is protected under both rules. Also, transfer agents will be required to comply with the safeguards rule.
- *Recordkeeping and Annual Notice Amendments.* The final amendments will add requirements for covered institutions, other than funding portals,[36] to make and maintain written records documenting compliance with the requirements of the safeguards rule and the disposal rule. Further, the final amendments amend the existing requirement to provide annual privacy notices to codify a statutory exception.

II. DISCUSSION

Since Regulation S-P was first adopted in 2000, 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 increases the risk of customers' information being accessed or used without authorization, for example in a cyberattack or if customer information is improperly disposed of or stolen. In particular, as a frequently-targeted industry, the financial sector has observed increased exposure to cyberattacks that threaten not only the financial firms themselves, but also their customers, especially considering that customer records

[36] As discussed below, funding portals are already subject to recordkeeping requirements with regard to documenting their compliance with Regulation S-P, which are not being amended by these final amendments. *See infra* footnote 385 and accompanying discussion.

and other information that covered institutions possess can be particularly sensitive.[37] The final amendments will modernize and enhance the protections that Regulation S-P already provides to address this changed landscape.

A. Incident Response Program Including Customer Notification

As set forth in the proposal, security incidents may result in, among other things, misuse, exposure or theft of a customer's nonpublic personal information, and potentially leave affected individuals vulnerable to having their information further compromised. Threat actors can use customer information to cause harm in a number of ways, such as by stealing customer identities to sell to other threat actors on the dark web, 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.

To help protect against harms that may result from a security incident involving customer information, the Commission proposed and is adopting amendments to the safeguards rule largely as proposed, with certain modifications to the notification requirement as discussed further below.[38] The amendments will require that covered institutions' safeguards policies and procedures include an incident response program for unauthorized access to or use of customer information, including customer notification procedures.[39] The amendments will require the incident 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

---

37 *See infra* section IV.C.1.

38 *See infra* section II.A.3.

39 *See* final rule 248.30(a)(3). For clarity, when the amendments to the safeguards rule refer to "unauthorized access to or use", the word "unauthorized" modifies both "access" and "use."

release, an "incident").[40] Any instance of unauthorized access to or use of customer information will trigger a covered institution's incident response program. The amendments will also require that the response program include procedures for notifying affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.[41]

In this regard, requiring covered institutions to have incident response programs will help mitigate the risk of harm to affected individuals stemming from incidents where a customer's information has been accessed or used without authorization. For example, incident response programs will help covered institutions to be better prepared to respond to such incidents, and providing notice to affected individuals will 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 incident 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. Requiring the incident 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.

As proposed, the amendments will require that a covered institution's incident response program include policies and procedures containing certain general elements but will not

---

40 *See* final rule 248.30(a)(3). *See also infra* section II.B.1 for a discussion of "customer information."

41 *See* final rule 248.30(d)(9) for the definition of "sensitive customer information." *See also infra* section II.A.3.b, which includes a discussion of "sensitive customer information." Notice must 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 occurred at the covered institution or one of its service providers that is not itself a covered institution, that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.

prescribe specific steps a covered institution must undertake when carrying out incident response activities, thereby enabling covered institutions to create policies and procedures best suited to their particular circumstances. Specifically, a covered institution's incident response program will 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;[42]

(ii) Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information;[43] 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,[44] 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.[45]

---

42 *See* final rule 248.30(a)(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* final rule 248.30(d)(6).

43 *See* final rule 248.30(a)(3)(ii).

44 *See* i*nfra* section II.A.3.

45 *See* final rule 248.30(a)(3)(iii).

The Commission received multiple comments regarding the proposed requirement for an incident response program generally.[46] One commenter supported requiring the incident response program and appreciated its similarity to the Banking Agencies' Incident Response Guidance.[47] Another commenter stated that there should not be a one-size-fits-all approach to incident response programs, stating that an adviser should have discretion to determine how the incident response program should be implemented, and requested that any final rule make clear that specific steps for incident response are not required.[48] Moreover, this commenter requested that the final rule expressly indicate that in developing their programs, advisers should employ a principles- and risk-based approach.[49] This commenter also opposed the addition of any requirement in the policies and procedures for an adviser to designate an employee with specific qualifications and experience (or hire a similarly qualified third party) to coordinate its incident response program.[50]

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

---

46 Comments for specific components of the incident response program are discussed in more depth separately. *See infra* sections II.A.1-4.

47 *See* ICI Comment Letter 1; *see also supra* footnote 26 (discussing the Banking Agencies' Incident Response Guidance).

48 *See* IAA Comment Letter 1.

49 *See id.; see also* CAI Comment Letter stating that policies and procedures should be based on the specific risks of the particular covered institution and commensurate with the size and complexity of the covered institution's activities.

50 *See id.*

will require that a covered institution's incident response program include policies and procedures containing certain general elements, so covered institutions may tailor their policies and procedures to their individual facts and circumstances. Additionally, advisers, like other covered institutions, can continue to use a risk-based approach to tailor their assessment and containment policies and procedures if they choose to do so, as long as the required elements of the incident response program are met.

Two commenters opposed the scope of the proposed incident response program.[51] Specifically, these commenters stated that, consistent with the notification requirements, the assessment and containment and control components of the incident response program should be limited to sensitive customer information (and not encompass all nonpublic customer information).[52] According to one commenter, because sensitive customer information is the information likely to cause substantial harm or inconvenience to a customer and that requires notification to customers, it follows that incident response programs should be tailored to sensitive customer information.[53] The other commenter stated that clients would view the protection of their sensitive customer information as a critically important aspect of their relationship with their adviser and that an adviser's efforts and resources should appropriately be focused on this information.[54]

We are adopting as proposed final rules which require the incident response program's assessment and containment and control components to cover a broader scope of information than the notification requirements. The scope of information covered by the assessment and

---

51 *See* Comment Letter of Schulte Roth & Zabel LLP (June 5, 2023) ("Schulte Comment Letter") and IAA Comment Letter 1.

52 *See* Schulte Comment Letter; IAA Comment Letter 1.

53 *See* Schulte Comment Letter.

54 *See* IAA Comment Letter 1.

containment and control requirements is designed to help ensure all information covered by the requirements of the GLBA[55] are appropriately safeguarded and that sufficient information is assessed to fulfill the more narrowly tailored obligation to notify affected individuals. For example, assessment of any incident involving unauthorized access to or use of customer information will help facilitate the evaluation of whether sensitive customer information has been accessed or used without authorization, which informs whether notice has to be provided. Additionally, 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. Therefore, the scope of the incident response program is appropriate, and we are adopting as proposed.

1. Assessment

The final amendments will 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.[56] We did not receive comments addressing the assessment portion of the incident response program and are adopting it as proposed.[57]

---

55 The GLBA directs the Commission to establish standards to insure the security and confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of records or information which could result in substantial harm or inconvenience to any customer. 15 U.S.C. 6801(b).

56 *See* final rule 248.30(a)(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.

57 Although no comments discussed only the assessment requirement, multiple comments discussed the incident response program generally, which includes the assessment requirement. These comments are discussed in section II.A.

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.[58] Information developed during the assessment process may also help covered institutions develop a contextual understanding of the circumstances surrounding an incident, as well as enhance their technical understanding of the incident, which should be helpful in guiding incident response activities such as containment and control measures. The assessment process may also be helpful for identifying and evaluating existing vulnerabilities that could benefit from remediation in order to prevent such vulnerabilities from being exploited in the future. Further, covered institutions generally should consider reviewing and updating the assessment procedures periodically to ensure that the procedures remain reasonably designed.[59]

2. Containment and Control

The final amendments will require that the response program have procedures for taking appropriate steps to contain and control a security incident, in order to prevent further unauthorized access to or use of customer information.[60] We did not receive comments discussing the containment and control portion of the incident response program and are adopting as proposed.[61]

---

58 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.

59 *See also* 17 CFR 270.38a-1, 275.206(4)-7.

60 *See* final rule 248.30(a)(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 at 15752.

61 Although no comments discussed only the containment and control requirements, multiple comments

As set forth in the proposal, the objective of containment and control is to prevent additional damage from unauthorized activity and to reduce the immediate impact of an incident by removing the source of the unauthorized activity.[62] Strategies for containing and controlling an incident vary depending upon the type of incident and may include, for example, isolating compromised systems or enhancing the monitoring of intruder activities, searching for additional compromised systems, changing system administrator passwords, rotating private keys, and changing or disabling default user accounts and passwords, among other interventions. Because incident response may involve making complex judgment calls, such as deciding when to shut down or disconnect a system, developing and implementing written containment and control policies and procedures will provide a framework to help facilitate improved decision making at covered institutions during potentially high-pressure incident response situations. Further, covered institutions generally should consider reviewing and updating the containment and control procedures periodically to ensure that the procedures remain reasonably designed.[63]

3. Notice to Affected Individuals

As part of their incident response programs, covered institutions will be required under the final amendments to provide a clear and conspicuous notice to affected individuals under certain circumstances.[64] We are adopting this requirement substantially as proposed, with some changes in response to comments.

---

discussed the incident response program generally, which includes the containment and control requirement. These comments are discussed in section II.A.

[62] *See* Proposing Release at Section II.A.2. For a further discussion of the purposes and practices of such containment measures, *see generally* CISA Incident Response Playbook, 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.

[63] *See also* 17 CFR 270.38a-1, 275.206(4)-7.

[64] *See* final rule 248.30(a)(4).

We are adopting as proposed, a requirement for a covered institution to 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 will be required to 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. Also as proposed, the final amendments require the notice to 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. Lastly, in a modification from the proposal, the final amendments provide for an incrementally longer period of time than the proposal for a covered institution to delay providing notice to affected individuals in cases where the Attorney General has determined that providing the notice would pose a substantial risk to national security or public safety. These requirements are discussed in detail below.

a. Standard for Providing Notice and Identification of Affected Individuals

We are adopting as proposed a 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, unless, 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.[65] The final amendments reflect a presumption of notification: a covered institution must provide a notice unless it determines notification is not required following a reasonable investigation. Also as proposed, if an incident of unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred, but a covered institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization, the final amendments require the covered institution to 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 without authorization ("affected individuals").[66]

While the incident response program is generally required to address information security incidents involving any form of customer information,[67] notification is only required when there has been unauthorized access to or use of sensitive customer information, a subset of customer information, because it presents increased risks to affected individuals.[68] This notice standard is designed to give affected individuals an opportunity to mitigate the risk of substantial harm or inconvenience arising from an information security incident that potentially implicates their sensitive customer information by affording them an opportunity to take timely responsive

---

65 Final rule 248.30(a)(4)(i).

66 Final rule 248.30(a)(4)(ii). This proposed provision was not intended to require notification of customers whose sensitive customer information resided in the affected customer information system if the covered institution has reasonably determined that such customers' sensitive customer information was not accessed or used without authorization. Accordingly, we have modified the final rule to reflect this intended result. *See infra* footnote 102 and accompanying text.

67 *See infra* section II.B.1.

68 *See infra* section II.A.3.b. Additionally, customer information that is not disposed of properly could trigger the requirement to notify affected individuals under final rule 248.30(a)(4)(i). For example, a covered institution whose employee leaves un-shredded customer files containing sensitive customer information in a dumpster accessible to the public would be required to notify affected customers, unless the institution has determined that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.

actions, such as monitoring credit reports for unauthorized activity, placing fraud alerts on relevant accounts, or changing passwords used to access accounts. At the same time, the final amendments provide a mechanism for covered institutions to avoid making unnecessary notifications in cases where, following a reasonable investigation, the institution determines that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience to the affected individual.[69]

Whether an investigation is reasonable will depend on the particular facts and circumstances of the unauthorized access or use. For example, unauthorized access or use that is the result of intentional intrusion by a threat actor may warrant more extensive investigation than inadvertent unauthorized access or use by an employee. The investigation may occur in parallel with an initial assessment and scoping of the incident and may build upon information generated from those activities. The scope of the investigation generally should be refined by using 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 use of sensitive customer information 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.[70]

A covered institution cannot avoid its notification obligations in cases where an investigation's results are inconclusive. Instead, the notification requirement is excused only where a reasonable investigation supports a determination that sensitive customer information

---

69 *See infra* section II.A.3.c.

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

has not been and is not reasonably likely to be used in a manner that would result in substantial harm or inconvenience. Thus, in a case where a threat actor has gained access to a customer information system that stores sensitive customer information, and the covered institution lacks information indicating that any particular individual's sensitive customer information 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 will be required to provide notice to affected individuals even though it may not have a sufficient basis to determine whether the breach would result in substantial harm or inconvenience.[71] Pursuant to the amendments, as proposed and adopted, for any determination that a covered institution makes that notice is not required, covered institutions other than funding portals will be required to maintain a record of the investigation and basis for its determination.[72]

As further described below,[73] a number of commenters supported the proposal's requirement for covered institutions to provide notices promptly, emphasizing the importance of ensuring that customers receive timely notification when their sensitive customer information is reasonably likely to have been subject to unauthorized access or use so they have an opportunity to effectively respond to the incident.[74] One commenter stated that timeliness is key because any delay will impact consumers' ability to take steps to protect themselves from identify theft, account compromise, and other downstream impacts resulting from the initial harm of the unauthorized access or use.[75] According to this commenter, a breach notification regime is

---

71 *See* final rule 248.30(a)(4)(ii).

72 *See infra* section II.C; *see also infra* footnote 385.

73 *See infra* section II.A.3.d.

74 *See*, *e.g.*, Better Markets Comment Letter; EPIC Comment Letter; NASAA Comment Letter; ICI Comment Letter 1; Nasdaq Comment Letter.

75 *See* EPIC Comment Letter; *see also* Better Markets Comment Letter (customers whose information has

fundamentally deficient if it does not empower consumers with the information and tools necessary to take action to protect themselves or understand what risks they may face as a result of a breach.[76]

Several commenters proposed alternative notification standards, some expanding the circumstances requiring customer notification, and others suggesting a narrower notification regime.[77] One commenter suggested we require notification for any incident of unauthorized access to or use of sensitive information, regardless of the risk of harm or inconvenience.[78] According to this commenter, customers should always be notified when their sensitive information is accessed or used without authorization, which would allow customers to determine for themselves whether they believe there is a risk of substantial harm or inconvenience that should prompt action on their part. Similarly, another commenter suggested that the notification standard should be expanded from a "reasonably likelihood" standard to a "reasonably possible" standard with regard to whether an individual's sensitive customer information was accessed or used without authorization.[79] This commenter stated that this change was necessary to protect against the possibility that a covered institution might conclude it lacked sufficient information to find the reasonably likely standard satisfied if, for example, it knows it has been hacked but is unable to determine the scope of the hack. According to these commenters, the seemingly higher threshold proposed by the Commission, coupled with their

---

been exposed need appropriate and timely notifications to decide for themselves whether and how to address the breach to avoid being "victimized twice": first when the breach occurs, and then again when "bad actors use the information to steal their identity, drain their bank accounts, or run up their credit cards").

76 *See* EPIC Comment Letter.

77 *See*, *e.g.*, Better Markets Comment Letter, NASAA Comment Letter (proposing more expansive standards); SIFMA Comment Letter 2, CAI Comment Letter, IAA Comment Letter 1 (proposing narrower standards).

78 *See* Better Markets Comment Letter.

79 *See* NASAA Comment Letter.

belief that businesses want to avoid making disclosures that could incur liability or lose customers, leaves open the potential that customers will not be notified of some information security compromises that could threaten their investments.[80] One commenter suggested that, in addition to requiring notifications to affected individuals, the rules should be modified to also require that covered institutions provide notice to the Commission whenever they are providing notice to affected individuals.[81]

By contrast, with regard to narrowing the standard, some commenters suggested eliminating the presumption of notification altogether, such that covered institutions would have a notification obligation only after having affirmatively determined, following an investigation, a likelihood of a breach or resulting harm to customers.[82] These commenters suggested that eliminating the notification presumption, and allowing for the completion of an investigation, would provide covered institutions with additional time to respond to and mitigate an incident as opposed to spending time deliberating over notification obligations, and would allow for more informed notifications. These commenters also suggested that this approach would be more consistent with certain state law regimes that only require notification where an investigation shows a risk of harm and the Banking Agencies' Incident Response Guidance.[83] To address the

---

80 *See* Better Markets Comment Letter; NASAA Comment Letter; *see also* EPIC Comment Letter ("EPIC agrees that businesses have a natural tendency to want to avoid making disclosures that could incur liability or lose customers").

81 *See* Better Markets Comment Letter.

82 *See*, *e.g.*, SIFMA Comment Letter 2 (notification should only be required if the covered institution makes an affirmative finding of substantial harm or inconvenience); CAI Comment Letter (proposing revised notification trigger to no later than 30 days from a determination that actual or reasonably likely unauthorized access to sensitive customer information has occurred); ACLI Comment Letter (suggesting trigger should instead be only after the completion of a reasonable investigation and conclusion of the incident response process).

83 The Banking Agencies' Incident Response Guidance advises that a covered institution should provide notice to affected customers if, following the conclusion of a reasonable investigation, it has determined that misuse of sensitive customer information has occurred or is reasonably possible. *See* Banking

concern that lengthy investigations might unduly delay customer notifications, one commenter suggested revising the rule to separately require covered institutions "to conduct a prompt investigation of potential incidents," which the commenter stated would better align with certain existing state law standards while still providing a mechanism for timely notifications.[84]

We considered the alternative approaches suggested by commenters but determined that adopting the standard as proposed strikes an appropriate balance in accommodating the relevant competing concerns. The suggestions to expand the circumstances requiring notification (either by requiring notification regardless of the risk of harm, or by expanding notification to include cases where it is "reasonably possible" that an individual's sensitive customer information was accessed or used without authorization) raise over-notification concerns, particularly given that the adopted standard already has a presumption towards notification.[85] We also disagree that the "reasonably likely" standard would allow a covered institution that knows it suffered a breach to avoid providing notice simply by pointing to a lack of information about the scope of the breach as the commenter recommending this approach suggested.[86] To the contrary, under the proposed and final amendments, if it is reasonably likely that a malicious actor gained access to a covered institution's information system containing sensitive customer information but the scope of the breach is unclear (i.e., the covered institution is unable to determine which specific individuals' sensitive customer information has been accessed or used without authorization and cannot make the determinations required under the rule to avoid sending notices), the covered institution

---

Agencies' Incident Response Guidance. *See also* section II.A.3.d(1) (responding to commenters' concerns that the proposed notification timing requirements provide an insufficient amount of time for covered institutions to conduct a reasonable investigation of a data breach incident and prepare and send notices to affected individuals).

84 *See* CAI Comment Letter.

85 *See supra* footnotes 78-80 and accompanying text.

86 *See* NASAA Comment Letter.

would be required to provide notice to each individual whose sensitive customer information resides in the customer information system.[87] In addition, providing notice of every incident, regardless of the risk of harm to affected individuals or the need to take protective measures, could diminish the impact and effectiveness of the notice in a situation where enhanced vigilance is necessary. Utilizing a "reasonably possible" standard raises similar concerns, as it could require covered institutions to provide notice in situations where it is possible, but not reasonably likely, that sensitive customer information was compromised. This could result in over-notification where, for example, a customer's sensitive information ultimately was not accessed or used without authorization, but it was not possible to rule out that possibility at the time of the incident or in the course of a reasonable investigation during the 30-day period for notices.

Additionally, we are not adopting a commenter's recommendation that the Commission require covered institutions to provide notices to the Commission when they are required to send notices to affected individuals, as one commenter suggested.[88] A primary reason for these amendments was to require a reasonably designed incident response program, including policies and procedures for assessment, control and containment, and customer notification, in order to mitigate the potential harm to individuals whose sensitive information is exposed or compromised in a data breach.[89] Providing timely notices to affected individuals accomplishes this goal without the need for covered institutions also to provide copies of the notice to the Commission.

Conversely, the narrower alternative standards suggested by commenters (i.e., that covered institutions have a notification obligation only after an investigation, and only if they

---

87 *See* final rule 248.30(a)(4)(i) and (ii).

88 *See* Better Markets Comment Letter.

89 Proposing Release at section I.

affirmatively determine a likelihood of a breach or resulting harm to customers) could result in an unreasonable risk of significant delays in providing notice and in notification not being provided to affected individuals. A principal purpose of these amendments is to provide a notification regime that allows affected individuals to take actions to avoid or mitigate the risk of substantial harm or inconvenience.[90] If customer notification of a potential breach was delayed to allow a covered institution to complete an investigation that comes to a definitive conclusion about the precise details of the breach, even if done promptly, it would frustrate this goal by postponing (or potentially limiting or foreclosing) the ability of affected individuals to take mitigating actions pending the conclusion of that investigation. For these same reasons, we were not persuaded by those commenters who suggested that we should allow for the completion of an investigation in order to align with the Banking Agencies' Incident Response Guidance. After considering the comments, we continue to believe the notification standard we proposed (and are adopting in the final amendments) is necessary to enable affected individuals to make their own determinations on needed self-protections regarding the incident.[91]

Regarding commenters' concerns about harmonizing Regulation S-P with state law requirements, state law notification standards vary widely such that broad harmonization would be impracticable, and a benefit of the final amendments is that they provide a consistent minimum federal notification standard to protect affected individuals in an environment of enhanced risk. This will, for example, provide additional protections for customers in states whose laws do not mandate notification without an affirmative determination of harm or provide

---

[90] *See* Proposing Release at nn.97-98 and accompanying text.

[91] *See* Proposing Release at n.100 (discussing reasons for divergence from Banking Agencies' Incident Response Guidance); *see also infra* sections II.A.3.b, II.A.3.e, II.A.4, II.B.2, and IV.C (also discussing the Banking Agencies' Incident Response Guidance).

an outside time by which notification must be provided.[92] This standard will protect all customers, regardless of their state of residence and reduce the potential confusion that could result from customers in one state receiving notice of an incident while customers in another state do not. Moreover, to the extent a covered institution will have a notification obligation under both the final amendments and a similar state law, a covered institution may be able to provide one notice to satisfy notification obligations under both the final amendments and the state law, provided that the notice includes all information required under both the final amendments and the state law, which may reduce the number of notices an individual receives.[93]

Relatedly, some commenters suggested eliminating or narrowing the concept of "affected individuals" entitled to notification in situations where a covered institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization. Instead of the proposed requirement that 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, commenters urged narrowing notification to individuals whose sensitive customer information was, or was reasonably likely to have been, accessed or used without authorization based on the covered institution's reasonable investigation.[94] These commenters stated that, by

---

92 *See* Proposing Release at nn.107-108 and accompanying text (discussing variation in state laws); *see also infra* section IV.C.2 for a fuller discussion of state law variations, and *infra* section IV.D.1.b(2) discussing timing of state law notification regimes.

93 *See also infra* section IV.C.2.a(2) (discussing states that excuse covered entities from individual notification under state law if the entities comply with the notification requirements of another regulator).

94 *See, e.g.,* IAA Comment Letter 1 (suggesting the rule's affected individuals' provision be modified to remove the reference to situations where an institution is unable to identify which specific individual's sensitive customer information has been accessed or used without authorization, as well as the presumption that affected individuals include individuals whose sensitive customer information resides in the breached customer information system); CAI Comment Letter (suggesting the provision be revised to remove the requirement to notify all individuals whose information is on an affected system, and instead require the institution to notify individuals whose information it reasonably believes was, or reasonably could have

requiring a covered institution to provide all affected individuals notice prior to the conclusion of an investigation and particularized determination, the proposed notification standard could result in the over-notification of individuals whose sensitive customer information may not have been accessed but was residing on a system that was compromised.[95] For example, one commenter posited a situation where a threat actor was able to compromise an employee's email account through a phishing email, and access documents accessible through that account's shared file server. According to this commenter, if the covered institution were unable to determine which files containing personal information actually were accessed, the institution would be required to provide notice in connection with millions of records, even though the "vast majority of files and data on that file server would not have been accessible to the employee or to the threat actor."[96] These commenters stated that the resulting over-notification could, in turn, desensitize or unnecessarily disturb individuals whose information was not actually compromised, and might increase costs and litigation and reputational risks for the covered institution, its service providers, or other financial institutions whose contracts reside on the system.[97]

For similar reasons to those discussed above,[98] we were not persuaded by commenter suggestions to narrow the scope of affected individuals entitled to notification in cases where a breach has or is reasonably likely to have occurred, but the covered institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization.[99] Because of the potential that customers might be adversely affected by

---

been, subject to unauthorized access based on the finding of its investigation).

95 *See, e.g.*, CAI Comment Letter; Computershare Comment Letter; IAA Comment Letter 1.

96 CAI Comment Letter.

97 *See also infra* section IV.D.1.b.(4) (discussing reputational costs).

98 *See supra* footnotes 90-93 and accompanying text.

99 *See supra* footnotes 94-97 and accompanying text.

the breach, covered institutions should be required to provide notice to affected individuals in these circumstances so they may make their own determination as to whether to take remedial actions.

Contrary to the concerns expressed by some commenters, under the proposed and final amendments, a covered institution would not need to provide notice in connection with files or data residing on a system where it knows that information was not used or accessed.[100] Rather, a covered institution is only required to provide notification to an affected individual where her sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.[101] Additionally, a covered institution need not provide notice where, after a reasonable investigation of the facts and circumstances of the incident, it 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. To address these commenters' concerns, in a change from the proposal, the final amendments explicitly provide that, in cases where a covered institution reasonably determines that a specific individual's sensitive customer information that resides in the customer information system was not accessed or used without authorization, the covered institution need not provide notice to that individual.[102] Thus, a covered institution would not have an obligation to provide notice to an affected individual whose files happened to reside on a breached information system if it was able to reasonably conclude that those files were not subject to unauthorized use or access.

The notification standard should help to improve security outcomes by incentivizing covered institutions to conduct more thorough investigations after an incident occurs because the

---

100 *See supra* footnote 96 and accompanying text.

101 *See* final rule 248.30(a)(4)(i).

102 *See* final rule 248.30(a)(4)(ii).

rule does not permit a covered institution to rebut the presumption of notification without conducting a reasonable investigation. Further, the rule's requirement that a covered institution provide notice to all affected individuals where it is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization should incentivize covered institutions to establish procedures (for themselves and their service providers) that provide robust protections for sensitive customer information. For example, it may encourage covered institutions to employ a principle of least privilege, so that users' access rights to sensitive customer information on a particular information system are limited to the information strictly required to do their jobs.[103] Protections that limit the scope of any breaches reduce the investigation and notification costs (and as a consequence, the potential harm) resulting from a breach.

For a covered institution's customer notification procedures to remain reasonably designed to notify each affected individual whose sensitive customer information was reasonably likely to have been compromised, as required by the final amendments, the covered institution's policies and procedures generally should be designed to include revisiting notification determinations whenever the covered institution becomes aware of new facts that are potentially relevant to the determination.[104] For example, if at the time of the incident, a covered institution determines that risk of use in a manner that would result in substantial harm or inconvenience is

---

[103] *See, e.g.*, *Defend Privileges and Accounts,* National Security Agency Cybersecurity Information ("Least privilege is the restriction of privileges to only those accounts that require them to perform their duties, while limiting accounts to only those privileges that are truly necessary. Doing this reduces the exposure of those privileges to a smaller, more easily manageable set of accounts. Local administrative accounts and accounts for software program management and installation are particularly powerful, but have small scopes of control and should be restricted as much as possible") (available at https://media.defense.gov/2019/Sep/09/2002180330/-1/-1/0/Defend%20Privileges%20and%20Accounts%20-%20Copy.pdf).

[104] *See* final rule 248.30(a)(3).

not reasonably likely based on the use of encryption in accordance with industry standards, 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 revisit its determination.

As discussed in more detail below, the scope of the final amendments will apply to customer information in a covered institution's possession or that is handled or maintained on the covered institution's behalf, regardless of whether such information pertains to (a) individuals with whom the covered institution has a customer relationship or (b) to the customers of other financial institutions where such information has been provided to the covered institution.[105] Some commenters expressed concern that, as a result of this scope, covered institutions would be required to provide notification to customers of other institutions with whom they do not have a preexisting relationship.[106] One of these commenters suggested that it was unclear how a third-party service provider's notice to a covered institution of a breach would affect that covered institution's obligations.[107] Additionally, some commenters addressed circumstances where multiple covered institutions would all be required to notify affected individuals concerning the same incident, asserting that requiring all covered institutions involved to provide notices to customers would be burdensome, duplicative, and confusing to customers.[108]

Where a covered institution experiences an incident involving sensitive customer information related to the customers of another covered institution, commenters generally suggested that the covered institution that has the customer relationship with the customer whose

---

105 *See infra* section II.B.1.

106 *See* ACLI Comment Letter; Federated Hermes Comment Letter; ICI Comment Letter; SIFMA Comment Letter 2.

107 *See* ACLI Comment Letter.

108 *See* CAI Comment Letter; Computershare Comment Letter.

information was affected should be responsible for providing the required notice.[109] These commenters asserted that this would be more efficient because, if the covered institution that experienced the incident did not have a customer relationship with an affected individual, that covered institution might not have contact information for the individual necessary to send a notice.

After considering comments, we are modifying the proposal to avoid requiring multiple covered institutions to notify the same affected individuals about a given incident. In an effort to minimize duplicative notices, rather than requiring the covered institution with the customer relationship to send the notice as some commenters suggested, the final amendments only require a covered institution to provide notice where unauthorized access to or use of sensitive customer information has occurred at the covered institution or one of its service providers that is not itself a covered institution.[110] That covered institution will have information about the incident itself that is necessary to properly inform affected individuals. Thus, in response to the commenter question about the relationship between a covered institution's receipt of a breach notification from a third party service provider and the covered institution's own obligations,[111] where a service provider (that is not itself a covered institution) provides notice to a covered institution that a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider,[112] that covered institution will be required to initiate

---

109 *See* SIFMA Comment Letter 2; ACLI Comment Letter; Federated Hermes Comment Letter; CAI Comment Letter. Two of these commenters suggested that the covered institution with the customer relationship may make arrangements with other institutions to provide the notice on its behalf. SIFMA Comment Letter 2; ACLI Comment Letter.

110 Final rule 248.30(a)(4). If a covered institution is acting as a service provider, in addition to its own obligations under rule 248.30, it must provide notification to the other covered institution as required by the policies and procedures required in rule 248.30(a)(5)(i).

111 *See* ACLI Comment Letter.

112 *See* final rule 248.30(a)(5)(i)(B).

its incident response program under the final amendments[113] and thereafter, if applicable, provide notice to affected individuals.[114] While we appreciate, as offered by commenters,[115] that a covered institution may not have access to the contact information for some customers, it can coordinate with the covered institution that has a customer relationship to receive contact information as needed for the notices.[116]

Moreover, in another modification from the proposal, the final amendments also provide that a covered institution that is required to notify affected individuals may satisfy that obligation by ensuring that the notice is provided.[117] Accordingly, if a covered institution experiences an incident affecting another covered institution's customers, although the covered institution that experienced the incident is responsible for notification under the final amendments, the two covered institutions can coordinate with each other as to which institution will send the notice.

b. Definition of "Sensitive Customer Information"

As discussed above, covered institutions will be required to notify customers when "sensitive customer information" was, or is reasonably likely to have been, accessed or used without authorization, subject to a reasonable investigation. As proposed and as adopted, the final amendments define the term "sensitive customer information" to mean "any component of customer information alone or in conjunction with any other information, the compromise of

---

113 *See id.*; *see also infra* Section II.A.4.a.

114 *See* final rule 248.30(a)(4)(iii). As described above, a covered institution need not provide notice where, after a reasonable investigation of the facts and circumstances of the incident, it has determined that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. *See* final rule 248.30(a)(4)(i).

115 *See* ACLI Comment Letter, SIFMA Comment Letter 2.

116 Further, as discussed below, a covered institution will be permitted to enter into a written agreement with its service provider to notify affected individuals on its behalf in accordance with the notice requirements. *See* final rule 248.30(a)(5)(ii); *see also supra* section II.A.4.

117 Final rule 248.30(a)(4) (requiring covered institutions to either provide notice or ensure that such notice is provided).

which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information."[118] This definition is calibrated to include types of information that, if exposed, could put affected individuals at a higher risk of suffering substantial harm or inconvenience through, for example, fraud or identity theft enabled by the unauthorized access to or use of the information.[119] As with the proposal, the final amendments provide examples of the types of information that will be considered sensitive customer information.[120] These examples include certain customer 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,[121] along with examples of combinations of identifying information and authenticating information that could create such a risk to an individual identified with the information.[122]

One commenter supported our proposed definition of sensitive customer information and emphasized the benefits of a broad definition.[123] According to this commenter, this breadth helps protect customers by ensuring that they can take the necessary steps to minimize their exposure

---

118 *See* final rule 248.30(d)(9)(i). The definition is limited to information identified with customers of financial institutions. *See* final rule 248.30(d)(5)(i); *infra* section II.B.1. As proposed, 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 are subject to the safeguards rule under the final amendments, including the incident response program and customer notice requirements. *See* final rule 248.30(a); *infra* section II.B.1.

119 *See supra* section II.A.3.a.

120 *See* final rule 248.30(d)(9)(ii).

121 These examples include Social Security numbers and other types of identifying information that can be used alone to authenticate an individual's identity such as a driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, biometric records, a unique electronic identification number, address, or routing code, or telecommunication identifying information or access device.

122 These examples include information identifying a customer, such as a name or online user name, in combination with authenticating information such as a partial Social Security number, access code, or mother's maiden name.

123 *See* Better Markets Comment Letter.

risks and will assist covered institutions in formulating and improving their security standards. Another commenter suggested the proposed definition might be too narrow because it includes the separate concept of substantial harm or inconvenience in the definition, resulting in under-notification.[124] This commenter stated that harms can take many forms, and customers should receive notice of breaches involving customer information even where that information's compromise might not have obvious financial implications to the customer.

Conversely, a number of commenters asserted that the proposed definition was too broad and could lead to over-notification, suggesting that the definition be narrowed to focus on information whose exposure would be more likely to lead to tangible economic harms.[125] For example, some commenters suggested that, rather than providing examples, the definition should list specific data elements that, when combined with an individual's name, are sufficiently sensitive to require notification.[126] These commenters focused on those data elements that could be used to commit identity theft or access the customer's financial account, such as a Social Security number, driver's license or state ID number, or financial account number combined with information necessary to access the account. According to one of these commenters, by using illustrative examples rather than a circumscribed list, covered institutions would face uncertainty over the definition's meaning and would likely err on the side of over-inclusion, which could lead to over-notification.[127] A number of commenters stated that narrowing the definition would be more consistent with the Banking Agencies' Incident Response Guidance

---

124 *See* EPIC Comment Letter.

125 *See, e.g.*, CAI Comment Letter; IAA Comment Letter 1; SIFMA Comment Letter 2; ICI Comment Letter 1.

126 *See* CAI Comment Letter; SIFMA Comment Letter 2.

127 *See* CAI Comment Letter.

and with various state laws.[128] One commenter also suggested the proposed use of the term "compromise" in the definition was unclear, and should be replaced with "unauthorized access or use," consistent with other authorities and language used elsewhere in the proposal.[129]

After considering these comments, we are adopting the definition of "sensitive customer information" as proposed. We recognize that this definition is broader than that used by some states and the Banking Agencies' Incident Response Guidance.[130] However, in contrast to the narrower definition used in some states, the definition of sensitive customer information we are adopting includes identifying information that, in combination with authenticating information (such as a partial Social Security number, access code, or mother's maiden name), could create a substantial risk of harm or inconvenience to the customer because they may be widely used for authentication purposes.[131] Similarly, in contrast to the definition provided in the Banking Agencies' Incident Response Guidance (which 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), the definition in the Commission's final amendments includes customer information identified with an individual (such as Social Security numbers, driver's license numbers, biometric records) that, without any other identifying information, could create a substantial risk of harm or inconvenience to an individual identified with the information.[132]

---

128 *See, e.g.*, SIFMA Comment Letter 2; Computershare Comment Letter; CAI Comment Letter.

129 *See* CAI Comment Letter.

130 *See* Proposing Release at nn.113 and 115 (describing the differences). *But see id.* at n.115, stating that a number of states define the scope of personal information subject to a notification obligation in a manner that generally aligns with the definition of sensitive customer information under these final rules.

131 *See infra* footnote 810 and surrounding text (discussing that 14 states more narrowly define the kind of information that trigger notice requirements than our adopted definition of sensitive customer information in that only the compromise of a customer's name together with one or more enumerated pieces of information triggers the notice requirement).

132 *See* Proposing Release at n.114 and accompanying text, stating that Social Security numbers alone, without any other information linked to the individual, are sensitive because they have been used by malicious

Accordingly, our adopted definition could help affected individuals take measures to protect themselves.

Given the varied and evolving nature of security practices across covered institutions, it would be impractical to provide an exhaustive list of data elements whose exposure could put affected individuals at risk of substantial harm or inconvenience. Further, while we are mindful of concerns about overbreadth and potential over-notification, those concerns are tempered by the definition's harm component and the ability of covered entities to rebut the notification presumption following a reasonable investigation and determination. Given these considerations, we are not broadening the definition of sensitive customer information to encompass information whose exposure does not pose a reasonably likely risk of substantial harm or inconvenience. Nor do we agree that the definition's use of the verb "compromise," which is commonly used to mean "to expose or make liable to danger," is ambiguous in this context or inconsistent with other federal authorities.[133] Individuals are less likely to need to take protective measures in cases where the exposure of their information is not likely to involve a substantial harm or inconvenience.[134]

Finally, several commenters suggested we include an exception or safe harbor in the definition of sensitive customer information for encrypted information.[135] These commenters

---

actors in "Social Security number-only" or "synthetic" identity theft, to open new financial accounts, and that a similar sensitivity exists with other types of identifying information that can be used alone to authenticate an individual's identity such as a biometric record of a fingerprint or iris image.

133 *See, e.g.*, Harmonization of Cyber Incident Reporting to the Federal Government, Homeland Security Office of Strategy, Policy, and Plans, Appendix B: Federal Cyber Incident Reporting Requirements Inventory (Sept. 10, 2023) (summarizing cyber incident reporting regulations of multiple agencies that use the term "compromise," including Departments of Defense, Justice, and Energy, the Federal Communications Commission, the Nuclear Regulatory Commission, and the Federal Energy Regulatory Commission).

134 *See infra* section II.A.3.c.

135 *See* AWS Comment Letter; Google Comment Letter; IAA Comment Letter 1; SIFMA Comment Letter 2.

stated that excepting encrypted information would protect customers by incentivizing covered institutions to adopt encryption practices, limit the potential for voluminous over-reporting of less severe incidents, and align with existing state data breach notification rules. Some of these commenters acknowledged that an exception should not apply in cases where there is reason to believe that the encryption key has been compromised or that the encryption method is outdated.[136] One commenter suggested that if we did not include an exception in the rule text, we should acknowledge that encryption is a factor that covered institutions may take into account in determining whether an incident will result in substantial harm or inconvenience.[137]

After considering these comments, we are not excepting encrypted information from the rule's definition of sensitive customer information because the rule text effectively addresses encrypted information without the need for a provision specifically tailored to that information. Specifically, in applying the final rule, a covered institution may consider encryption as a factor in determining whether the compromise of customer information could create a reasonably likely harm risk to an individual identified with the information.[138] Specifically, we acknowledge that encryption of information using current industry standard best practices is a reasonable factor for a covered institution to consider in making this determination. To the extent such encryption minimizes the likelihood that the cipher text could be decrypted, it would also reduce the likelihood that the cipher text's compromise could create a risk of harm, as long as the associated decryption key is secure.[139] Covered institutions may also reference commonly used

---

136 *See* Google Comment Letter, IAA Comment Letter 1; SIFMA Comment Letter 2.

137 *See* IAA Comment Letter 1.

138 *See* Proposing Release at n.116 and accompanying text.

139 As discussed in the Proposing Release, 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. *See* Proposing Release at n.117 and accompanying text.

cryptographic standards to determine whether encryption, in fact, does substantially impede the likelihood that the cipher text's compromise could create a risk of harm.[140] As industry standards continue to develop in the future, covered institutions generally should review and update, as appropriate, their encryption practices. While we agree with commenters that it is important to incentivize the use of encryption consistent with state law regimes, the final amendments' approach accomplishes this goal while also addressing concerns that any particular approach to encryption may become outdated as technologies and security practices evolve. Relatedly, and for the same reasons, when information that would otherwise constitute sensitive customer information is encrypted, the covered institution may consider the security provided by that encryption in determining whether the cipher text (i.e., the data rendered in a format not understood by people or machines without an encryption key) is sensitive customer information. Accordingly, while the final amendments provide illustrative examples of information (such as a customer's Social Security number) that can constitute sensitive customer information when unencrypted,[141] a covered institution could nevertheless determine that the encrypted representation of that information is not sensitive customer information if the encryption renders the cipher text sufficiently secure, such that the compromise of that encrypted information does not create a reasonably likely risk of substantial harm or inconvenience to an individual.[142]

---

140 We understand that standards included in Federal Information Processing Standard Publication 140-3 (FIPS 140-3) are widely referenced by industry participants. *See* Proposing Release at n.118.

141 *See* final rule 248.30(d)(9)(ii)(A)(*1*) through (*4*) and 248.30(d)(9)(ii)(B).

142 To the extent a covered institution's determination about the security of cipher text affects its determination about whether notice of a breach is required under the final rules, the covered institution would be required to make and maintain written documentation of that determination. *See* final rule 248.30(c)(1)(iii).

c. Substantial Harm or Inconvenience

The GLBA directs the Commission and other Federal financial regulators to, among other things, establish appropriate standards requiring financial institutions subject to their jurisdiction to protect against unauthorized access to or use of customer records or information which could result in "substantial harm or inconvenience" to any customer, without defining what constitutes a substantial harm or inconvenience under the statute.[143] The Commission proposed to define "substantial harm or inconvenience" to mean all personal injuries, as well as instances of financial loss, expenditure of effort, or loss of time when they are "more than trivial," with the proposal also providing a non-exhaustive list of examples of included harms or inconveniences.[144] This proposed definition included a broad range of financial and non-financial harms and inconveniences that may result from the failure to safeguard sensitive customer information.[145] After considering comments, and as discussed further below, we have determined not to define the term "substantial harm or inconvenience" in the final amendments.

Commenters raised various concerns with the proposed definition. Some commenters proposed expanding the definition to include a broader array of harms requiring notification.[146] For example, one commenter suggested revising it to enumerate a list of specific personal injuries requiring notification to help clarify to covered institutions that there are a range of personal injuries that can result from an exposure of customer data.[147] Commenters also

---

143 *See* 15 U.S.C. 6801(b). The Banking Agencies' Incident Response Guidance likewise does not define the term "substantial harm or inconvenience."

144 *See* proposed rule 248.30(e)(11).

145 *See* Proposing Release at n.124.

146 *See* EPIC Comment Letter; NASAA Comment Letter; Better Markets Comment Letter.

147 *See* EPIC Comment Letter (suggesting the definition specifically list as examples of personal injuries: theft, fraud, harassment, physical harm, psychological harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit or government benefits, or the misuse of information identified with an

suggested we remove the requirement that personal or financial harms be nontrivial because, according to these commenters, there might always be some set of individuals to whom a particular personal or financial harm is material, and securities firms are not well positioned to determine what potential personal or financial harms to their customers are significant enough to require customer notice.[148] One of these commenters observed that, while it made sense to apply the concept of nontriviality to potential harms or inconveniences that would infringe upon a customer's time and personal labors, risks to the customer's person and pocketbook are materially different from risks to the customer's time and energies.[149] This commenter also suggested broadening the definition to include the term "cyberattack" as one of the enumerated events that could give rise to the customer notice obligation.

Alternatively, a number of commenters suggested that the proposed standard was ambiguous and urged narrowing the definition to reduce the types of injuries that would require notification.[150] For example, one commenter suggested that we not attempt to define "substantial harm or inconvenience" at all, and further expressed concern that the proposed definition would require notice for harms or inconveniences that are unrelated to identify theft, the means to access an account without authority, or other "tangible harms."[151] Another commenter proposed narrowing the kinds of financial loss or time and effort cognizable under the rules from "more than trivial" to only "material" financial loss or "significant" expenditure of effort or loss of

---

individual to obtain a financial product or service, or to access, log onto, effect a transaction in, or otherwise misuse the individual's account).

148 *See* NASAA Comment Letter; EPIC Comment Letter (agreeing with NASAA's comment).

149 *See* NASAA Comment Letter.

150 *See, e.g.*, Comment Letter of Cambridge ("Cambridge Comment Letter"); CAI Comment Letter; IAA Comment Letter 1; SIFMA Comment Letter 2.

151 *See* SIFMA Comment Letter 2.

time, suggesting that the proposed definition would be inconsistent with the usual meaning of the term "substantial" and could include any financial loss that is slightly above trivial as substantial.[152] Another commenter stated that the use of "more than trivial" set a very low bar that could result in second-guessing and over notification by covered intuitions that could lead to notification in practically all instances, not just instances of what the commenter viewed as a substantial harm or inconvenience.[153] This commenter also stated that, as drafted, it was unclear whether the proposed "more than trivial" standard was meant to apply to instances of personal injury or financial loss and suggested replacing "more than trivial" with substantial, while making clear that the word substantial modified all elements of the definition. Other commenters suggested narrowing the proposed definition by removing the term "inconvenience" from the definition, with notification only required in cases of substantial harm that were more than trivial.[154]

After considering comments, we have determined, consistent with the approach of the Banking Agencies, not to define the term "substantial harm or inconvenience." As the range of commenter concerns discussed above reflects, commenters found the proposed definition simultaneously too broad and too narrow, suggesting it could consequently lead to both under-notification and over-notification. Eliminating the proposed definition avoids this result without diminishing investor protection.

Determining whether a given harm or inconvenience rises to the level of a substantial harm or a substantial inconvenience would depend on the particular facts and circumstances

---

152 *See* IAA Comment Letter 1.

153 *See* CAI Comment Letter ("it is hard to imagine any instance of unauthorized access or use of customer information that could not create a reasonably likely risk of more than trivial inconvenience, and therefore not require notification").

154 *See* Cambridge Comment Letter; Financial Services Institute Comment Letter.

surrounding an incident. As stated in the Proposing Release, 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 them.[155] At the same time, consistent with the GLBA, the rules are intended to protect against unauthorized access to or use of customer records or information which could result in substantial harm or inconvenience to any customer. Given the wide variety of ways that a data breach can injure a customer,[156] and the potentially varied nature of those harms and inconveniences,[157] the range of harms outlined in the proposed definition may be a useful starting point for this determination. A personal injury, financial loss, expenditure of effort, or loss of time, each could constitute a substantial harm or inconvenience depending on the particular facts and circumstances. Some examples of these harms could include theft, fraud, harassment, physical harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the misuse of information identified with an individual to obtain a financial product or service, or to access, log into, effect a transaction in, or otherwise misuse the individual's account.

d. Timing Requirements

(1) General Timing Requirements

Consistent with the proposal, the final amendments require covered institutions to provide notices to affected individuals as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred, except under the limited circumstances discussed below.[158]

---

155 *See* Proposing Release at Section II.A.4.c.

156 *See* Proposing Release at n.124.

157 *See*, *e.g.*, NASAA Comment Letter; IAA Comment Letter 1.

158 *See* final rule 248.30(a)(4)(iii); *see also* section II.A.3.d(2) (discussing the national security and public

This approach reflects the goal of giving covered institutions adequate time to make an initial assessment of an incident and prepare and send notices to affected individuals, while helping to ensure that those individuals receive sufficient notice to protect themselves.

A few commenters expressed support for the proposed notification timing requirements.[159] As described above, these commenters viewed timeliness as important because any delay in notification could impact individuals' ability to take steps to protect themselves from the downstream impacts resulting from the unauthorized access to or use of their sensitive customer information.[160] One commenter asserted that 30 days after becoming aware of an incident is more than an ample amount of time for covered institutions to determine the scope of the compromised information and compile a list of affected customers that must be notified.[161] Accordingly, this commenter suggested that the Commission should shorten the outside notification date from 30 days after becoming aware of a data security incident to 14 days, asserting that the longer an instance of identity theft goes undetected, the greater the damage that usually follows.

In contrast, some commenters objected to the proposed notification timing requirements because, in their view, it provided an insufficient amount of time to notify affected individuals.[162] These commenters emphasized the logistical tasks associated with responding to an information breach, asserting that in some cases it would be impossible to accomplish these steps within 30

---

safety delay to the notification timing requirements).

159 EPIC Comment Letter; Better Markets Comment Letter.

160 *See supra* section II.A.3.a.

161 Better Markets Comment Letter.

162 *See*, *e.g.*, SIFMA Comment Letter 2; IAA Comment Letter 1; FSI Comment Letter; NASDAQ Comment Letter; CAI Comment Letter.

days.[163] Commenters expressed that these steps often include remediating the security incident directly, conducting a risk assessment and investigation to determine what information may have been affected, obtaining the information needed to make notification to affected individuals, arranging identity protection services for affected individuals, and generating and delivering the notifications to affected individuals, all while simultaneously engaging in extensive communication with and oversight from senior management, the board of directors, and external parties (such as outside counsel, expert consultants, and regulators).[164]

Some commenters also suggested that the proposed timing requirements would lead to covered institutions delivering unnecessary or incomplete notifications to customers, which would have the result of confusing or desensitizing customers to such notifications.[165] Similarly, commenters expressed that requiring a covered institution to notify affected individuals before the covered institution has had time to fully assess an incident could result in incorrect or incomplete conclusions being drawn and disclosed.[166] One commenter suggested, for this reason, that notices would be subject to continuous revision during an ongoing investigation.[167] Accordingly, commenters stated that the Commission should revise the proposal to allow more time for covered institutions to provide notices to affected individuals, asserting that premature,

---

163 For example, one commenter offered the example of a ransomware attack that successfully shuts down systems and requires significant remediation to recover backup systems, as well as rebuilding and redeploying essential systems prior to conducting a forensic investigation to determine the scope of data subject to unauthorized access or use. *See* CAI Comment Letter. According to this commenter, it would be practically impossible to accomplish these tasks within 30 days of becoming aware of a possible issue, as required under the proposed rules.

164 *See*, *e.g.*, CAI Comment Letter, NASDAQ Comment Letter; IAA Comment Letter 1.

165 *See*, *e.g.*, ACLI Comment Letter; AWS Comment Letter, NASDAQ Comment Letter.

166 NASDAQ Comment Letter; AWS Comment Letter.

167 AWS Comment Letter.

incomplete, or frequent notifications would ultimately mislead and confuse customers rather than provide clarity about an incident.[168]

Several commenters suggested alternatives to the proposed timing requirements.[169] For instance, a few commenters urged the Commission to expand the 30-day outside date to 45 or 60 days, stating that this modification would allow more time for a proper investigation and notification process.[170] In addition, a couple of commenters suggested that the rule should not specify a number of days at all.[171] One of these commenters stated that simply requiring a covered institution to notify affected individuals as soon as possible after the conclusion of an investigation, without including an outside date timeframe, would permit appropriate notification in both simple cases—where notification in less than 30 days may be appropriate—and more complex cases—where it may take significantly longer to identify the appropriate notice population and prepare and deliver notifications.[172]

Some commenters suggested that the trigger for notification should be the completion of a reasonable investigation and conclusion of the incident response process following the actual or reasonably likely unauthorized access to or use of sensitive customer information, rather than the proposal's trigger of a covered institution "becoming aware" of a breach of customer information.[173] These commenters stated this alternative would allow covered institutions

---

168 ACLI Comment Letter; AWS Comment Letter, NASDAQ Comment Letter.

169 *See*, *e.g.*, IAA Comment Letter 1; FSI Comment Letter; Cambridge Comment Letter; Federated Comment Letter; SIFMA Comment Letter 2.

170 *See* FSI Comment Letter; Cambridge Comment Letter; IAA Comment Letter 1.

171 Federated Comment Letter; SIFMA Comment Letter 2.

172 SIFMA Comment Letter 2.

173 *See* SIFMA Comment Letter 2; ACLI Comment Letter; *see also* CAI Comment Letter (suggesting that a revised rule could require covered institutions to conduct a prompt investigation of potential incidents to address concerns about lengthy investigations unduly delaying customer notification.).

sufficient time to engage in system and data analysis to determine what data was impacted and what individuals were affected. Moreover, some commenters stated that their suggested alternatives would harmonize the rule's approach to timing with existing data breach requirements and guidance, such as the Banking Agencies' Incident Response Guidance and some current state laws.[174] Lastly, one commenter urged that the 30-day outside timeframe to provide notices should run from the time that the covered institution determines that an incident involved "sensitive customer information," rather than "customer information" as proposed. [175]

After considering comments and alternatives suggested by commenters, we are adopting the final amendments as proposed. We considered the concern raised by commenters that it may be logistically challenging for covered institutions to provide notice to affected individuals within the proposed rule's notification timing requirements, particularly for more complex data breach incidents.[176] We recognize that modifying the timing trigger in the rule to start after a covered institution has completed an investigation that comes to a definitive conclusion about the precise details of the breach, as suggested by some commenters, could avoid over-notification in cases where a covered institution is able to determine that a given individual's customer information ultimately was not affected after a lengthy investigation. We agree with commenters, however, that timeliness is important in the context of a breach of sensitive customer information because delay in notification would impact the ability of affected individuals to take measures to

---

174 *See* FSI Comment Letter; SIFMA Comment Letter 2 (suggesting conforming to Banking Agencies' Incident Response Guidance which does not mandate specific number of days to provide notices); *see also* IAA Comment Letter 1 (stating that "over half of state data breach notification laws do not specify a number of days to report a breach and a majority of those states that do require notification allow for 45-60 days for reporting").

175 IAA Comment Letter 1 (suggesting that referring to "customer information," rather than "sensitive customer information," in this part of the proposed rule was an inadvertent omission).

176 *See, e.g.,* CAI Comment Letter; ACLI Comment Letter.

protect themselves. Accordingly, the final amendments maintain the proposed timing trigger of after the covered institution "becomes aware" that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred.[177]

In addition, the final amendments adopt the proposed 30-day outside date. We disagree that the rule should not include a specified notification deadline, as such an approach would diminish the goal of providing customers (regardless of state residency) with early and consistent notification of data breaches so that they may take remedial action because many states do not have any specific deadline for sending notices or provide deadlines exceeding 30 days.[178]

We understand that there are a number of steps a covered institution may have to take after becoming aware of a data breach incident to determine if it has met the standard for providing notice. In the context of the final amendments, 30 days should be sufficient to conduct an initial assessment and notify affected individuals. While a covered institution may still be working towards remediating the breach after the 30-day timeframe, the final amendments

---

[177] While this "becoming aware" standard differs from the reporting trigger in the Public Company Cybersecurity Rules (which require public disclosure of public issuer cybersecurity incidents four business days from when an issuer determines that a cybersecurity incident that it has experienced is material), that difference is attributable to the different purposes underlying the rules. The Public Company Cybersecurity Rules were designed to inform investment and voting decisions and to reduce information asymmetry and mispricing in the market, and therefore tie public disclosure to an issuer making a determination that information about an incident would be material, meaning there would be a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision. As we stated in that release, "we reiterate, consistent with the standard set out in the cases addressing materiality in the securities laws, that information is material if 'there is a substantial likelihood that a reasonable shareholder would consider it important' in making an investment decision, or if it would have 'significantly altered the "total mix" of information made available.'" *See* Public Company Cybersecurity Rules. By contrast, the notice provisions under these final rules do not require covered institutions to make a materiality determination, and balance the need for timely notifications with a regime that allows for reasonable investigations to avoid over-notification by allowing covered institutions up to 30 days to conduct a reasonable investigation after becoming aware of an incident. In light of this 30-day window, and the fact that covered institutions are not required to make a materiality determination, there is less need for a trigger based on a determination standard, and greater risk of harm to affected individuals if customer notification were further delayed by requiring that a covered institution come to a determination before triggering the 30-day notification window.

[178] *See infra* section IV.D.1.b(2).

require a covered institution to notify affected customers within the 30-day timeframe so that affected individuals may take measures to protect themselves. The final amendments remove the specific requirement in the proposal that the notice describe what has been done to protect the sensitive customer information from further unauthorized access or use.[179] This change will help address some of the timing and logistical concerns raised by commenters because the process of preparing the requisite notices will be less time intensive, such that, once a covered institution has made its initial assessment of the incident and determined the universe of affected individuals, it should possess the information necessary to provide the requisite notices.

In addition, with regard to the commenter concern that it may be logistically challenging to provide a notice within the rule's timing requirements in cases where a ransomware attack has denied the covered institution access to its systems,[180] that comment does not account for the fact that, under the proposed and final amendments, covered institutions will now be required to have an incident response program that includes policies and procedures to, among other things, assess the nature and scope of any qualifying incidents, identify customer information systems and types of customer information that may have been accessed or used without authorization, and respond to and recover from those incidents.[181] Thus, as proposed, consistent with the final amendments, covered institutions will need to anticipate and prepare for the possibility that they may be denied access to a particular system (such as in the ransomware example offered by one commenter) and have procedures in place for complying with the notice requirements when applicable.

---

179 *See* final rule 248.30(a)(4)(iv); *infra* section II.A.3.e. (discussing in more detail the modification to the notice content requirements).

180 *See* CAI Comment Letter.

181 *See supra* section II.A; final rule 248.30(a).

Consistent with the proposal, the final amendments will require that covered institutions provide notices "as soon as practicable," but not more than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred. 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.[182] The requirement to notify affected individuals as soon as practicable but not more than 30 days in the final amendments is consistent with the purposes of the GLBA and reflects the importance of expeditious notification. The amendments are designed to help ensure that customers receive notification in a timely manner. It would be contrary to this policy goal for a covered institution to unduly delay notification to customers, for example by delaying notice until it has definitively concluded that a data breach incident has occurred, because this could result in excessively delayed notifications that could unnecessarily hinder affected customers from engaging their own remedial measures to protect their data. A covered institution should act promptly and must not delay its initial assessment of the available details of the incident as delaying notices could deprive customers of the ability to take prompt action to protect themselves.

The 30-day outside timeframe under both the proposed and final rules begins following an incident involving customer information. This is consistent with the scope of the incident response program, which is required to address unauthorized access to or use of customer information. The outside timeframe does not begin from the time that the covered institution determines that an incident involved "sensitive customer information," as suggested by one

---

[182] 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 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. *See* Proposing Release at n.133.

commenter.[183] The commenter's suggested modification would likely delay notification as compared to the final rule because covered institutions could take considerable time to determine that an incident involved sensitive customer information before the outside timeframe would begin and this could further delay any potential notice to affected individuals.

(2) National Security and Public Safety Delay

The final amendments will allow covered institutions to delay providing notice if the Attorney General determines that the notice required under the final amendments poses a substantial risk to national security or public safety, and notifies the Commission of such determination in writing, in which case the covered institution may delay such notice for a time period specified by the Attorney General, up to 30 days following the date when such notice was otherwise required to be provided.[184] Previously referred to as the "law enforcement exception" in the proposal, the national security and public safety delay has been expanded to incorporate risks related to public safety in addition to national security. In a modification of the proposal, in which the Attorney General would have informed only the covered institution in cases where this delay is granted, in the final amendments the Attorney General will instead inform the Commission, in writing, if the Attorney General determines that the notice poses a substantial risk to national security or public safety. This modification is designed to ensure that the Commission receives information related to a delay in notice in an efficient and timely manner. We have consulted with the Department of Justice to establish an interagency communication process to allow for the Attorney General's determination to be communicated to the Commission in a timely manner. The Department of Justice will notify the covered institution

---

183 IAA Comment Letter 1.

184 *See* final rule 248.30(a)(4)(iii).

that communication to the Commission has been made so that the covered institution may delay providing the notice.

In another change from the proposal, the notice may be delayed for an additional period of up to 30 days if the Attorney General determines that the notice continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. In a further change in response to comments, in extraordinary circumstances, notice may be delayed for a final additional period of up to 60 days if the Attorney General determines that notice continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. Beyond the final 60-day delay, if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such delay through a Commission exemptive order or other action. By contrast, the proposed rules would have allowed a covered institution to delay notice only for an aggregate period of 30 days following a written request from the Attorney General to the covered institution, upon the expiration of which the covered institution would have been required to provide notice immediately. The modification to the proposed rule is designed to respond to concerns raised by commenters.[185]

One commenter stated that a delay in notifying affected individuals for law enforcement activity may cause harm to customers whose personal information has been exposed.[186] In addition, this commenter asserted that notifying affected individuals would not impede a law enforcement investigation of the data security incident.

---

[185] The final amendments will align more closely with the Public Company Cybersecurity Rules on this point by incorporating a similar scope and timing for its national security and public safety delay.

[186] Better Markets Comment Letter.

Other commenters, however, urged the Commission to expand the proposed law enforcement exception because, in their view, the proposed exception was too narrowly drawn.[187] Several of these commenters expressed concern that requests by local or State police, or even other Federal agencies, would not be sufficient to delay notification under the proposed rule.[188] Some commenters stated concerns about the feasibility and process of reaching out to the Attorney General to request a delay in support of expanding the exception to permit other law enforcement agencies to direct a covered institution to delay a notice.[189] Commenters also expressed particular concern around competing requirements, noting that many state regulations include a more permissive delay and that covered institutions, in an effort to comply with the proposed exception, may be put into the difficult and unnecessary position of being subject to conflicting requirements from the Commission and a state law enforcement entity.[190] Further, commenters articulated that the proposed exception is excessively narrow because it only accommodates law enforcement actions that address concerns that rise to the level of "national security."[191]

In addition to concerns regarding the scope of the proposed law enforcement exception, several commenters opposed the length of time that a covered institution would be permitted to

---

187 *See*, *e.g.*, IAA Comment Letter 1; SIFMA Comment Letter 2; NASDAQ Comment Letter; CAI Comment Letter; FII Comment Letter.

188 *See*, *e.g.*, CAI Comment Letter; ICI Comment Letter 1; FII Comment Letter; SIFMA Comment Letter 2 (suggesting that the proposed law enforcement exception should also contemplate foreign law enforcement and include cooperation with international authorities).

189 *See* ICI Comment Letter; SIFMA Comment Letter 2.

190 *See*, *e.g.*, ICI Comment Letter 1; NASDAQ Comment Letter; FII Comment Letter; IAA Comment Letter 1 (viewing the proposed exception as creating broader security risks for clients and advisers and forcing an adviser to choose between disregarding a law enforcement request or violating the rule).

191 CAI Comment Letter; ICI Comment Letter 1; SIFMA Comment Letter 2.

delay notice under the proposed rule.[192] These commenters suggested that there should be no outside time limitation on the proposed law enforcement exception, asserting that the judgment of any law enforcement agency investigating a breach should be an adequate and respected basis for delaying a regulatory notice regarding such breach. Commenters urged the Commission to expand the scope and timing requirements of the proposed law enforcement exception, expressing that they failed to understand the public purpose that would be served by ignoring the request of a law enforcement agency to delay notification.[193]

In response to commenters' concerns, we have broadened both the scope and timing requirements of the delay in the final amendments. The final amendments will allow covered institutions to delay notice in cases where disclosure would pose a substantial risk to national security or public safety, contingent on a written notification by the Attorney General to the Commission.[194] This provision has been expanded to incorporate risks related to public safety, and not just national security, as proposed. This expansion allows for notice delay in scenarios where there may be significant risk of harm from disclosure; however, there may not be a substantial risk to national security. This modification should make the provision sufficiently expansive to protect against significant risks of harm from disclosure—such as the risk of alerting malicious actors targeting critical infrastructure that their activities have been

---

192 *See*, *e.g.*, IAA Comment Letter 1; ICI Comment Letter 1; NASDAQ Comment Letter; SIFMA Comment Letter 2; CAI Comment Letter.

193 *See*, *e.g.*, IAA Comment Letter 1; NASDAQ Comment Letter; *see also* SIFMA Comment Letter 2 (stating its view that only for a limited number of cases would delay be requested or mandated by other government entities, or court orders, so notification delays would not become routine or be otherwise abused).

194 A covered institution requesting that the Attorney General determine that notification under the rule would pose a substantial risk to national security or public safety does not change the covered institution's obligation to provide notice to affected customers within the timing required under the final amendments. This is because the rule permits a delay only upon the Attorney General making that determination and communicating it to the Commission in writing.

discovered—while also helping to ensure that individuals are not unduly denied timely access to information about the unauthorized access to or use of their sensitive customer information.

With respect to commenters who recommended that other Federal agencies, State and local law enforcement agencies, and foreign law enforcement authorities also be permitted to trigger a delay or suggested that the perceived limited nature of this delay would cause conflict with state authorities, the rule does not preclude any such entity from requesting that the Attorney General determine that the disclosure poses a substantial risk to national security or public safety and communicate that determination to the Commission. Designating a single law enforcement agency as the point of contact for both the covered institution and the Commission on such delays is critical to ensuring that the rule is administrable. Some commenters stated concerns about the feasibility and process of reaching out to the Attorney General to request a delay, urging the Commission to expand the delay to apply to requests made by other law enforcement agencies in addition to the Attorney General. The FBI, in coordination with the Department of Justice, has since provided guidance on how firms can request disclosure delays for national security or public safety reasons in connection with the Public Company Cybersecurity Rules.[195] To the extent needed, further guidance may be issued on how other law enforcement agencies may contact the Department of Justice to request a delay.

The final amendments also will expand the amount of time that a covered institution can delay notice under this provision. However, we are not persuaded, as some commenters suggested, that the rules should not incorporate a timing component at all because such an approach would diminish the goal of providing customers (regardless of state residency) with

---

[195] *See* FBI Guidance to Victims of Cyber Incidents on SEC Reporting Requirements, available at: https://www.fbi.gov/investigate/cyber/fbi-guidance-to-victims-of-cyber-incidents-on-sec-reporting-requirements.

timely and consistent notification of data breaches so that they may take remedial action. This includes permitting, in extraordinary circumstances, a delay for a final additional period of up to 60 days—following two previous 30-day extensions—if the Attorney General determines that disclosure continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. We are providing for this additional delay period in the final amendments, beyond what was originally proposed, and in addition to the two 30-day delays that may precede it, in recognition that, in extraordinary circumstances, national security concerns may justify additional delay beyond that warranted by public safety concerns, due to the relatively more critical nature of national security concerns.[196] Beyond the final 60-day delay, if the Attorney General indicates to the Commission in writing that further delay is necessary, the covered institution can request an additional delay that the Commission may grant through exemptive order or other action. These modifications acknowledge that additional time beyond that proposed may be necessary, as called for by commenters, while balancing national security and public safety concerns against affected individuals' informational needs.

e. Notice Contents and Format

The final amendments, consistent with the proposal, require that notices include key information with details about the incident, the breached data, and how affected individuals can respond to the breach to protect themselves. This requirement is designed to help ensure that covered institutions provide basic information to affected individuals that will help them avoid or mitigate substantial harm or inconvenience. In a modification from the proposal, however, the

[196] Under the proposal, in contrast, the covered institution could delay a notice if the Attorney General informed the covered institution, in writing, that the notice poses a substantial risk to national security. The proposal provided that the covered institution could delay such a notice for a time period specified by the Attorney General, but not for longer than 15 days, plus an additional period of up to 15 days if the Attorney General determines that the notice continues to pose a substantial risk to national security.

final amendments will not require the notice to "[d]escribe what has been done to protect the sensitive customer information from further unauthorized access or use."

Some of the information required by the final amendment, including information regarding a description of the incident, and the type of sensitive customer information accessed or used without authorization, will provide affected individuals with basic information to help them understand the scope of the incident and its potential ramifications. As proposed, the final amendments will 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 affected individuals can easily seek additional information from the covered institution. All of this information may help affected individuals assess the risk posed by the incident and whether to take additional measures to protect against harm from unauthorized access or use of their information.

Similarly, as proposed, the final amendments will require information regarding the date of the incident, the estimated date of the incident, or the date range within which the incident occurred, if such information is reasonably possible to determine at the time the notice is provided. This requirement reflects the reality 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.[197]

In addition, as proposed, the final amendments will require that covered institutions include certain information to assist affected individuals in evaluating how they should respond

[197] *See* Proposing Release at n.142.

to the incident. Specifically, if the affected individual has an account with the covered institution, the final amendments will require the notice to recommend that the customer review account statements and immediately report any suspicious activity to the covered institution. The final amendments will also require the notice to explain what a fraud alert is and how an affected individual may place a fraud alert in credit reports. Further, the final amendments will require that the notice recommend that the affected individual periodically obtain credit reports from each nationwide credit reporting company and that the individual have information relating to fraudulent transactions deleted. The notice must also explain how a credit report can be obtained free of charge. Lastly, the final amendments require that notices include information regarding FTC and usa.gov guidance on steps an affected individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the FTC, and the FTC's website address. These specific requirements are designed to give affected individuals resources and additional information to help them evaluate how they should respond to the incident.

As proposed, under the final rules covered institutions will be required to provide the information specified in the final amendments in each required notice. While we recognize that relevant information may vary based on the facts and circumstances of the incident, customers will benefit from the same minimum set of basic information in all notices. Accordingly, the final amendments will permit covered institutions to include additional information but will not permit omission of the prescribed information. In addition, the final amendments will require covered institutions to provide 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.[198]

---

[198] *See* final rule 248.30(a)(4)(i); *see also* 17 CFR 248.9(a) (delivery requirements for privacy and opt out

Pursuant to 17 CFR 248.3, notices will therefore 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.[199] To the extent that a covered institution includes information in the notice that is not required to be provided to customers under the final amendments or provides notice contemporaneously with other disclosures, the covered institution will still be required to ensure that the notice is designed to call attention to the important information required to be provided under the final amendments; the inclusion of any additional information in the notice may not prevent the required information from being presented in a clear and conspicuous manner. The requirement to provide notices in writing, further, will 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.[200] These requirements are designed to help ensure that customers are provided informative notifications and alerted to their importance.

Several commenters broadly supported the proposed notice contents and format requirements.[201] One commenter stated that the provision will lead to notices that contain important information in a clear and conspicuous manner, which will allow affected individuals to assess the risk of the incident paired with guidance on potential protective measures to take.[202]

---

notices) and 17 CFR 248.3(c)(1) (defining "clear and conspicuous").

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

200 This requirement to provide notice "in writing" could be satisfied either through paper or, for customers who agree to receive information electronically, though electronic means consistent with existing Commission guidance on electronic delivery of documents. *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)].

201 *See*, *e.g.*, Better Markets Comment Letter, IAA Comment Letter 1; NASAA Comment Letter.

202 Better Markets Comment Letter (stating that the provision "avoids some common problems with the

Another commenter agreed with the proposed approach of requiring notices to contain certain information but not prescribing the specific format for the notices, asserting that this approach will "make it easier for covered institutions to fulfill all their notice obligations under federal and state laws with as few notice documents as possible (ideally through a single notice to all affected customers nationwide)."[203]

Conversely, a few commenters opposed certain aspects of the notice content and format requirements.[204] One commenter expressed concern related to the proposed requirement for covered institutions to include in the notice specific efforts they have taken to protect the sensitive customer information from further unauthorized access or use.[205] This commenter articulated that this information could be extremely useful to threat actors and not particularly useful to affected individuals.[206] Another commenter urged the Commission to remove the requirement for covered institutions to provide "the date of the incident, the estimated date of the incident, or the date range," asserting that this specific information is not required by the Banking Agencies' Incident Response Guidance and should not be included in an amended Regulation S-P.[207] In addition, two commenters suggested that the final amendments should provide more flexibility for covered institutions to determine the manner and method in which

---

content of many data breach notifications, such as confusing language, a lack of details, and insufficient attention to the practical steps customers should take in response.").

203 *See* NASAA Comment Letter (stating that "[b]eing prescriptive here could potentially create inconsistencies with current or future state notice laws, which in turn could cause covered institutions to feel compelled to deliver entirely duplicative notices to customers simply for reasons of form. Customers should not be burdened in this way, and the Reg. S-P Proposal rightly takes this into account.").

204 *See*, *e.g.*, CAI Comment Letter; ICI Comment Letter 1; IAA Comment Letter.

205 IAA Comment Letter 1.

206 *Id.* (further stating that in many cases "the adviser will have already remediated the vulnerability, making the information even less relevant to a client's decision.").

207 ICI Comment Letter 1.

they should be contacted by affected individuals inquiring about an incident.[208] Lastly, one commenter urged the Commission to consider whether it should require specific notice obligations at all, asserting that Federal notice would simply add another layer on top of existing State data breach notice requirements and would offer limited benefits to affected individuals.[209]

After considering comments, we are removing the specific requirement in the proposal that the notice "[d]escribe what has been done to protect the sensitive customer information from further unauthorized access or use." We agree that this information has the potential to advantage threat actors and does not provide actionable information for affected individuals. Accordingly, the provision has been removed from the final amendments, which should reduce the perceived risk of providing a roadmap for threat actors compared with the proposal. Covered institutions may, however, voluntarily disclose details related to the incident's remediation status.

The final amendments do not modify the proposed requirement for covered institutions to provide information about the date of the incident, as suggested by one commenter.[210] Providing this information to affected individuals, to the extent the information is reasonably possible to determine, can help affected individuals identify the point in time in which their sensitive customer information was compromised, thus providing critical details that affected individuals can use to take targeted protective measures (e.g., review account statements) to mitigate the potential harm that could result from the unauthorized access to or use of their sensitive customer

---

[208] CAI Comment Letter; SIFMA Comment Letter 2 (asserting that the rule should not require each of a telephone number, an email address, a postal address and a specific office contact, but rather should allow covered institutions to choose one or more of those contact options based on how the covered institution normally interacts with its customers).

[209] *See* CAI Comment Letter; *see also* NASDAQ Comment Letter (asserting that covered institutions "should be permitted to comply with various state and federal cybersecurity notification obligations with a single streamlined form.").

[210] ICI Comment Letter 1.

information. For this reason, we disagree with the commenter that stated firms should not be required to provide this information in their notice.

Similarly, the final amendments do not modify the requirement for notices to include the prescribed contact information sufficient to permit an affected individual to contact the covered institution to inquire about the incident. We understand that covered institutions communicate with their customers using many different methods and formats. However, providing a telephone number, an email address or equivalent method or means (e.g., an online submission form), a postal address, and the name of a specific office to contact, is designed to provide sufficient optionality for affected individuals, who may have differing preferences and aptitudes in their use of contact methods.[211] Nothing in this requirement, however, prevents a covered institution from choosing to provide additional contact methods.

Lastly, the final amendments do not prescribe a specific format for the notice to affected customers. We agree with the commenter that asserted that such flexibility will make it easier for covered institutions to provide notices that meet the requirements of the final amendments while also meeting the requirements of other notice obligations, such as certain state requirements, and thereby mitigates commenter concerns about the potential for more than one notice covering a given incident.

---

[211] In addition, the final rule's requirement to provide contact information sufficient to permit an affected individual to inquire about the incident does not preclude a covered institution from providing the contact information of a third-party service provider that has been engaged by the covered institution to provide specialized information or assistance about the unauthorized access or use of sensitive customer information on the covered institution's behalf. *See* CAI Comment Letter (asserting that it is current business practice for companies to hire vendors who provide specialized breach response call centers to handle consumer inquiries).

4. Service Providers

The final amendments require that each covered institution's incident response program include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence on and monitoring, of service providers, including to ensure that the covered institution satisfies the customer notification requirements set forth in paragraph (a)(4) of the final amendments.[212] In a modification from the proposal, rather than requiring written policies and procedures requiring the covered institution to enter into a written contract with its service providers to take certain appropriate measures, the policies and procedures required by the final amendments must be reasonably designed to ensure service providers take appropriate measures to: (A) protect against unauthorized access to or use of customer information; and (B) provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware of a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider.[213] In a modification from the proposal, upon receipt of such notification, a covered institution must initiate its incident response program pursuant to paragraph (a)(3) of this section.[214] The final amendments thus modify the proposal by removing the written contract requirement and shifting the notification deadline for the service provider's

---

212 *See* final rule 248.30(a)(5)(i).

213 *See id.* In the proposal, the covered institution's written contract with its service provider would have needed to require the service providers to take appropriate measures 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 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. *See* proposed rule 248.30(b)(5)(i).

214 *See id*. As discussed further below, this modification responds to comments by incorporating into rule text the Commission's intention that covered institutions would "expeditiously" implement their incident response program following the receipt of such notification from a service provider, as discussed in the Proposing Release. *See infra* footnote 223 and accompanying discussion on clarifying modifications. *See also* Proposing Release at Section II.A.3.

notification of the covered institution from 48 to 72 hours, while retaining the notice trigger of the service provider "becoming aware of" a breach in security resulting in unauthorized access to a customer information system maintained by the service provider.[215]

However, the Commission is adopting as proposed final amendments that provide that a covered institution, as part of its incident response program, may enter into a written agreement with its service provider to notify affected individuals on the covered institution's behalf in accordance with paragraph (a)(4) of the final amendments.[216] In a modification from the proposal, the final amendments provide that even where a covered institution uses a service provider in accordance with paragraphs (a)(5)(i) and (ii) of the final amendments, the covered institution's obligation to ensure that affected individuals are notified in accordance with paragraph (a)(4) of the final amendments rests with the covered institution.[217]

Finally, the Commission is also defining a "service provider" at adoption to mean any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution.[218] As discussed further below, this definition removes language from the proposed definition relating to third parties, but does so solely to make plain that the definition of a "service provider" can include affiliates of a covered institution.[219]

---

215 *See* final rule 248.30(a)(5)(i).

216 *See* final rule 248.30(a)(5)(ii).

217 *See* final rule 248.30(a)(5)(iii). As discussed further below, this modification is intended to clarify covered institutions' responsibilities under the final amendments by incorporating into rule text the Commission's intended scope, as discussed in the Proposing Release. *See* discussion on Delegation of Notice and Covered Institutions' Customer Notification Obligations *infra* Section II.A.4.c. and footnote 264, including accompanying discussion on clarifying modifications.

218 *See* final rule 248.30(d)(10).

219 As stated below, this modification from the proposal responds to comments by incorporating into rule text the Commission's intended scope of the "service provider" definition, as discussed in the Proposing Release. *See* discussion on the Service Provider definition *infra* footnote 271, including accompanying

a. Covered Institutions' Incident Response Program Obligations Regarding Service Providers

In a change from the proposed rule, the Commission is adopting the final amendments without requiring covered institutions to enter into a written contract with their service providers.[220] Instead, the final amendments require that a covered institution's incident response program "include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of the covered institution's service providers, including to ensure that the covered institution notifies affected individuals as set forth in paragraph (a)(4)," in the event of a breach at the service provider.[221] Further, while the final amendments do not require covered institutions to enter into a written contract, the final amendments incorporate the protections that would have been required in the proposed written contract[222] by requiring that a covered institution's policies and procedures be reasonably designed to ensure service providers take the appropriate measures to: (A) protect against unauthorized access to or use of customer information, and (B) provide notification to the covered institution in the event of a breach resulting in unauthorized access to a customer information system maintained by the service provider, in accordance with the timing

---

discussion on clarifying modifications. *See also* proposed rule 248.30(e)(10).

220 *See* proposed rule 248.30(b)(5)(i). *See also supra* footnote 213 and accompanying discussion.

221 *See* final rule 248.30(a)(5)(i). In the Proposing Release, we requested comment on whether the proposed written contract requirement should instead require that a covered institution adopt policies and procedures that "require due diligence of or some type of reasonable assurances from its service providers." *See* Proposing Release at section II.A.3. We also encouraged commenters to review our separate proposal to prohibit registered investment advisers from outsourcing certain services or functions without first meeting minimum due diligence and monitoring requirements to determine whether that proposal might affect their comments on the Proposing Release. *See* Proposing Release at section G.2, n.300; *see also* Outsourcing by Investment Advisers, Investment Advisers Act Release No. 6176 (Oct. 26, 2022) [87 FR 68816 (Nov. 16, 2022)]. The due diligence standards we are adopting are intended to address related concerns raised by commenters who requested that we adopt a more principles-based set of requirements.

222 *See supra* footnote 213 and accompanying discussion of the substantive obligations that were included in the proposal's written contract requirement.

and notice trigger conditions discussed further below. Finally, in a modification from the proposal, upon receipt of such notification, a covered institution must initiate its incident response program adopted pursuant to paragraph (a)(3) of this section.[223]

Two commenters expressed varying degrees of support for requiring a written contract between a covered institution and its service providers.[224] One such commenter expressed support for requiring a specific contractual agreement with a service provider, stating that the information covered by the service provider provision is already subject to a contractual agreement between the covered institution and the service provider.[225] The other commenter agreed that service providers should be contractually required to take appropriate risk-based measures and due diligence to protect against unauthorized access to or use of customer information, but suggested that for flexibility in oversight covered institutions should be permitted to rely on "reasonable assurances" from service providers that they have taken appropriate measures to protect customer information.[226]

Several commenters opposed this proposed requirement.[227] Specifically, two commenters asserted that the written contract requirement would harm covered institutions, which may not

---

223 *See* final rule 248.30(a)(5)(i).

224 *See* ICI Comment Letter. While this commenter supported a written contract requirement, it did assert that the Commission should adopt a longer compliance period due to the necessity of renegotiating existing contracts with service providers to align the breach notification provisions in those contracts to the rule's requirements. This comment is separately addressed below. *See also* SIFMA Comment Letter 2.

225 *See* ICI Comment Letter. Specifically, this commenter stated that the information that is covered by proposed rule 248.30(b)(5) "is already subject to a contractual agreement between the covered institution and the service provider." *Id.* This commenter further explained it is opposing the contractual requirement because of its very narrow scope, specifically stating that "as drafted, [the requirement] would only apply to any service provider that receives, maintains, processes, or otherwise is permitted access to customer information through the service provider's provision of services directly to the covered institution." *Id.*

226 *See* SIFMA Comment Letter 2.

227 *See*, *e.g.*, AWS Comment Letter; IAA Comment Letter 1 (stating that [covered institutions] should not be required to enter into written agreements with service providers); Google Comment Letter; STA Comment Letter 2; and CAI Comment Letter (stating that many leading service providers (such as cloud service

have the negotiating power or leverage to demand specific contractual provisions from large third-party service providers, particularly where specific provisions are "inconsistent with the business imperatives" of the service provider and/or in the case of small covered institutions.[228] A number of commenters also suggested alternatives to either adopting a written contract requirement or, if such a requirement is adopted, to mandating specified contractual requirements.[229] Two commenters suggested that rather than requiring specific practices to be included within a written contract, the Commission should structure the final amendments to enable covered institutions to take a risk-based approach to due diligence and third-party risk management that integrates reliance on independent certifications, attestations, and industry standards as a sufficient means of assessing and determining whether the service provider is appropriately addressing these risks to an adequate standard.[230] Meanwhile, another commenter who opposed the contractual requirement suggested the Commission should provide covered institutions with the flexibility to oversee their service providers "based on the nature and size of their businesses and in light of the risks posed by the facts and circumstances."[231] Finally, one

---

providers) do not negotiate the standard terms of their services with customers and those standard terms generally would not meet the proposed contractual requirements).

228 *See* IAA Comment Letter 2; *see also* STA Comment Letter 2.

229 *See* SIFMA Comment Letter 2; AWS Comment Letter; Google Comment Letter; and IAA Comment Letter 1.

230 *See* AWS Comment Letter (suggesting that in order to address the practical difficulties of compliance, the Commission should provide covered institutions with a flexible approach to achieving compliance with the service provider provisions that relies on the use of independent certifications, attestations, and adherence to industry standards); *see also* Google Comment Letter (suggesting that rather than prescribing the specific practices that must be included in the contract, (a) contracts should require service providers to implement and maintain appropriate measures that are consistent with industry standards, and (b) each covered entity should oversee its providers to assess if the provider addresses the relevant practices to an adequate standard—noting this activity can be supported with third party certifications and standards).

231 *See* IAA Comment Letter 1.

commenter suggested that it was unclear how a third-party service provider's notice to a covered institution would affect a covered institution's own obligations.[232]

Eliminating the written contract requirement from the final amendments, while enhancing the policies and procedures obligation, strikes an appropriate balance between providing covered institutions with greater flexibility in achieving compliance with the requirements of this rule within the context of their service provider relationships, while also helping to ensure the investor protections afforded by the final amendments are maintained when covered institutions utilize service providers.

In particular, as adopted, the enhanced policies and procedures obligations will enable covered institutions to identify and utilize the most appropriate means for their business of achieving compliance with the final amendments through policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of their service providers. Providing this flexibility will help address commenters' concerns about imposing a written contractual agreement for covered institutions, particularly those that are small entities, which may not have sufficient negotiating power or leverage to demand specific contractual provisions from a large third-party service provider. At the same time, the enhanced policies and procedures requirements will provide for effective safeguarding of customer information when it is received, maintained, processed, or otherwise accessed by a service provider, as well as timely notice to customers affected by a breach at a covered institution's service provider, by requiring that the policies and procedures be reasonably designed to: (1) require oversight, including through due diligence and monitoring, of service providers, including to ensure that the covered institution notifies affected individuals as required in paragraph (a)(4) and (2) ensure service

---

232 *See* ACLI Comment Letter.

providers take appropriate measures to protect against the unauthorized access to or use of customer information and provide covered institutions with timely notification of a breach so that the covered institution can carry out their incident response program.

While the final amendments thus provide increased flexibility as to a covered institution's means of overseeing its service providers, the modification the Commission is making at adoption does not lower the standard of a covered institution's substantive oversight obligations. Some covered institutions may find that such oversight can be accomplished more easily and less expensively through less formal arrangements in certain circumstances, based on the covered institution's relationship with its service provider, as well as the scope of the services that are now or will be provided over the course of the relationship.[233] However, regardless of the means and arrangements employed, the covered institution must ensure that any service provider it decides to utilize takes appropriate measures to (A) protect against unauthorized access to or use of customer information, and (B) provide breach notifications to the covered institution as required by these final amendments.

Further, while it may be helpful to a covered institution in achieving compliance with the final amendments to receive "reasonable assurances" from its service providers that they have taken appropriate measures to both protect customer information and provide timely notification to the covered institution in the event of a relevant breach of the service provider's customer information systems, reliance solely on such assurances may be insufficient depending on the facts and circumstances, for example when a covered institution knows, or has reason to know, that such assurance is inaccurate. Instead, the final rules require the establishment, maintenance,

---

[233] Although a written contract is not required under the final amendments, covered institutions should generally consider whether a written contract that memorializes the expectations of both covered institutions and their service providers is appropriate.

and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of the service provider to ensure the covered institution will be able to satisfy the obligations of paragraph (a)(4). Further, covered institutions generally should consider reviewing and updating these policies and procedures periodically throughout their relationship with a service provider, including updates designed to address any information learned during the course of their monitoring.

The final amendments provide covered institutions with flexibility in overseeing their service provider relationships, while helping to ensure the additional investor protections intended by these final amendments are still achieved. Consistent with this risk-based approach, covered institutions may wish to consider employing such tools as independent certifications and attestations obtained from the service provider, as suggested by some commenters, as part of their policies and procedures to require oversight, including through due diligence and monitoring, of the service provider. However, the covered institution's written policies and procedures must be reasonably designed under the circumstances, and the covered institution's oversight of its service providers pursuant to those written policies and procedures generally should be tailored to the facts and circumstances of the two parties' relationship, which may or may not include the use of such tools.

Further, as stated above, we are modifying the proposed rule to state that upon a covered institution's receipt of a service provider's notification, the covered institution must initiate its incident response program required by paragraph (a)(3) of the rule.[234] The Commission is adopting this modification in response to comment requesting clarification of a covered

[234] *See* final rule 248.30(a)(5)(i).

institution's obligations upon receipt of service provider breach notifications.[235] Further, this modification helps further align the final amendments with the intended purpose of the service provider's breach notifications, as discussed in the Proposing Release.[236] While receipt of such notice automatically triggers the covered institution's obligation to initiate the procedures of its incident response program, such notice is not a necessary predicate to trigger this obligation for incidents occurring at the service provider. A covered institution also must initiate its incident response program where the covered institution has otherwise independently detected an incident of unauthorized access to or use of customer information at the service provider.[237]

Finally, some commenters asked that we consider making any new obligations with respect to a written contract requirement forward-looking so as not to disrupt contracts already in existence by requiring renegotiation, and that we should further extend the compliance date to address this.[238] As we are adopting the rule without a written contract requirement, these comments have become moot.[239]

b. Deadline for Service Provider Notice to Covered Institutions and Notice Trigger

As described above, the final amendments require that a covered institution's policies and procedures be reasonably designed to ensure service providers take appropriate measures to provide covered institutions with notice "as soon as possible, but no later than 72 hours after

---

235 *See* ACLI Comment Letter.

236 This modification is consistent with the intended purpose of this notification, as discussed in the Proposing Release. *See* Proposing Release at Section II.A.3 stating that the purpose of breach notifications to be provided by service providers to a covered institution is "to enable the covered institution to implement its incident response program expeditiously."

237 *See* final rule 248.30(a)(3). *See also* discussion on covered institutions' required Incident Response Program Including Customer Notification *supra* Section II.A.

238 *See*, *e.g.,* Computershare Comment Letter; Google Comment Letter; ICI Comment Letter.

239 *See* discussion of compliance date *infra* section II.F.

becoming aware of a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider."[240] This modification extends the proposed timeframe for service providers to provide such notice to 72 hours, but maintains the proposed notice triggering event to initiate this timeframe of the service provider becoming aware of a breach."[241]

Commenters addressed both the notification deadline and the triggering event for notifications to be provided by service providers to covered institutions in the event of a relevant breach involving unauthorized access to a customer information system maintained by the service provider. As to the notification deadline, one commenter supported requiring service providers to notify a covered institution within 48 hours of a breach impacting the covered institution or affected individuals, stating its understanding is that this is "not an uncommon arrangement" today between covered institutions and service providers maintaining their nonpublic personal information (e.g., between investment companies and transfer agents).[242] Another commenter raised concerns that a standard of "as soon as possible, but no later than 48 hours after becoming aware of a breach," when paired with a written contract requirement, might impose formidable challenges to covered institutions in mandating such contractual provisions with service providers who are not explicitly subject to Commission jurisdiction, and may have their own policies and procedures addressing breaches.[243] Several commenters suggested the

---

240 *See* final rule 248.30(a)(5)(i). In the proposed rule, such notice would have been required "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." *See* proposed rule 248.30(a)(5)(i).

241 *See* Proposing Release at section II.A.3.

242 *See* ICI Comment Letter.

243 *See* Computershare Comment Letter.

Commission adopt a 72-hour notification deadline.[244] In particular, one such commenter stated that this notification provision should be extended to "as soon as possible but no later than 72 hours," to harmonize the Commission's standard with a number of related Federal, State, and international regulatory deadlines governing required service provider notification to financial institutions in the event of a cyber incident, and also further the White House's and Congress's express policy of harmonizing cyber incident reporting requirements.[245] Finally, this commenter stated that a consistent 72-hour reporting deadline would promote more effective cybersecurity incident response and cyber threat information sharing than shorter, or varied reporting periods, and that a 48-hour deadline in the commenter's experience would lead to "premature reporting" that increases the likelihood of reporting inaccurate or incomplete information and tends to create confusion and uncertainty.[246]

In contrast, some commenters recommended modifying the proposal to remove any specified duration for a reporting deadline.[247] Several commenters suggested that rather than an inflexible time deadline, the Commission should require that notification be provided without

---

244 *See* Letter from Microsoft Corporation (June 5, 2023) ("Microsoft Comment Letter"); AWS Comment Letter (this commenter "encourage[d] the Commission" to consider a longer reporting deadline than 48 hours to "support the dedication of resources needed to discover and mitigate potential harm caused by an incident," and highlighted the 72-hour reporting timeframe that "CIRCIA contemplates…for national critical infrastructure, including the financial services sector" in the alternative.).

245 *See* Microsoft Comment Letter (explaining that use of this 72-hour reporting deadline would align the SEC's rules with other notification requirements that may apply to entities covered by the Proposed Rules, and identifying additional authorities that use the 72-hour deadline, such as the CIRCIA, Pub. L. No. 117-103, 136 Stat. 49 (2022); Executive Order 14028, "Improving the Nation's Cybersecurity," 86 FR 26,633 (May 12, 2021), directing the Federal government to incorporate a 72-hour reporting period into the Federal Acquisition Regulation ("FAR"); the Defense Federal Acquisition Regulation Supplement ("DFARS"), 48 CFR 204.7302(b) and 252.204-7012(c); the New York State Department of Financial Services' ("NYDFS") Cybersecurity Requirements for Financial Service Companies, 23 NYCRR § 500.17(a); the European Union's General Data Protection Regulation ("GDPR"), Regulation (EU) 2016/679; and Article 23 of the EU's new Network and Information Security Directive ("NIS 2 Directive"), Directive (EU) 2022/2555).

246 *Id*.

247 *See, e.g.*, Schulte Comment Letter; SIFMA Comment Letter 2.

unreasonable delay after a reasonable investigation has been performed by the service provider.[248] Another commenter stated that rather than mandating any form of a deadline, the time period should be left to covered institutions and service providers to negotiate, accounting for the nature of services and customer data.[249]

As to the triggering event requiring service providers to notify covered institutions of a relevant breach, one commenter urged the Commission to shift from the service provider "becoming aware" of a breach that entailed unauthorized access to customer information, to the service provider "determining" that such a breach had occurred.[250] This commenter asserted that the process of "becoming aware" will involve time and resources to investigate and that changing to a "determining" standard may minimize pressure on the service provider to report prior to performing sufficient investigation, while helping harmonize regulatory approaches across the financial sector, as it would align with similar requirements adopted by Federal banking agencies related to notice provided by bank service providers.[251] Another commenter stated the Commission should, in addition to shifting to a 72-hour reporting deadline, amend the

---

248 *See*, *e.g.,* SIFMA Comment Letter 2 (stating this modification would harmonize with the Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 FR 38182, 38184 (proposed July 19, 2021)); ACLI Comment Letter (stating this modification would harmonize service provider and covered entity requirements); and Federated Comment Letter.

249 *See* Schulte Comment Letter. This commenter stated that by mandating a 48-hour limit, service providers would be "left with the impractical challenge of allocating resources to making disclosures to counterparties (i) when resources could be better allocated to identifying and containing the scope of the data breach, and (ii) before the service provider has a complete picture of the impact of a data breach." *See id.*

250 *See* Google Comment Letter.

251 *See* Google Comment Letter (referencing Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, *available at*: fdic.gov/news/board-matters/2021/2021-11-17-notational-fr.pdf?source=govdelivery&utm_medium=email&utm_source=govdelivery).

trigger initiating this reporting deadline to the moment the service provider "has a reasonable basis to conclude that a notifiable incident has occurred or is occurring."[252]

Other commenters suggested narrowing the scope of incidents that would trigger required notice by service providers to a covered institution.[253] One commenter asserted that incident response program requirements should only address and be triggered by incidents that involve unauthorized access to or use of a subset of customer information (e.g., *sensitive* customer information).[254] Another commenter stated that the proposal would result in notices to a covered institution if there has been unauthorized access to the service provider's customer information system, regardless of whether the covered institution's customers were in any way affected by the breach.[255] Instead, the commenter stated that the Commission should limit the scope of incidents requiring notification to a covered institution to only those resulting in unauthorized access to that covered institution's "customer information" maintained by the service provider.[256]

After consideration, the Commission is extending the deadline for providing notification from 48 to 72 hours. Although we appreciate that the 48-hour standard in the proposed amendments may not be an uncommon arrangement between covered institutions and their service providers in the market today, extending this deadline by 24 hours will provide service providers with additional time to conduct more effective investigations of a breach at the service provider, resulting in more relevant and accurate notifications to the covered institution. Further, the 72-hour standard brings this notification deadline in alignment with other existing regulatory

---

252 *See* Microsoft Comment Letter.

253 *See* Schulte Comment Letter; SIFMA Comment Letter 2.

254 *See* Schulte Comment Letter.

255 *See* SIFMA Comment Letter 2.

256 *See id.*

standards, which should reduce costs to service providers and covered institutions without sacrificing the investor protection benefits of the rule.[257]

The Commission disagrees that there should be no specified notification deadline and that covered institutions and service providers should be able to negotiate the appropriate timing for such notification. As discussed above, upon receipt of the breach notification from the service provider, a covered institution must initiate its incident response program adopted pursuant to paragraph (a)(3) of the final amendments.[258] As covered institutions cannot reasonably be expected to initiate their incident response programs for incidents occurring at a service provider that the covered institution is not yet aware have occurred, providing the indefinite timeline commenters suggest could significantly hinder the effectiveness of covered institutions' incident response programs.[259] For example, delays in the service provider's notification to the covered institution of a breach could result in further delays in the initiation of the incident containment and control procedures the covered institution has adopted pursuant to its incident response program obligations, consequently diminishing their effectiveness. Further, any excess delay in the service provider's notification to the covered institution and resulting delay in the covered

---

257 As discussed above, a 72-hour reporting deadline aligns with, among others, requirements in CIRCIA that include a 72-hour deadline for entities to report cyber incidents to CISA, Executive Order 14028 on "Improving the Nation's Cybersecurity," which directs the Federal government to incorporate a 72-hour reporting period into the FAR, the DFARS, NYDFS's cybersecurity regulations, which include a 72-hour reporting deadline to NYDFS after any determination that a cybersecurity incident has occurred at the covered entity, its affiliates, or a third-party service provider, the European Union's GDPR, as well as the European Union's NIS 2 Directive. *See* discussion of Microsoft Comment Letter and cited regulatory frameworks *supra* footnote 245.

258 *See supra* footnote 237 and accompanying discussion.

259 While a covered institution's receipt of such notice from a service provider establishes such awareness, as discussed above, where a covered institution has otherwise independently detected an incident of the unauthorized access to or use of customer information at the service provider, it must implement its incident response program under paragraph (a)(3) of the final amendments regardless of any notice provided by the service provider. *See supra* footnote 237 and accompanying discussion. *See also* final rule 248.30(a)(3).

institution's initiation of its incident response program, could significantly hinder the goal of the final amendments of providing customers with timely notification of data breaches so that they may take remedial action. In light of this, reasonably designed policies and procedures generally should also account for instances where the covered institution determines that a service provider has failed to provide notice to the covered institution within 72 hours as required. In such circumstances, in addition to initiating its incident response program upon receipt of the notice as required, a covered institution generally should reevaluate its policies and procedures governing its relationship with the service provider and make adjustments as necessary to ensure the service provider will take the required appropriate measures going forward.

Further, the Commission is adopting as proposed the "becoming aware of" standard for triggering a service provider's breach notifications to a covered institution. This standard is intended to enable the covered institution to implement its incident response program expeditiously. While the Commission believes it is appropriate, as discussed above, to extend the timeframe for service provider notifications from 48 to 72 hours, adopting either a "having a reasonable basis to conclude" standard or a "determining" standard could frustrate the investor protection goals of these final amendments. Specifically, adopting either of these alternative standards could result in undue delays in a service provider's notification to the covered institution beyond the point at which the service provider is already aware that a relevant breach has occurred. Such a delay would frustrate the goal of both enabling covered institutions to initiate their incident response program expeditiously, as well as the goal of providing timely notification to affected individuals. For similar reasons, given that the "determining" standard used by Federal banking regulators involves a different context—notice to the banking organization of downgraded or degraded services—adopting it here solely to harmonize

regulatory approaches would be inappropriate.[260] Accordingly, the final amendments maintain the proposed "becoming aware of" standard for triggering a service provider's notification.

The Commission also is not limiting the scope of incidents to be reported to covered institutions to only those involving "sensitive customer information" or alternatively to breaches that result in unauthorized access to "customer information" maintained by the service provider rather than those that result in unauthorized access to a service provider's "customer information system." Under the final amendments, a covered institution's incident response program must be reasonably designed to "detect, respond to, and recover from unauthorized access to or use of customer information," and must include provisions to assess such incidents to "identify the *customer information systems* and *types of customer information* that may have been accessed or used without authorization" and take appropriate steps to "contain and control the incident to prevent further unauthorized access to or use of customer information."[261] As discussed above, in doing so, we are requiring that covered institutions' incident response programs address any incident involving customer information—not merely those involving *sensitive* customer information—and also account for the identification of affected customer information *systems* in addition to the types of customer information that may have been accessed or used without authorization.[262] For the same reasons, we are not limiting the scope of reportable incidents to

---

260 Specifically, the Federal banking agency regulations require notification from the bank service provider to "each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to the banking organization for four or more hours." *See* 12 CFR 304.24(a).

261 *See* final rule 248.30(a)(3)(i) and (ii). *See also* discussion of the Assessment and Containment and Control portions of covered institutions' incident response program requirements *supra* sections II.A.1 and II.A.2.

262 *See* discussion of incident response program Assessment and Containment and Control requirements, and the reasons for not restricting such requirements to only "sensitive customer information" *supra* Sections II.A.1 and II.A.2. *See also* discussion of incident response program Containment and Control requirements and the reasons for requiring identification of both the customer information systems as well as types of customer information that may have been accessed or used without authorization *supra* Section II.A.2.

only those breaches in security at the service provider that result in unauthorized access to sensitive customer information, or alternatively to only those breaches that result in unauthorized access to "customer information" maintained by the service provider.

c. Delegation of Notice and Covered Institutions' Customer Notification Obligations

The Commission is adopting as proposed language that permits covered institutions, as part of their incident response programs, to enter into a written agreement with their service providers to notify affected individuals on the covered institution's behalf.[263] However, the Commission is also adopting a new paragraph that states that, notwithstanding any covered institution's use of a service provider, the covered institution's obligation to ensure that affected individuals are notified in accordance with this rule rests with the covered institution.[264]

One commenter stated that it is appropriate to permit a covered institution to enter into a written agreement with its service provider to notify affected individuals on the covered institution's behalf, so long as the notification is actually ultimately provided to customers in a manner that satisfies the covered institution's notice obligations.[265] The Commission agrees that there may be situations where a covered institution's service provider is better situated than the covered institution to provide a customer a breach notification. Thus, the Commission is adopting paragraph (a)(5)(ii) as proposed.[266]

---

263 *See* final rule 248.30(a)(5)(ii) (stating "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 (a)(4) of this section."); *see also* proposed rule 248.30(b)(5)(ii).

264 *See* final rule 248.30(a)(5)(iii).

265 *See* Schulte Comment Letter (stating that if the service provider was the victim of a cyber-attack that included unauthorized access to the covered institution's sensitive customer information, the service provider would be better situated to notify the affected customers).

266 As discussed below *infra* footnote 391 and in the accompanying discussion, in accordance with the recordkeeping provisions adopted in these final amendments, covered institutions, other than funding

At the same time, the Commission is adopting a new paragraph (a)(5)(iii) to specify that even where a covered institution uses a service provider, the obligation to ensure that affected individuals are notified in accordance with the rule rests with the covered institution.[267] While the proposing release included similar language,[268] the final rule explicitly provides that the covered institution will be obligated to satisfy the customer notification requirements of paragraph (a)(4) in the event of a relevant breach occurring at the service provider. The Commission agrees that in providing flexibility to covered institutions by permitting them to enter into a written agreement with their service providers to notify affected individuals on the covered institution's behalf, such notification to customers should be provided in a manner that satisfies the covered institution's notice obligations. Accordingly, where a covered institution has entered into a written agreement with its service provider to provide notice on the covered institution's behalf, the covered institution must ensure that the service provider has satisfied the customer notification obligations.[269] To accomplish this, the covered institution's policies and procedures

---

portals, are required to preserve a copy of any notice transmitted by the service provider to any customer on the covered institution's behalf following the covered institution's determination made regarding whether notification is required pursuant to 17 CFR 248.30(a)(4). *See also* discussion of funding portal recordkeeping requirements *infra* footnote 385.

267 *See* final rule 248.30(a)(5)(iii) (specifically stating "Notwithstanding a covered institution's use of a service provider in accordance with paragraphs (a)(5)(i) and (ii), the obligation to ensure that affected individuals are notified in accordance with paragraph (a)(4) of this section rests with the covered institution").

268 In the proposal, the Commission stated that in such a circumstance where the covered institution has delegated performance of its notice obligation to a service provider through written agreement, the covered institution would remain responsible for any failure to provide a notice as required by the proposed rule. *See* Proposing Release at II.A.3. The Commission also stated in the proposal that 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, but covered institutions would remain responsible for these functions even if they are delegated to service providers. *See id.* at footnote 93; *see also* discussion of paragraph (a)(4) customer notification obligations *supra* section II.A.3. Under new paragraph (a)(5)(iii), covered institutions may still delegate such functions to service providers as stated in the proposal, but the rule text expressly states that the ultimate obligation to ensure affected individuals are notified in accordance with paragraph (a)(4) will remain with the covered institution.

269 *See* final rule 248.30(a)(5)(iii); *see also* final rule 248.30(a)(4) (enumerating the scope of the covered institution's customer notification obligations).

should consider including steps for conducting reasonable due diligence to confirm that the service provider has provided notice to affected customers. In addition to maintaining a copy of any notice transmitted to affected individuals by the service provider on the covered institution's behalf as required by the covered institution's (other than funding portals) recordkeeping obligations under the final amendments,[270] effective due diligence might also include obtaining confirmation of delivery of such notification in the form of attestations or certifications made by the service provider. Covered institutions could also consider confirming with a sample of affected customers that they received such service provider notifications.

In addition, where the covered institution has entered into a written agreement with its service provider to provide notice on the covered institution's behalf pursuant to paragraph (a)(5)(ii), and the covered institution determines that the service provider has not provided such notifications in a manner that satisfies the conditions of paragraph (a)(4), the covered institution must still ensure that notification is provided to the customer, and the covered institution's policies and procedures generally should be designed to address these instances. To accomplish this, the covered institution generally should conduct timely due diligence to identify any lack of notification by the service provider to the customer and remedy the matter in advance of the deadline set out in paragraph (a)(4).

d. Service Provider Definition

The Commission is adopting the definition of "service provider" to mean "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer

---

[270] *See, e.g.* final rule 17 CFR 240.17a-4(e)(14)(iii). *See also* discussion on a covered institution's recordkeeping obligations as to notices delivered to customers by its service providers *infra* footnote 391 and accompanying discussion. Funding portals generally should maintain all copies of such notices in connection with their own requirements to demonstrate compliance with Regulation S-P. *See* discussion of existing funding portal recordkeeping obligations *infra* footnote 385.

information through its provision of services directly to a covered institution."[271] This definition thereby includes affiliates of covered institutions if they are permitted access to this information through their provision of services. The scope of this definition is intended to help protect against the risk of harm that may arise from service providers' access to a covered institution's customer information and customer information systems.[272]

A number of commenters addressed the scope of the proposed definition. Several commenters suggested narrowing the scope of the service provider definition by revising it to exclude affiliates or other GLBA regulated entities.[273] Similarly, three commenters asserted that the Commission should revise the definition to exclude affiliates and other entities under common control with the covered institution, as those affiliates are typically subject to the same cybersecurity and privacy programs, including service provider management, which are frequently structured and operate on a group-wide basis.[274] One of these commenters also stated the Commission should also exclude entities subject to the GLBA that have direct contractual relationships with the client.[275] This commenter separately asserted that the service provider definition should be narrowed to only cover those persons or entities that are a third party and receive, maintain, process, or otherwise are permitted access to *sensitive* customer information, so that covered institutions can prioritize "higher-risk service providers" and not expend

---

271 *See* final rule 248.30(d)(10); *see also* proposed rule 248.30(e)(10).

272 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 had incorporated requirements related to cybersecurity risk into their contracts with vendors and business partners. *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.

273 *See*, *e.g.*, CAI Comment Letter; IAA Comment Letter 1; SIFMA Comment Letter 2; and Schulte Comment Letter.

274 *See* CAI Comment Letter; IAA Comment Letter 1, SIFMA Comment Letter 2.

275 *See* IAA Comment Letter 1.

resources unnecessarily on an overly broad set of service providers.[276] Finally, one commenter requested that the Commission "clarify the scope of the service provider definition, including whether service providers would include financial counterparties such as brokers, clearing and settlement firms, and custodial banks."[277]

As stated above, we are modifying the definition of service provider from the proposal to remove reference to third parties in response to commenters to incorporate into rule text the Commission's intended scope of the "service provider' definition, as discussed in the Proposing Release.[278] It would not be appropriate to narrow the definition to exclude affiliates or non-affiliates that are also subject to the GLBA, as commenters have suggested. While a covered institution's affiliates may collectively operate under the same cybersecurity and privacy programs, such uniformity in approach does not diminish the risk of harm to the institution's customers in the event of a cyber incident involving unauthorized access to or use of customer information at the affiliate.[279] This risk is similarly not diminished where a cyber incident involving unauthorized access to or use of customer information occurs at a covered institution's unaffiliated service provider that is subject to the GLBA, even where the service provider has a direct contractual relationship with the client. In such instances, maintaining such an entity's inclusion within the service provider definition will help ensure that the covered institution is

---

276 *See id.*

277 *See* SIFMA Comment Letter 2.

278 *See* Proposing Release at Section II.A.3, stating "This definition would include affiliates of covered institutions if they are permitted access to this information through their provision of services."

279 While we are not narrowing the service provider definition to exclude affiliates of the covered institution, in most instances it generally should be appropriate for the covered institution to rely upon the adherence of any affiliated service provider to enterprise-wide cybersecurity and privacy programs that cover both the covered institution and its affiliates, so long as such programs satisfy the requirements of the final rules and the covered institution does not know, or have reason to know, that the affiliate is not adhering to such enterprise-wide programs.

made aware of cyber incidents that occur at the service provider to aid in both the covered institution's oversight of its service providers, as well as satisfaction of its customer notification and broader customer information safeguarding obligations under the final amendments. It is thus important for the service provider definition to remain sufficiently broad to address these risks by setting out clear obligations for all parties possessing legitimate access to customer information regarding both the safeguarding of that information, and, where necessary, ensuring notification to the affected customers in the event of a breach involving unauthorized access to or use of customer information. However, while we are not narrowing the scope of the "service provider" definition to exclude either affiliates of the covered institution or unaffiliated service providers that are independently subject to the GLBA, pursuant to paragraph (a)(5)(ii) of these final amendments the covered institution and a service provider may enter into a written agreement for the service provider to notify affected individuals on its behalf in in the event of a breach at the service provider, as discussed above. [280]

Further, it would not be appropriate to narrow the service provider definition to only address those persons or entities that operate as "higher-risk service providers" that receive, maintain, process, or are otherwise permitted access to *sensitive* customer information, as one commenter suggested. As discussed above, the scope of information covered by the assessment and containment and control requirements of the final amendments is designed to help ensure all information covered by the requirements in the GLBA is appropriately safeguarded, and that

---

[280] *See* discussion on Delegation of Notice and Covered Institutions' Customer Notification Obligations *supra* Section II.A.4.c. *See also* 17 CFR 248.30(a)(5)(ii). The permissibility of such written agreements between covered institutions and their service providers, including both their affiliates and those unaffiliated service providers that are also subject to the GLBA, may also help reduce costs related to customer notifications at the covered institution, and help reduce the risk of over-notification of affected individuals in instances where both the covered institution and its affiliated service provider are independently subject to customer notification obligations for the same breach in security.

sufficient information is assessed to fulfill the more narrowly tailored obligation to notify affected individuals.[281] Specifically, consistent with the GLBA, the final amendments are tailored to require that a covered institution's written policies and procedures must be reasonably designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer, not merely all *sensitive* customer information.[282] Narrowing the service provider definition in a manner that would fail to cover the full scope of information that the GLBA requires to be covered in a covered institution's safeguarding policies and procedures, as would result from commenters' suggestion, would be inappropriate.[283] Further, we are also concerned that limiting the service provider definition to only address those persons or entities that receive, maintain, process, or are otherwise permitted access to sensitive customer information, as commenters suggest, would result in insufficient notification to covered institutions in the event of a breach at a service provider. The purpose of this service provider notification is to enable the covered institution to begin carrying out its

---

281 *See* discussion on Incident Response Program Including Customer Notification *supra* Section II.A.

282 *See* 17 CFR 248.30(a)(2)(iii). *See also* 15 U.S.C. 6801(b)(3) (mandating that the Commission shall establish appropriate standards for the financial institutions subject to its jurisdiction relating to administrative, technical, and physical safeguards "to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.").

283 As discussed below, the definition of "customer information" we are adopting in these final amendments is intended to ensure that the standard for covered institutions' safeguards rule policies and procedures is consistent with the objectives of the GLBA, which focuses on protecting "nonpublic personal information" of those who are "customers" of financial institutions. See discussion on the Definition of Customer Information *infra* Section II.B.1. *See also* 17 CFR 248.30(d)(5) (defining "customer information"). In contrast, the definition of "sensitive customer information" that we are adopting is more narrowly tailored to only cover 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. *See* 17 CFR 248.30(d)(9)(i). As discussed above, this definition is more narrowly tailored, and has been specifically calibrated to include types of information that, if exposed, could put affected individuals at a higher risk of suffering substantial harm or inconvenience through, for example, fraud or identity theft enabled by the unauthorized access to or use of the information. See discussion on the Definition of "Sensitive Customer Information" *supra* Section II.A.3.b. The narrower tailoring than is used in the "customer notification" definition is intended to protect customers by ensuring that they can take the necessary steps to minimize their exposure to these risks, while also being mindful of concerns of how a broader definition could increase the potential for over-notification of customers to address such risks. *See id*.

response program, which requires an assessment of the nature and scope of any incident involving unauthorized access to or use of customer information, not merely those involving sensitive customer information.[284] For these reasons, the Commission is adopting the service provider definition as modified.

The Commission also acknowledges the request to clarify the scope of what is included within the service provider definition, including "whether service providers would include financial counterparties such as brokers, clearing and settlement firms, and custodial banks." In alignment with the service provider definition we are adopting, covered institutions should make this determination based on the facts and circumstances about the substance of the relationship with the covered institution, rather than the form of the entity in question. Where financial counterparties receive, maintain, or otherwise are permitted access to customer information through the provision of services directly to the covered institution, they meet the service provider definition as adopted.

B. Scope of Safeguards Rule and Disposal Rule

1. Scope of Information Protected

We are adopting amendments to rule 248.30 that define the scope of information covered by the safeguards and disposal rules. These amendments will broaden and more closely align the scope of both rules by applying them to the information of not only a covered institution's own customers, but also the customers of other financial institutions that has been provided to the covered institution.[285] These amendments further specify that the rules also apply to customer

---

284 *See* final rule 248.30(b)(i). *See also* discussion on the assessment required by paragraph (a)(3) as to a covered institution's incident response program *supra* section II.A.1 above.

285 Final rule 248.30(a), (b), and (d)(5)(i). 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)). 17 CFR 248.3(n).

information handled or maintained on behalf of the covered institution.[286] We are adopting these changes substantively as proposed, with changes to the structure of the rule in response to comments as discussed in more detail below.

Specifically, the amendments:

- Adopt a new definition of "customer information" defining the scope of information covered by both the safeguards and disposal rules. These amendments provide greater specificity regarding what constitutes customer information that must be protected under the safeguards rule. They also expand the scope of the disposal rule, which currently applies only to consumer information (defined as "consumer report information" in the current rule) so that it applies to both customer and consumer information.
- Provide that customer information protected under both the safeguards and disposal rules includes both customer information in the possession of a covered institution as well as customer information handled or maintained on its behalf.
- Provide that both customer and consumer information include information that pertains to individuals with whom the covered institution has a customer relationship, as well as to the customers of other financial institutions where such information has been provided to the covered institution. We are adopting this expansion as proposed but, as discussed below, have reorganized the rule provisions effectuating the change in response to comments.

Definition of Customer Information

[286] Final rule 248.30(d)(5)(i).

Currently, Regulation S-P's protections under the safeguards rule and disposal rule apply to different, and at times overlapping, sets of information.[287] Specifically, as required under the GLBA, the safeguards rule currently 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,"[288] 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.[289]

To align more closely the information protected by both rules, as proposed, we are amending 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. For covered institutions other than transfer agents, the term "customer information" will mean, as proposed, "any record containing nonpublic personal information as defined in section 248.3(t) about a customer of a financial institution, whether in paper, electronic, or other form."[290]

---

287 *See* Disposal of Consumer Report Information, Investment Company Act Release No. 26685 (Dec. 2, 2004) [69 FR 71322 (Dec. 8, 2004)], at n.13 ("Disposal Rule Adopting Release").

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

289 *See* 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," defined 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" had 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 amending 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); OCC Information Security Guidance at I.C.2.b; FRB Information Security Guidance") at I.C.2.b; FDIC Information Security Guidance at I.C.2.b.

290 As discussed below, the customer information definition also specifies that the definition covers information in the possession of a covered institution or that is handled or maintained by the covered

Commenters did not object to the proposed definition of "customer information." As discussed in the Proposing Release, the customer information 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.[291] The customer information definition is also based on the definition of "customer information" in the safeguards rule adopted by the FTC.[292]

Additionally, adding customer information to the coverage of the disposal rule is also 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.[293] The final amendments specify that this obligation continues through disposal of customer information. The final amendments also are consistent with the objectives of the FACT Act, which focuses on protecting "consumer information," a category of information that will remain within the scope of the disposal rule.[294] Adding customer information to the disposal provisions will simplify compliance with the FACT Act by eliminating a covered institution's

---

institution or on its behalf, regardless of whether such information pertains to individuals with whom the covered institution has a customer relationship or the customers of other financial institutions where such information has been provided to the covered institution. This is being adopted substantively as proposed, but reflects structural modifications to the rule text to address the concerns of a commenter who asked for increased clarity. *See infra* section II.B.2 for a discussion of the term customer information with respect to transfer agents.

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

292 *See* 16 CFR 314.2(d) (The 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 final amendments do not require covered institutions to be responsible for their affiliates' policies and procedures for safeguarding customer information because covered institutions affiliates generally are financial institutions subject to the safeguards rules of other Federal financial regulators.

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

294 *See* 15 U.S.C. 1681w(a)(1); 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."

need to determine whether its customer information is also consumer information subject to the disposal rule. Covered 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.[295] Commenters did not address the expansion of the disposal rule to cover customer information.

One commenter sought clarification regarding the proposal's coverage of customer information handled or maintained on behalf of a covered institution. This commenter stated that proposed paragraph (a) of rule 248.30, which set out the scope of information collectively covered under the safeguards and disposal rules, could be interpreted to limit the application of the rules to customer information in the possession of the covered institution, while proposed paragraph (e)(5) defined customer information to include information that is handled or maintained on behalf of the covered institution. The proposal included both customer information in the possession of a covered institution as well as customer information handled or maintained on its behalf in both the safeguards and disposal rules. This is because rule 248.30 provided the rules applied to "customer information" and, as the commenter observed, the proposal defined customer information to include "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

---

[295] *See*, *e.g.*, OCC Information Security Guidance (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 (similar Federal Reserve Board provisions for state member banks). *See also* 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(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).

behalf." Applying these rules to information handled or maintained on behalf of a covered institution is necessary so that the incident response program applies to information about a covered institution's customers that is handled or maintained by a service provider on the covered institution's behalf and to require that such information is disposed of properly.

In response to this comment, we have removed the dedicated scope paragraph (a) from the proposed rule and moved all the requirements for customer information and consumer information into the definitions of those terms, now in renumbered paragraphs (d)(5)(1) and (d)(1) respectively. Accordingly, and substantively as proposed, the definition of consumer information covers information that a covered institution maintains or otherwise possesses for a business purpose, and the customer information definition covers information in the possession of a covered institution or that is handled or maintained by the covered institution or on its behalf.[296] These structural changes do not change the scope of the proposed rule, but rather consolidate in each definition the scope of covered information as opposed to referring to information possessed by a covered institution in one paragraph of the rule and referring to information handled on its behalf in another.

[296] We also eliminated language in paragraph (b)(1) that now appears in the final amendments' definitions of customer information and consumer information.

Safeguards Rule and Disposal Rule Coverage of Customer Information

We also are adopting the requirement, substantively as proposed, that both the safeguards rule and the disposal rule apply to the information specified in those definitions regardless of whether such information pertains to (a) individuals with whom the covered institution has a customer relationship or (b) the customers of other financial institutions where such information has been provided to the covered institution.[297] As discussed above, however, we are structurally reflecting this requirement in the definitions of customer information and consumer information, rather than in proposed paragraph (a).

Comments were mixed on expanding the safeguards and disposal rules to cover nonpublic personal information received by covered institutions from third party financial institutions. Some commenters supported the expansion.[298] Two of these commenters stated that sensitive nonpublic information should be protected regardless of how it came into a covered institution's possession.[299] Other commenters opposed the proposed expansion, suggesting that the rules should be limited to the customer information of the covered institution's own customers and stating that the safeguards rule in its current form is appropriately calibrated.[300] One of these commenters stated that requiring notification of customers of other financial institutions under the proposed expansion would be confusing to customers and impractical for covered institutions.[301]

---

297 The safeguards rule is applicable to "consumer information" only to the extent it overlaps with "customer information." *See supra* footnote 291. 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).

298 *See* EPIC Comment Letter; ICI Comment Letter; Better Markets Comment Letter.

299 *See* ICI Comment Letter; Better Markets Comment Letter.

300 *See* SIFMA Comment Letter 2; CAI Comment Letter.

301 *See* SIFMA Comment Letter 2; *see also supra* footnote 110 and accompanying text.

After considering comments, the final amendments 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 another financial institution about that institution's customers. Currently, in contrast, 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. The final amendments better align the scope of the safeguards and disposal rules by requiring that a covered institution protect the information of individuals even if those individuals are not customers of that particular institution but customers of another financial institution.

The amendments also are designed to help ensure that the nonpublic personal information of covered institution customers is better protected from unauthorized disclosure on an ongoing basis, regardless of what entity is maintaining or handling that information.[302] For example, information that a registered investment adviser has received from the custodian of a former client's assets would be covered under both the safeguard and disposal 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.[303] Applying the safeguards rule and the disposal rule to customer information that a covered institution receives

---

302 *See* Proposing Release at the text accompanying nn.156-158.

303 *See* final rule 248.30(d)(5)(i) (customer information is covered by the rule if it pertains to "the customers of other financial institutions where such information has been provided to the covered institution").

from other financial institutions will help ensure customer information safeguards are not lost because a third party financial institution shares that information with a covered institution.

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

As discussed in more detail below, the final amendments, which are the same as proposed except for the modifications to the structure of the rules discussed above,[304] extend both the safeguards rule and the disposal rule to apply to any transfer agent registered with the Commission or another appropriate regulatory agency.[305] We are extending these provisions to transfer agents because, as discussed in the Proposing Release, transfer agents maintain sensitive, detailed information related to securityholders.[306] Like other market participants, systems maintained by transfer agents are subject to threats and hazards to the security or integrity of those systems. Likewise, the individuals whose information is maintained by those transfer agents' systems are subject to similar risks of substantial harm and inconvenience as individuals whose customer information is maintained by other covered institutions. Yet, prior to the amendments, the safeguards rule did not apply to any transfer agents, and the disposal rule applied only to those transfer agents registered with the Commission. To address these risks, and help ensure that individuals whose customer information is held by a transfer agent are protected and receive appropriate notice of a breach in the same manner as individuals whose customer information is held by any other covered institution, the final amendments apply both the safeguards rule and the disposal rule to all transfer agents, even if the transfer agent is registered

---

304 *See supra* section II.B.1 (discussing the changes to the structure of final rule 248.30(d)).

305 The term "transfer agent" is defined by rule 248.30(d)(12) to have the same meaning as in section 3(a)(25) of the Exchange Act (15 U.S.C. 78c(a)(25)).

306 *See* Proposing Release at section II.C.3.

with another appropriate regulatory agency. The final amendments do this by including "transfer agents registered with the Commission or another appropriate regulatory agency" in the definition of a "covered institution," in the same manner as we proposed.[307]

As proposed, the final amendments also account for the fact that transfer agents' clients generally are the issuers whose securities are held by investors, not the individual investors themselves, by defining "customer" with respect to a transfer agent registered with the Commission or another appropriate regulatory agency as any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent. Some commenters supported extending these rules to all transfer agents. These commenters stated that doing so would: (i) be consistent with current market practice; (ii) benefit investors; and (iii) create a single, equal standard for all transfer agents.[308] Other commenters opposed extension of the safeguards rule and disposal rule to all transfer agents. In general, these commenters stated that doing so would: (i) exceed the scope of the Commission's authority; (ii) fail to recognize that a transfer agent's customer is an issuer of securities; (iii) potentially conflict with state law; (iv) confuse securityholders; and (v) impose unnecessary costs on transfer agents.[309] As discussed below, the Commission agrees with the commenters who supported extending the safeguards rule and disposal rule to all transfer agents and is adopting the amendments as proposed.

Extending to all Transfer Agents, Including Transfer Agents Subject to Existing Federal and State Requirements, and Scope of the Commission's Authority

---

307 Final rule 248.30(d)(3).

308 *See* Better Markets Comment Letter, ICI Comment Letter 1, EPIC Comment Letter.

309 *See* SIFMA Comment Letter 2, Comment Letter from the Securities Transfer Association (May 10, 2023) ("STA Comment Letter 1"), STA Comment Letter 2, Computershare Comment Letter.

We received some comments in support of our proposed extension of scope to include transfer agents. One commenter stated that extending the protections of the safeguards rule and the disposal rule to all transfer agents would benefit the public and protect investors, due to the sensitive information they possess, and would equalize the standards that are applicable to transfer agents.[310] This commenter stated that due to their role, transfer agents have information related to securityholders that may include names, addresses, phone numbers, email addresses, employers, employment history, bank account information, credit card information, transaction histories, and securities holdings.[311] This commenter further stated that the systems transfer agents maintain are subject to the same risks of a breach as other covered institutions, and therefore the individuals whose customer information transfer agents maintain are subject to the same risks as customers of other covered institutions.[312] Finally, the commenter stated that extending the safeguards rule and disposal rule to all transfer agents will promote regulatory parity and fair competition among firms, regardless of their registration status.[313]

Similarly, one commenter supported including transfer agents and requiring breach notifications,[314] and another commenter stated that establishing incident response and minimum data breach reporting requirements for transfer agents would be a significant step toward a stronger and more comprehensive national data breach regime.[315]

Other comments, however, objected to scoping transfer agents into the Safeguards Rule. For example, one commenter suggested that applying the rules to all transfer agents could

---

310 *See* Better Markets Comment Letter.

311 *See id.*

312 *See id.*

313 *See id.*

314 *See* ICI Comment Letter 1.

315 *See* EPIC Comment Letter.

subject transfer agents registered with an appropriate regulatory agency that is not the Commission to conflicting data security requirements from those regulators, resulting in regulatory confusion.[316] One commenter stated that extending the rules to all transfer agents would exceed the scope of the Commission's authority.[317] Similarly, two commenters stated that the Commission should exempt certain transfer agents from the safeguards rule, such as transfer agents subject to existing state and Federal banking laws addressing privacy and safeguarding customer information, or those that do not engage in paying agent services.[318] One of these commenters stated that transfer agents "do not have the type or scope of personal information which could lead to further complications for securityholders" because transfer agents are not subject to know-your-customer obligations, do not have extensive background information concerning securityholders, and generally do not have possession of shareholder assets or have information which could be used to take or transfer assets of shareholders.[319] One of these commenters also stated that it is already subject to banking laws and inter-agency guidelines that address privacy, breach notification, and disposal of personal information, such as the Banking Agencies' Incident Response Guidance.[320]

The Commission does not agree that extending the rules to all transfer agents would result in regulatory confusion. As discussed above, the GLBA and FACT Act oblige us to adopt regulations, to the extent possible, that are consistent and comparable with those adopted by the

---

316 *See* SIFMA Comment Letter 2.

317 *See* SIFMA Comment Letter 2.

318 *See* STA Comment Letter 2 and Computershare Comment Letter. We use the term "paying agent services" 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.

319 *See* STA Comment Letter 2.

320 *See* Computershare Comment Letter.

Banking Agencies, the CFPB, and the FTC.[321] The Commission has been mindful of the need to set standards for safeguarding customer records and information that are consistent and comparable with the corresponding standards set by these agencies, and to this end, we have modified the final amendments from the proposal to promote greater consistency with other applicable Federal safeguard standards where such changes do not affect the investor protection purposes of this rulemaking, as discussed in more detail above.[322] Thus, although there are some differences, the final amendments are largely aligned with the Banking Agencies' Incident Response Guidance and Safeguards Guidance to which some transfer agents supervised by one of the Banking Agencies are already subject.[323] We recognize, however, that transfer agents registered with the Banking Agencies are already subject to the Banking Agencies' Incident Response Guidance and Safeguards Guidance and therefore may need to review their existing procedures under the Banking Agencies' Guidance for compliance with the final amendments. To the extent there are differences between their existing procedures and the final amendments, given the Commission's efforts to promote consistency between the final amendments and other federal safeguards standards, it will be possible for transfer agents to update their existing policies, procedures, and practices to ensure consistency with both the Banking Agencies' Guidance and the final amendments.[324] Finally, even if the final amendments impose additional requirements on some transfer agents already subject to the Banking Agencies' Guidance, it is appropriate to establish a minimum nationwide standard for the notification of securityholders

---

321 *See supra* section I.

322 For example, the final amendments require covered institutions to ensure that their service providers provide notification as soon as possible, but no later than 72 hours after becoming aware that an applicable breach has occurred, which is informed by the 72-hour deadline that is required under CIRCIA. *See supra* section II.A.4.b.

323 *See infra* sections IV.C.2.b and IV.D.2.b.

324 *See supra* section I.

who are affected by a transfer agent data breach that is tailored to the Commission's mission and the specific requirements.[325] For these reasons, the Commission does not agree that it should exempt from the safeguards rule transfer agents that are subject to existing Federal banking laws addressing privacy and safeguarding customer information.

Moreover, the Commission is not exempting from the safeguards rule transfer agents that do not engage in paying agent services. The population of transfer agents that maintain sensitive, detailed and individualized information related to securityholders is not limited to those transfer agents that engage in paying agent services. Providing the exemption suggested by this commenter would deprive securityholders whose sensitive customer information is maintained by a non-paying agent transfer agent of the important protections afforded under the final amendments.

The Commission does not agree that extending the rules to all transfer agents would exceed the scope of the Commission's authority. As discussed in the proposal, 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 derived from a consumer report for a business purpose to properly dispose of the information.[326] 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.[327] The Commission also stated at that time that the GLBA did not include transfer

---

325 *See supra* section I.

326 *See* Proposing Release at section II.C.3; *see also* 15 U.S.C. 1681w.

327 *See* Disposal of Consumer Report Information, Exchange Act Release No. 50361 (Sept. 14, 2004), 69 FR 56307 at n.23 (Sept. 20, 2004).

agents within the list of covered entities for which the Commission was required to adopt privacy rules.[328] 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.[329]

The Commission, however, has broad authority under Section 17A of the Exchange Act that is 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 the purposes of Title I of the Exchange Act.[330] Specifically, whether transfer agents initially register with the Commission or another appropriate regulatory agency,[331] section 17A(d)(1) of the Exchange Act authorizes the 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 registered with either the Commission or another appropriate regulatory agency. Once a transfer agent is registered with any appropriate regulatory agency, the Commission "is empowered with broad rulemaking

---

328 *See id.* at n.27.

329 *See id.*

330 *See* 15 U.S.C 78q-1.

331 *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.").

authority over all aspects of a transfer agent's activities as a transfer agent."[332] Pursuant to its statutory authority, the Commission has adopted rules that address various aspects of transfer agents' activities, including annual disclosures, transaction processing, responses to written inquiries, recordkeeping, safeguarding of funds and securities, lost securityholder searches, among others.[333] These and the Commission's other transfer agent rules[334] currently apply to and are enforceable against *all* registered transfer agents, including those that initially registered with an appropriate regulatory agency other than the Commission.[335]

The FTC has not adopted disposal and privacy rules to govern transfer agents registered with an appropriate regulatory agency that is not the Commission. The Commission is exercising its authority under section 17A(d)(1) of the Exchange Act to extend the safeguards rule to apply to any transfer agent registered with either the Commission or another appropriate regulatory agency and to extend the disposal rule to apply to transfer agents registered with another appropriate regulatory agency. The Commission does so to address the risks of market disruptions and investor harm posed by cybersecurity and other operational risks faced by transfer agents. Extending the safeguards rule and disposal rule to address those risks is in the

---

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

333 *See*, *e.g.*, SEC Form TA–2, 17 CFR 249b.102 (Form for Reporting Activities of Transfer Agents Registered Pursuant to Section 17A of the Securities Exchange Act of 1934) (annual disclosures); Exchange Act Rule 17Ad-2, 17 CFR 240.17Ad-2 (transaction processing); Exchange Act Rule 17Ad-5, 17 CFR 240.17Ad-5 (written inquiries); Exchange Act Rule 17Ad-6, 17 CFR 240.17Ad-6 (recordkeeping); Exchange Act Rule 17Ad-7, 17 CFR 240.17Ad-7 (record retention); Exchange Act Rule 17Ad-12, 17 CFR 240.17Ad-12 (safeguarding); Exchange Act Rule 17Ad-17, 17 CFR 240.17Ad-17 (lost securityholder searches).

334 *See*, *e.g.*, Exchange Act Rules 17Ad-1 through 17Ad-20, 17 CFR 240.17Ad-1 through 240.17Ad-20.

335 For example, the Commission has found bank-registered transfer agents in violation of various Commission rules. *See In the Matter of Citibank, N.A.*, Exchange Act Release No. 31612 (Dec. 7, 1992) (settled matter) (Exchange Act Rules 17Ad-12 and 17f-1); *In the Matter of the Chase Manhattan Bank*, Exchange Act Release No. 44835 (Sept. 24, 2001) (settled matter) (Exchange Act Rules 17Ac2-2, 17Ad-10, and 17Ad-11); *In the Matter of Wilmington Trust Company*, Exchange Act Release No. 49904 (Jun. 23, 2004) (settled matter) (Exchange Act Rules 17Ac2-2, 17Ad-10, 17Ad-11, and 17Ad-13); *In the Matter of the Bank of New York*, Exchange Act Release No. 53709 (Apr. 24, 2006) (settled matter) (Exchange Act Rule 17Ad-17).

public interest, and necessary for the protection of investors and for the safeguarding of funds and securities.

As explained in the proposal, transfer agents are subject to many of the same risks of data system breach or failure that other market participants face.[336] For example, transfer agents are vulnerable to a variety of software, hardware, and information security risks that could threaten the ownership interests of securityholders or disrupt trading within the securities markets.[337] A software, hardware, or information security breach or failure at 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. 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, due to the information about securityholders that transfer agents maintain.[338]

At the same time, the scope and volume of funds and securities that are processed or held by transfer agents have increased dramatically since Regulation S-P was first adopted.[339] 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. For example, transfer agents that provide paying agent services on behalf of issuers play a significant role within that system. According to Form TA-2 filings in 2023, transfer agents distributed approximately $3.68 trillion in securityholder dividends and bond principal and interest payments. Critically, because

---

336 *See* Proposing Release at section II.C.3.

337 *See generally* SEC Cybersecurity Roundtable transcript (Mar. 26, 2014), *available at* https://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt.

338 *See* Proposing Release at section II.C.3.

339 *See id*.

Form TA-2 does not include information relating to the value of purchase, redemption, and exchange orders by mutual fund transfer agents, the $3.68 trillion amount stated 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 $3.68 trillion number would be significantly higher.[340]

Moreover, contrary to some commenters' statements, transfer agents do maintain personal information about individual securityholders that could be used to take or transfer assets of securityholders or otherwise lead to further complications for securityholders. As stated in the proposal, transfer agents may 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).[341] For example, any registered transfer agent that maintains a master securityholder file on behalf of an issuer must post to that file debits and credits containing minimum and appropriate certificate detail representing every security transferred, purchased, redeemed, or issued.[342] Pursuant to Exchange Act Rule 17Ad-9, certificate detail must include, among other things, the name and address of the registered securityholder, the number of shares or principal dollar amount of the equity or debt security, and any other identifying information about the securityholder or the securityholder's securities that the transfer agent reasonably deems essential to its recordkeeping system for the efficient and effective research of record differences.[343] This can include date of birth, social security or tax

---

340 As stated in the proposal, Commission staff has observed through supervisory activities 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. *See* Proposing Release at section II.C.3.

341 *See* Proposing Release at section I, section II.C.3.

342 *See* 17 CFR 240.17Ad-10.

343 *See* 17 CFR 240.17Ad-9(a).

payer identification number, phone numbers, email addresses, information about relatives, and other sensitive personal information.[344] Transfer agents also maintain additional personal information about securityholders in connection with ancillary account, administrative, and other services transfer agents provide to securityholders on behalf of issuers, such as plan administration, proxy services, corporate action processing, and disbursement of dividend and interest payments.[345] This is the same type of customer information collected and maintained by other covered institutions and warrants the same level of protection. For example, the Commission is aware of instances in which threat actors have utilized securityholder information obtained from a transfer agent to steal securities and funds from those securityholders.[346]

For these reasons, the Commission is extending the safeguards rule and disposal rule to cover *all* registered transfer agents because it is in the public interest and will help protect investors and safeguard their securities and funds. Extending the safeguards rule to cover any registered transfer agent addresses the risks to the security and integrity of customer information associated with the systems those transfer agents maintain. This in turn helps prevent securityholders' customer information from being compromised, which, as discussed above, could threaten the ownership interest of securityholders or disrupt trading within the securities markets. Extending the final amendments to all registered transfer agents also helps establish

---

344 *See In the Matter of Columbia Management Investment Services Corp.*, Exchange Release No. 80016 (Feb. 10, 2017) (settled matter) (finding that the transfer agent's Records Management Manager "viewed sensitive personal account information such as addresses, dates of birth, and identification numbers" to misappropriate foreign deceased shareholders' funds and securities).

345 *See* Proposing Release at section II.C.3 (discussing generally the services provided by transfer agents); Advanced Notice of Proposed Rulemaking, Concept Release, Transfer Agent Regulations, Exchange Act Release No. 76743 (Dec. 22, 2015), 80 FR 81948 (Dec. 31, 2015) (describing the recordkeeping, shareholder communications, securities issuance, and tax reporting services provided by transfer agents).

346 *See In the Matter of Columbia Management Investment Services Corp.*, Exchange Act Release No. 80016 (Feb. 10, 2017) (settled matter) (finding that the transfer agent's Records Management Manager "viewed sensitive personal account information such as addresses, dates of birth, and identification numbers" to misappropriate foreign deceased shareholders' funds and securities).

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. Finally, as discussed above, extending the disposal rule to cover those transfer agents registered with another appropriate regulatory agency helps ensure all registered transfer agents are subject to the same minimum nationwide standard, tailored to the Commission's mission and requirements, and will 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.

Definition of a Transfer Agent's Customer

As stated above, the final amendments include a definition of customer that is specific to transfer agents, which is being adopted as proposed, except for a clarification noted below. For a transfer agent, 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.[347] The Commission is clarifying that this definition applies for purposes of section 248, meaning that it does not apply to any other rules, including those specific to transfer agents codified at 17 CFR 240.17Ad. Unless specified, securityholders of issuers are not customers of transfer agents for purposes of other rules. The Commission is adopting this definition because, as discussed above, although transfer agents' customers generally are issuers of securities, transfer agents collect and maintain non-public personal information about the individual registered owners who hold those issuers' securities in connection with various services and activities they engage in on behalf of issuers.

[347] *See* final rule 248.30(d)(4)(ii).

Some commenters supported this definition and approach of treating securityholders of an issuer as a transfer agent's customer, while other commenters did not. One commenter stated that this approach would close a "regulatory gap" – despite possessing and maintaining sensitive information about securityholders, no transfer agents are currently subject to the safeguards rule, and only transfer agents registered with the Commission are subject to the disposal rule.[348] Similarly, one commenter supported protecting customer information by subjecting that information to Regulation S-P, regardless of how it comes into the covered institution's possession.[349] On the other hand, one commenter opposed this proposed definition, stating that the need for a specific defined term for transfer agents indicated that the amendments were not well suited for transfer agents.[350] Three commenters stated that securityholders of issuers are not customers of the transfer agent, rather the issuer is the customer of the transfer agent.[351]

The Commission agrees that customer information held by a covered institution must be protected, regardless of how that customer information comes into the covered institution's possession. As discussed in the proposal and above, transfer agents 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).[352] They also collect detailed personal information in connection with various services provided directly to individual securityholders, such as facilitating legal and other transfers of securities, replacing lost or stolen securities certificates, facilitating corporate communications with investors, providing cost-basis

---

348 *See* Better Markets Comment Letter.

349 *See* ICI Comment Letter 1.

350 *See* STA Comment Letter 2.

351 *See* STA Comment Letter 2, Computershare Comment Letter, and SIFMA Comment Letter 2.

352 *See* Proposing Release at section I; section II.C.3; *see also supra* the text accompanying footnote 285.

calculations for tax purposes, and other services.[353] The fact that a transfer agent may not have a direct contractual relationship with an individual securityholder does not eliminate the need for transfer agents to protect the sensitive personal information about individual securityholders that is collected and maintained by the transfer agent.

Contrary to some commenters' statements, adopting a transfer agent-specific definition of customer does not indicate that the safeguards rule and disposal rule are not well-suited for transfer agents. Rather, it helps ensure that the rule is appropriately tailored to address transfer agents and the specific type of customer information they collect and maintain. Tailoring specific rule provisions to specific types of entities to address their unique functions, structures, and businesses does not render the rule inappropriate to the entity for which the provisions are being tailored, nor is it an approach that is unique to transfer agents or to Regulation S-P. For example, since the adoption of Exchange Act Rule 17Ad-12, transfer agents have been required to safeguard any funds and securities, including securityholder funds and securities, in the transfer agent's possession or control.[354] This is the case although securityholders may not be direct customers of transfer agents. As another example, final rule 248.30(d)(5)(i) defines customer information, for any covered institution other than a transfer agent as any record containing nonpublic personal information as defined in final rule 248.3(t) about a customer of a financial institution, whether in paper, electronic or other form, in the possession of a covered institution or that is handled or maintained by the covered institution or on its behalf, regardless of whether such information pertains to (a) individuals with whom the covered institution has a customer

---

[353] *See* Proposing Release at section II.C.3 (discussing generally the services provided by transfer agents); Advanced Notice of Proposed Rulemaking, Concept Release, Transfer Agent Regulations, Exchange Act Release No. 76743 (Dec. 22, 2015), 80 FR 81948 (Dec. 31, 2015) (describing the recordkeeping, shareholder communications, securities issuance, and tax reporting services provided by transfer agents).

[354] *See* 17 CFR 240.17Ad-12.

relationship, or (b) the customers of other financial institutions where such information has been provided to the covered institution.[355] The fact that the securityholder whose funds and securities the transfer agent is in possession of is not a direct customer of the transfer agent does not eliminate the need for the transfer agent to safeguard those funds and securities. The same is true for customer information in the possession of a transfer agent or that is handled or maintained by the transfer agent or on its behalf.

Finally, two commenters stated that the Commission should propose a rule specific to transfer agents as part of the existing rules that apply specifically to transfer agents.[356] In these commenters' views, such a rule would impose obligations similar to the final amendments but would apply only to transfer agents. One of these commenters further explained that it would support general safeguarding of securityholder information requirements, similar to those set forth in the safeguard rule, if the Commission enacted them as part of the regulations specific to transfer agents codified at 17 CFR 240.17Ad.[357]

The Commission is not taking the approach suggested by the commenters. The final amendments will accomplish a similar result to a transfer agent-specific rule, while helping to ensure consistent requirements among covered institutions. Further, the commenters did not explain how such a rule would differ from the final amendments, other than being in a different set of Commission regulations, or how such a rule would be a material improvement over the approach being adopted as proposed. The Commission does not agree that adopting something different from the final amendments is necessary to achieve the "Commission's privacy and

---

355 *See* final rule 248.30(d)(5)(i).

356 *See* STA Comment Letter 2 and Computershare Comment Letter.

357 *See* Computershare Comment Letter.

cybersecurity goals in a manner specific to the business and role of transfer agents."[358] Rather, doing so would undermine the Commission's goal of establishing a consistent minimum nationwide standard. Further, where necessary, the Commission has already tailored the final amendments in a manner specific to transfer agents. As noted above, the final amendments include a definition of customer that it is specific to transfer agents. Finally, to the extent one of commenters' goals is ensuring that all transfer agent rules are codified in the same place, specifically 17 CFR 240.17Ad, commenters' suggestion would not further that goal. Transfer agents registered with the Commission are already subject to the disposal rule, which is not part of the existing rule set codified at 17 CFR 240.17Ad, and a new safeguards or disposal rule within that section would necessarily cite to Regulation S-P for defined terms and other references.

Application of Laws, Requirements, and Contractual Provisions

Some commenters raised concerns about potential conflicts with, or duplication, of state law requirements. One commenter stated that securityholders of issuers are not customers of the transfer agent and imposing obligations on them creates conflicting and duplicative requirements to those already in place through state laws to safeguard securityholders' personal information.[359] Another commenter stated that under state law, transfer agents do not notify securityholders of a breach but issuers do.[360] Specifically, this commenter stated that all fifty states have laws that require transfer agents to notify their issuer clients of unauthorized access to personal information of securityholders, and issuers may then be required to notify securityholders depending on whether the standards of the state law have been met. This

---

358 STA Comment Letter 2.

359 *See* STA Comment Letter 2.

360 *See* Computershare Comment Letter.

commenter also stated that its existing policies, procedures, and contractual obligations are designed to track these state law requirements and that certain provisions in transfer agents' contracts with issuer clients could prohibit transfer agents from notifying securityholders of data breaches in the manner required by the amendments.[361] Both commenters stated that the Commission should consider preempting state laws to minimize the potential for multiple and competing obligations, and if not, prepare and produce a cost-benefit analysis to identify the specific ways in which the amendments would be an improvement over existing law.[362] This commenter further explained that the issuer client would notify securityholders depending on whether the standards of the state law have been met.[363]

While we acknowledge the commenters' concerns, the final amendments permit transfer agents and issuers to develop arrangements to address them. Nothing in the final amendments will prohibit or limit transfer agents' ability to enter into or modify their contracts with issuer clients in a manner that allows the transfer agent to comply with applicable legal requirements. Indeed, some transfer agents already send customer notices on behalf of their issuer clients. As one commenter stated in requesting that the Commission permit covered institutions to have their service providers send breach notices to affected individuals on their behalf, it is a common practice today for investment companies to have their transfer agents assume responsibility for sending affected customers breach notices.[364] The Commission acknowledges that, to the extent a transfer agent has contractual provisions with issuer clients that prevent securityholders from receiving notice of a breach directly from the transfer agent, the transfer agent may determine to

---

361 *See* Computershare Comment Letter.

362 *See* STA Comment Letter 2 and Computershare Comment Letter. *See also infra* section IV.D.2.b.

363 *See id*.

364 *See* ICI Comment Letter 1.

amend those contractual provisions to comply with the final amendments. Further, as discussed above, in a modification from the proposal, the final amendments provide that a covered institution that is required to notify affected individuals may satisfy that obligation by ensuring that the notice is provided by another party (as opposed to providing the notice itself). Accordingly, if a transfer agent experiences an incident affecting securityholders of another covered institution, it would have the option of coordinating with the covered institution as to which institution will actually send the notice.[365]

As explained in the proposal, the Commission understands that 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.[366] 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). However, the specific requirements regarding the timing of the notice, content of the notice, types of data covered, and other aspects may vary.[367] Indeed, one commenter highlighted the variation and uncertainty among different state law requirements.[368] Thus, while transfer agents may already be complying with one or more state notification laws, variations in these state laws could result in residents of one state receiving notice while residents of another do not receive notice, or receive it later, or receive different information for the same data breach incident. The final amendments address this concern by imposing a Federal

---

365 *See supra* section II.A.3.a.

366 *See* Proposing Release at section III.C.2.

367 *See supra* section I.

368 *See* Computershare Comment Letter.

minimum standard for customer notification, which will help ensure timely, consistent notice to affected securityholders regardless of their state of residence.

Impact of Notices from Transfer Agents

One commenter stated that the proposal would equalize standards governing transfer agents, and in doing so, promote investor protection.[369] On the other hand, several commenters stated that the proposed rule regarding transfer agents would confuse securityholders. One commenter suggested that requiring a transfer agent to identify and contact customers of another institution may cause those customers to be confused and concerned.[370] Two commenters similarly stated that the notification requirement is likely to confuse securityholders because it would result in securityholders receiving notice from both the transfer agent and the issuer with respect to the same breach.[371] One commenter further stated that a transfer agent should only be required to notify an issuer of an incident.[372]

We acknowledge that due to existing state law provisions, individuals affected by a breach at a transfer agent may receive notice from the issuer and the transfer agent with respect to the same breach. Moreover, transfer agents subject to the Banking Agencies' Incident Response Guidance may send notices under those provisions as well, and it is possible that an issuer may also send notices to securityholders, pursuant to state law or other requirements. We acknowledge that these existing provisions, coupled with the requirements of the final amendments, may result in multiple notices being sent for the same incident. That said, as

---

369 *See* Better Markets Comment Letter.

370 *See* SIFMA Comment Letter 2.

371 *See* STA Comment Letter 2 and Computershare Comment Letter.

372 *See* SIFMA Comment Letter 2.

explained above, we have modified the final amendments to minimize the likelihood of multiple notices being sent by covered institutions for the same incident.[373]

Regardless, we do not agree that individuals who receive a notice from both a transfer agent and the issuer with respect to the same breach or who are contacted by a transfer agent on behalf of another institution will be confused. Any potential confusion could be ameliorated through a clear description of the specific incident that would allow an individual to determine whether it is covered by a notice from any covered institution.[374] Rather than create confusion, as some commenters assert, the final amendments will establish a Federal minimum standard for covered institutions, thereby reducing any extant or potential confusion. As discussed in the proposal, there are variations in existing state laws regarding a firm's duty to investigate a data breach, the specific events that trigger when notice of a breach is required, the timing of any such notices, and other details of a notice. The Federal minimum standard established by the final amendments will eliminate this confusion by ensuring that *all* affected securityholders receive an appropriate notice, regardless of the securityholder's state of residence, thereby enhancing investor protection overall. This benefit justifies the remote risk of potential confusion suggested by some commenters.

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

The final amendments will, as proposed, contain a number of amendments to Regulation S-P that result in the continuation of the same regulatory treatment for notice-registered broker-

---

373 *See supra* section II.A.3.a.

374 It is possible that customers may not be aware of their relationship with a transfer agent or otherwise may not recognize the transfer agent and therefore could read the notification as a phishing attempt or another nefarious scheme. *See infra* section IV.D.2.b.

dealers as they were subject to under the existing safeguards rule and disposal rule.[375] Specifically, notice-registered broker-dealers are explicitly excluded from the scope of the disposal rule,[376] but subject to the safeguards rule. However, under substituted compliance provisions, notice-registered broker-dealers are deemed to comply with the safeguards rule (and all other aspects of Regulation S-P, other than the disposal rule) if they are subject to, and comply with, the financial privacy rules of the CFTC,[377] including similar obligations to safeguard customer information.[378] The Commission initially 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.[379] When the Commission later adopted the disposal rule, it excluded notice-registered broker-dealers from the rule's scope, stating 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.[380] For these reasons, the Commission tailored the proposal to ensure there would be no

---

375 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. *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").

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

377 *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)).

378 *See* 17 CFR 160.30.

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

380 *See* Proposing Release at n.203.

change in the treatment of notice-registered broker-dealers under the safeguards rule and the disposal rule.[381]

No comments were received regarding the treatment of notice-registered broker-dealers under the safeguards rule and the disposal rule. For the reasons outlined in the Proposing Release, the Commission is adopting the amendments as proposed.[382] Specifically, as proposed, the definition of a "covered institution" includes "any broker or dealer," without excluding notice-registered broker-dealers, thus ensuring that Regulation S-P's substituted compliance provisions still apply to notice-registered broker-dealers with respect to the safeguards rule.[383] In addition, the final amendments include the "covered institution" defined term within the disposal rule, while retaining the disposal rule's existing exclusion for notice-registered broker-dealers.[384]

C. Recordkeeping

We are adopting amendments to require covered institutions to make and maintain written records documenting compliance with the requirements of the safeguards rule and of the

---

381 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 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 final rule related to the disposal rule, as they would remain excluded from its scope. *See* Proposing Release.

382 *See* Proposing Release at Section II.C.4.

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

384 *See* proposed rule 248.30(c)(1). As we are not adopting the paragraph in proposed rule 248.30(a), we are similarly not adopting the proposed 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. *See* proposed rule 248.2(c); *see also* discussion on Scope of Information Protected *supra* Section II.B.1. This proposed technical amendment was intended to reflect the proposed shift in the disposal rule's citation from paragraph (b) of rule 248.30 to paragraph (c) of rule 248.30, to ensure continuity in the treatment of notice-registered broker-dealers under Regulation S-P. As the final amendments will not result in such a shift to the disposal rule's citation, this proposed technical amendment has been rendered unnecessary.

disposal rule as outlined in the table below (collectively, "recordkeeping requirements").[385] We are adopting these amendments substantially as proposed, but, in response to a comment, with modifications designed to provide additional specificity to the scope of certain of the recordkeeping requirements as discussed below. The table below reflects the time periods that covered institutions will be required to preserve these records, which are as proposed. These times vary by covered institution but are consistent with existing recordkeeping rules for these entities to the extent they have pre-existing recordkeeping obligations.

Table 1: Recordkeeping Requirements

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

[385] As discussed previously, pursuant to Regulation Crowdfunding, funding portals must comply with the requirements of Regulation S-P as they apply to brokers. Funding portals are not, however, subject to the recordkeeping obligations for brokers found under Rule 17a-4. *See* 17 CFR 240.17a-4; *see also supra* footnote 5 and accompanying text. Instead, funding portals are already obligated, pursuant to Rule 404 of Regulation Crowdfunding, to make and preserve all records required to demonstrate their compliance with, among other things, Regulation S-P for five years, the first two years in an easily accessible place. *See* 17 CFR 227.404(a)(5). While the final amendments do not modify funding portals' recordkeeping requirements to include the same enumerated list of obligations as those applied to brokers under the amendments to Rule 17a-4, funding portals generally should look to make and preserve the same scope of records in connection with demonstrating their compliance with this portion of Regulation S-P.

Transfer Agents	17 CFR 240.17ad-7(k)	All records for three years, in an easily accessible place.
Note: 1. 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 – are not subject to Regulation S-P. 2. All books and records required to be made under the provision of 17 CFR 275.204-2(a) must be maintained and preserved in an easily accessible place for a period of not less than five years. 17 CFR 275.204-2(e).		

These recordkeeping requirements should aid covered institutions in periodically reassessing the effectiveness of their safeguarding and disposal programs by helping to ensure that those institutions have the records needed to perform that assessment. Additionally, maintenance of these records for sufficiently long periods of time and in accessible locations will help the Commission and its staff to monitor compliance with the requirements of the amended rules. We received one comment broadly in support of these recordkeeping requirements.[386]

The text of the proposed recordkeeping rules were worded differently for different covered institutions. For example, the proposed recordkeeping rule text for broker-dealers and transfer agents detailed the specific records to be kept whereas the proposed rule for advisers stated that advisers would be required to make and keep true, accurate and current a copy of the written records documenting compliance with the requirements of the safeguards and disposal rules.[387] The Commission sought comment on whether the detailed requirements proposed for broker-dealers and transfer agents should be included in the recordkeeping rules for other covered entities. While no commenter specifically responded to this request, one commenter did

386 ICI Comment Letter.

387 *See* proposed 17 CFR 240.17a-4, 17 CFR 240.17ad-7, and 17 CFR 275.204-2.

suggest that a clarification of the adviser recordkeeping rule could assist in understanding their obligations under the rule.[388] We are modifying the text of the proposed recordkeeping rules for registered investment advisers and registered and unregistered investment companies to provide in the final amendments the same detailed description as found in the rule text for broker-dealers and transfer agents. This should provide specificity as to what records are required to be kept under all of the recordkeeping rules.[389] In addition, and in a change from the proposal, we are modifying the final rules to require a covered institution to retain any written documentation from the Attorney General related to a delay in notice.[390] This should help ensure that a covered institution can justify a valid delay in sending notifications to affected individuals and aid the Commission's examination and oversight program.

The records that will be required under these amendments are:

- Written policies and procedures required to be adopted and implemented pursuant to final rule 248.30(a)(1), which requires policies and procedures to address administrative, technical, and physical safeguards for the protection of customer information;
- 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 final rule 248.30(a)(3);
- Written documentation of any investigation and determination made regarding whether notification to affected individuals is required pursuant to final rule

388 IAA Comment Letter.

389 *See* Proposing Release at section II.D.

390 *See e.g.*, final 17 CFR 240.17a-4(e)(14)(iii) and final rule 248.30(c)(iii).

248.30(a)(4), including the basis for any determination made, any written documentation from the Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination;[391]

- Written policies and procedures required to be adopted and implemented pursuant to final rule 248.30(a)(5)(i), which requires policies and procedures to oversee, monitor, and conduct due diligence on service providers, including to ensure that the covered institution is notified when a breach in security has occurred at the service provider;
- Written documentation of any contract or agreement between a covered institution and a service provider entered into pursuant to final rule 248.30(a)(5); and
- Written policies and procedures required to be adopted and implemented pursuant to final rule 248.30(b)(2), which requires policies and procedures to address the proper disposal of consumer information and customer information.

The records that will be required include records of policies and procedures under the safeguards rule that address administrative, technical, and physical safeguards for the protection of customer information.[392] The requirements will also include records documenting, among other things: (i) a covered institution's 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) a covered institution's notifications to affected individuals

---

391 Covered institutions are required to preserve a copy of any notice transmitted following the determination required under the final amendments, including those notices provided by the service provider to the covered institution's customers on behalf of the covered institution. *See e.g.*, final 17 CFR 270.31a-1(b)(13)(iii) (requiring registered investment companies to keep a copy of "*any notice* transmitted following such determination") (emphasis added); *see also supra* Section II.A.4.c.

392 *See, e.g.*, final 17 CFR 240.17a-4(e)(14)(i) and final 17 CFR 270.31a-1(b)(13)(i); *see also* final rule 248.30(a)(1).

consistent with the requirements of the final amendments as discussed above, or, where applicable, any determination that notification is not required after a reasonable investigation of the incident.[393] Records required to be made and maintained will also include records of those written policies and procedures associated with the service provider notification requirements of the final amendments as well as related records of written contracts and agreements between the covered institution and the service provider.[394]

The disposal rule, as amended, will require that every covered institution adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information.[395] The only record required under the final amendments for purposes of the disposal rule is these written policies and procedures.[396]

D. Exception from Requirement to Deliver Annual Privacy Notice

Currently, Regulation S-P generally requires broker-dealers, investment companies, and registered investment advisers to provide customers with annual notices informing them about the institutions' privacy practices ("annual privacy notice").[397] The Commission is adopting as

---

393 *See*, *e.g.*, final 17 CFR 17a-4(e)(14)(ii) and (iii) and final 17 CFR 270.31a-1(b)(13)(ii) and (iii); *see also* final rule 248.30(a)(3)(i) through (iii).

394 *See*, *e.g.*, final 17 CFR 17a-4(e)(14)(iv) and (v) and final 17 CFR 270.31a-1(b)(13)(iv) and (v); *see also* final rule 248.30(a)(5)(i) through (ii).

395 *See* final rule 248.30(b)(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 at text accompanying n.20 ("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, rule 248.30(b)(2) is intended primarily to seek sufficient documentation of policies and practices addressing the specific provisions of the disposal rule.

396 *See*, *e.g.*, final 17 CFR 17a-4(e)(14)(vi) and final 17 CFR 270.31a-1(b)(13)(vi); *see also* final rule 248.30(b)(2).

397 17 CFR 248.4; 248.5. "Annually" for these purposes is defined as at least once in any period of 12 consecutive months during which that relationship exists. Institutions are permitted to define the 12-consecutive-month period, but must apply it to the customer on a consistent basis. 17 CFR 248.5(a)(1). The institution does not need to provide an annual notice in addition to an initial notice in the same 12-month period.

proposed amendments to conform Regulation S-P to the requirements of the Fixing America's Surface Transportation Act ("FAST Act"),[398] which provides an exception to the annual privacy notice required by Regulation S-P, provided certain requirements are met. As proposed, we are amending Regulation S-P to include an exception to the annual privacy notice requirement if the institution (1) only provides non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies and (2) the institution has not changed its policies and practices with regard to disclosing non-public personal information from its most recent disclosure sent to customers.[399] The amendments also, as proposed, provide the timing for when an institution must resume providing annual privacy notices in the event that the institution changes its policies and practices such that the exception no longer applies. We received one comment supporting the proposed exception and timing requirements.[400]

We are adopting as proposed amendments to the annual notice provision requirement of Regulation S-P to include the exception to the annual notice delivery added by the statutory exception Congress enacted in the FAST Act. 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 does not specify a date by which the annual privacy notice delivery must resume.[401] The amended timing requirements are designed to be consistent with the existing timing requirements for privacy notice delivery in Regulation S-P. Specifically, if the change in policies and practices will also result in the institution being

---

398 Pub. L. 114-94, Sec. 75001, 129 Stat. 1312 (2015) (adding section 503(f) to the GLBA, codified at 15 U.S.C. 6803(f)).

399 *See* final 17 CFR 248.5(e)(1).

400 ICI Comment Letter.

401 *See supra* footnote 398.

required to send a revised privacy notice under the current requirements, the revised notice will be treated as an initial notice for the purpose of the timing requirement and the institution will be required to resume notices at the same time it otherwise provides annual privacy notices.[402] If a revised notice is not required, the institution will be required to resume providing annual privacy notices within 100 days of the change. The amendments allow institutions to preserve their existing approach to selecting a delivery date for annual privacy notices, thereby avoiding the potential burdens of determining delivery dates based on a new approach and any 100-day period will accommodate the institution delivering the privacy notice alongside any quarterly reporting to customers. The amendments also are intended to be consistent with existing privacy notice delivery requirements of the CFTC, CFPB, and FTC.[403]

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

As stated in the Proposing Release, certain staff letters and other staff statements addressing Regulation S-P and other matters covered by the final amendments may be withdrawn or rescinded in connection with this adoption. Upon the compliance date of these rules, staff letters and other staff statements, or portions thereof, will be withdrawn or rescinded to the extent that they are moot, superseded, or otherwise inconsistent with the rules. This may include the letters and statements below. To the extent any staff statement is inconsistent or conflicts with the requirements of the rules, even if not specifically identified below, that statement is superseded.

---

402 *See* 17 CFR 248.8.

403 *See* 17 CFR 160.5(D) (CFTC); 12 CFR 1016.5(e)(2) (CFPB); 16 CFR 313.5(e)(2) (FTC). *See also* 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); FTC, Privacy of Consumer Financial Information Rule Under the Gramm-Leach-Bliley Act, 84 FR 13150 (Apr. 4, 2019).

Table 2: Letters and Statements

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

F. Compliance Period

The Commission is providing an 18-month compliance period after the date of publication in the Federal Register for larger entities, and a 24-month compliance period after the date of publication in the Federal Register for smaller entities. Table 3 below outlines which entities will be considered "larger entities" for these purposes. Smaller entities will be those covered institutions that do not meet these standards. The Commission generally has approved similar tiered compliance dates with respect to smaller versus larger entities in the past and, in our experience, these thresholds are a reasonable means of distinguishing larger and smaller entities for purposes of tiered compliance dates for rules affecting these entities.[404]

Table 3: Designation of Larger Entities

Entity	Qualification to be Considered a "Larger Entity"
Investment companies together with other investment companies in the same group of related investment companies[1]	Net assets of $1 billion or more as of the end of the most recent fiscal year

[404] *See*, *e.g.*, Investment Company Names, Investment Company Act Release No. 35000 (Sept. 20, 2023) [88 FR 70436 (Oct. 27, 2023)]; Investment Company Reporting Modernization, Investment Company Act Release No. 32314 (Oct. 13, 2016) [81 FR 81870 (Nov. 18, 2016)]; Investment Company Liquidity Risk Management Programs, Investment Company Act Release No. 32315 (Oct. 13, 2016) [81 FR 82142 (Nov. 18, 2016)]; Inline XBRL Filing of Tagged Data, Securities Act Release No. 10514 (June 28, 2018) [83 FR 40846 (Sept. 17, 2018)]; and Private Fund Advisers; Documentation of Registered Investment Adviser Compliance Reviews, Investment Advisers Act Release No. 6383 (Aug. 23, 2023) [88 FR 63206 (Sept. 14, 2023)].

Registered investment advisers[2]	$1.5 billion or more in assets under management
Broker-dealers[3]	All broker-dealers that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act
Transfer agents[4]	All transfer agents that are not small entities under the Securities Exchange Act for purposes of the Regulatory Flexibility Act

Note:

1. "Group of related investment companies" is as defined in 17 CFR 270.0-10. We estimate that, as of September 2023, 77% of registered investment companies would be considered to be larger entities. This estimate is based on data reported in response to Items B.5, C.19, and F.11 on Form N-CEN.

2. We estimate that, as of September 2023, 23% of registered investment advisers would be considered to be larger registered investment advisers. This estimate is based on data reported in response to Items 2.A and 5.F.2.(c) on Form ADV.

3. 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. This threshold was chosen to include all broker-dealers who do not fall within the definition of a small entity under the Regulatory Flexibility Act (5 U.S.C. 553). Based upon FOCUS filings for the third quarter of 2023, we estimate approximately 77% of broker-dealers, not including funding portals, would be considered larger entities. Based upon staff analysis and review of public filings, we estimate approximately 3% of funding portals would be considered larger entities.

4. 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. 17 CFR 240.0-10. This threshold was chosen to include all transfer agents who do not fall within the definition of a small entity under the Regulatory Flexibility Act. 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 filed with the Commission as of September 30, 2023, we estimate approximately 132 transfer agents may be considered small entities, of 315 total registered transfer agents. *See infra* section VI.

We proposed a 12-month transition period from the effective date for all covered institutions, regardless of asset size, and we solicited comment on whether the compliance period should be shorter or longer, and whether it should be the same for all covered institutions. Commenters that addressed this aspect of the proposal urged the Commission to provide additional time, generally suggesting a two-year or three-year period to provide time for covered institutions to prepare to comply with the rule's requirements.[405] Commenters suggested that the

[405] *See*, *e.g.*, SIFMA Comment Letter 2; Computershare Comment Letter; ICI Comment Letter 1; Federated Comment Letter; Google Comment Letter.

proposed compliance period underestimates the time it would take to implement any final rule.[406] In particular, commenters expressed that advisers will need to holistically reassess their current service provider infrastructure and may need time to find new service providers or renegotiate terms of service provider agreements in order to comply with the rule's requirements.[407] Separately, two commenters urged the Commission to consider a tiered compliance period that staggers the compliance date based on firm size, with larger firms having to comply with the rule's requirements prior to smaller firms.[408] These commenters asserted that a longer compliance period for smaller broker-dealers and investment advisers would allow these firms to benefit from the implementation of larger industry participants.

We have taken commenter concerns into account in determining the compliance schedule,[409] and we are adopting a compliance period of 18-months following the date of publication of the final amendments in the Federal Register for larger entities, and 24-months following the date of publication in the Federal Register for smaller entities.[410] The compliance

---

406 *See*, *e.g.*, IAA Comment Letter 1; FII Comment Letter; SIFMA Comment Letter 2; ICI Comment Letter 1; *see also* IAA Comment Letter 2 (stating that "advisers would need to holistically reassess their current service provider infrastructure and undergo the time-consuming and expensive process of negotiating terms with each Service Provider, re-evaluate their current policies, procedures, and practices in light of any new requirements, prepare for new and/or different client notification obligations, and create and implement modified written incident response program policies and procedures and recordkeeping requirements").

407 *See*, *e.g.*, Google Comment Letter; Federated Comment Letter; SIFMA Comment Letter 2; AWS Comment Letter; FII Comment Letter.

408 IAA Comment Letter 1; FSI Comment Letter.

409 ICI Comment Letter 1; Schulte Comment Letter; IAA Comment Letter 2 (asserting that the Commission's new rules could potentially require investment advisers to establish and implement new regulatory requirements during compressed and overlapping compliance periods while attempting to comply with existing ongoing regulatory obligations). For further discussion of other recent Commission rules that may have overlapping compliance periods for some covered entities, as well as the potential associated costs associated with implementing multiple rules at once, *see infra* section IV.

410 With respect to the compliance period, commenters requested the Commission consider interactions between the proposed rule and other recent Commission rules. In determining compliance dates, the Commission considers the benefits of the rules as well as the costs of delayed compliance dates and potential overlapping compliance dates. For the reasons discussed throughout the release, to the extent that there are costs from overlapping compliance dates, the benefits of the rule justify such costs. *See infra* section IV for a discussion of the interactions of the final amendments with certain other Commission rules.

period we are adopting is designed to strike the appropriate balance between allowing covered institutions adequate time to establish or adjust their data notification compliance practices and allowing customers and investors to benefit from the amended Regulation S-P framework. Taking concerns of smaller entities into account, smaller entities will benefit from having an additional six months to come into compliance with the final amendments, based on feedback from commenters and to the extent that smaller entities may face additional or different challenges in coming into compliance with the final amendments than larger entities. Although we are providing for a longer compliance period than proposed, we are not providing more than 18 or 24 months, as suggested by some commenters, because we have made modifications from the proposal that should alleviate commenters' concerns related to time needed to establish and implement processes to comply with the final amendments. In a modification from the proposal, the final amendments will no longer require covered institutions to have a written contract with its service providers mandating that service providers take appropriate measures to protect against unauthorized access to or use of customer information, but will instead require covered institutions to establish written policies and procedures reasonably designed to oversee, monitor, and conduct due diligence on service providers.[411] Accordingly, the compliance dates will provide an appropriate amount of time for covered institutions to comply with the final amendments.

III. OTHER MATTERS

Pursuant to the Congressional Review Act,[412] the Office of Information and Regulatory Affairs has designated the final amendments as a "major rule" as defined by 5 U.S.C. 804(2). If

---

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

412 5 U.S.C. 801 *et seq*.

any of the provisions of these rules, or the application thereof to any person or circumstance, is held to be invalid, such invalidity shall not affect other provisions or application of such provisions to other persons or circumstances that can be given effect without the invalid provision or application.

IV. ECONOMIC ANALYSIS

A. Introduction

The Commission is mindful of the economic effects, including the benefits and costs, of the adopted 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 will 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 final 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 adoption.

The final amendments require every broker-dealer,[413] every funding portal,[414] every investment company, every registered investment adviser, and every transfer agent to notify affected customers of certain data breaches.[415] To that end, the final amendments 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 to or use of customer information,[416] 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.[417] The final amendments also define the scope of information covered by the safeguards rule and by the disposal rule,[418] and extend the covered population to all transfer agents registered with the Commission or with another appropriate regulatory agency.[419] Finally, the final amendments impose various related

---

413 Notice-registered broker-dealers subject to and complying with the financial privacy rules of the CFTC will be deemed to be in compliance with the final provision through the substituted compliance provisions of Regulation S-P. *See supra* section II.B.3. As discussed above, unless otherwise stated, references elsewhere in this release to "brokers" or "broker-dealers" include funding portals. *See supra* footnote 5. For the purposes of this economic analysis, however, "broker" and "broker-dealer" do not include funding portals because the economic effects of the final amendments on funding portals differ in some respects from the effects on broker-dealers.

414 Pursuant to Regulation Crowdfunding, funding portals "must comply with the requirements of [Regulation S-P] as they apply to brokers." *See* 17 CFR 227.403(b); *see also supra* footnote 5 and accompanying text.

415 Notification is required in the event that sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. *See* final rule 248.30(a)(4)(i).

416 As discussed above, "customer information" includes not only information of customers of the aforementioned entities, but also information of customers of other financial institutions in the possession of covered institutions. *See supra* section II.B.1 and final rule 248.30(d)(5)(i). In addition, with respect to transfer agents, "customers" refers to "any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent." *See* final rule 248.30(d)(4)(ii).

417 *See* final rule 248.30(a)(4); *see also supra* section II.A. Notice will not be required, however, if a covered institution has determined, after a reasonable investigation of the facts and circumstances of an 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.

418 Under the final amendments, the safeguards rule applies to "customer information" and the disposal rule applies to "consumer information" and "customer information." *See* final rule 248.30(a)(1), 248.30(b), 248.30(d)(1), and 248.30(d)(5).

419 *See* final rule 248.30(d)(3).

recordkeeping requirements,[420] and include in the regulation an existing statutory exception to annual privacy notice requirements.[421]

The final amendments will affect covered institutions as well as customers who will receive the required notices. The final amendments will also have indirect effects on service providers that receive, maintain, process, or otherwise are permitted access to customer information on behalf of covered institutions: under the final amendments, unauthorized access to or use of sensitive customer information via service providers will fall under the customer notification requirement. The final amendments require that a covered institution's incident response program include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers.[422] These policies and procedures must be reasonably designed to ensure that service providers take appropriate measures to protect against unauthorized access to or use of customer information and provide notification to the covered institution of a breach of security resulting in unauthorized access to a customer information system maintained by the service provider.[423]

The main economic effects of the final amendments will result from the notification and incident response program requirements applicable to all covered institutions.[424] For reasons discussed later in this section, the extension of Regulation S-P to transfer agents will have more limited economic effects.[425] Finally, we anticipate the recordkeeping requirements and the

---

420 *See*, *e.g.*, final rule 17 CFR 275.204-2(a). *See also supra* section II.C and footnote 385.

421 *See* final rule 248.5(e).

422 *See* final rule 248.30(a)(5).

423 *See id*.

424 *See infra* sections IV.D.1.a and IV.D.1.b.

425 *See infra* section IV.D.2.b.

incorporation of the existing statutory exception to annual privacy notice requirements to have minimal economic effects, as discussed further below.[426]

The main economic benefits of the final notification and incident response program requirements, as well as the extension of Regulation S-P to include all transfer agents, will result from enhanced protection of customer information. Customers will directly benefit from the opportunity to take appropriate mitigating actions to protect their accounts and information in the event of unauthorized access to or use of their sensitive information. Direct benefits will result from covered institutions allocating additional resources towards policies and procedures, information safeguards, and cybersecurity to comply with the final requirements. There may lastly be indirect benefits from covered institutions undertaking these actions to the extent they seek to avoid reputational harm resulting from the mandated notifications. These additional resources will contribute to reducing the exposure of covered institutions, and of the broader financial system, to incidents resulting in unauthorized access to or use of customer information.[427] The main economic costs from these new requirements will be compliance costs related to the development and implementation of the required policies and procedures, reputational costs borne by firms that would not otherwise have notified customers of a data breach, and indirect costs from increased expenditures on additional safeguards for covered institutions who will choose to make such investments to avoid such reputational costs.[428]

---

426 *See infra* sections IV.D.3 and IV.D.4.

427 While the scope of the safeguards rule and of the final amendments is not limited to cybersecurity, in the contemporary context, their main economic effects are realized through their effects on cybersecurity. *See infra* footnote 507.

428 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 consequence of the Commission's rules (e.g., reputational costs resulting from disclosure of data breach, or increased cybersecurity spending aimed at avoiding such reputational costs).

We anticipate that the economic benefits and costs of the final notification requirements will—in the aggregate—be limited because all states already require some form of customer notification of certain data breaches,[429] and because many entities are likely to already have response programs in place.[430] Many customers already receive some level of data breach notification under other laws. This means that the benefits and costs, both direct and indirect, will only accrue from actions taken by covered institutions that are not already required by existing rules or caused by existing competitive forces. The final amendments will, however, afford many individuals greater protections by, for example, defining "sensitive customer information" more broadly than the current definitions used by certain states;[431] providing for a 30-day notification outside timeframe that is shorter than the timing currently mandated by many states, including states providing for no deadline or those allowing for various delays;[432] and providing for a more robust notification trigger than in many states.[433] The final amendments also limit the time a service provider can take to notify a covered institution of a breach to 72 hours, which is a shorter period of time than mandated by many states, allowing covered institutions to notify their customers faster if such notification is required under the final amendments.[434] Further, in certain states, state customer notification laws do not apply to entities subject to or in compliance with the GLBA, and the final amendments will help ensure that customers residing

---

429 *See infra* section IV.C.2.a.

430 *See infra* sections IV.C.1 and IV.C.2.

431 *See infra* section IV.D.1.b(3).

432 *See infra* section IV.D.1.b(2).

433 *See infra* section IV.D.1.b(4).

434 Upon receipt of such a notification from a service provider, a covered institution must initiate its incident response program. This may or may not result in the covered institution having to notify customers. *See* final rule 248.30(a)(5)(i); *infra* section IV.D.1.c.

in these states receive notice of a breach if it occurs.[435] The final amendments will help ensure that all customers, regardless of where they reside, receive a minimum of information regarding a given breach affecting their information and are therefore equally able to take appropriate mitigating actions.

For these reasons, the final requirements will improve customers' knowledge of when their sensitive information has been compromised. Specifically, we expect that the adopted Federal minimum standard for notifying customers of certain types of data breaches, along with the preparation of written policies and procedures for incident response, will result in more customers being notified of these data breaches as well as faster notifications for some customers, and that both of these effects will improve customers' ability to act to protect their personal information. Moreover, such improved notification will—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 will increase the disciplining effect on covered institutions, incentivizing them to improve customer information safeguards and reduce their exposure to data breaches, thereby improving the resilience of the financial system more broadly.[436] This will reduce economic inefficiency in that it will better align customers' and covered institutions' incentives to safeguard customer information, but will also result in new indirect costs for covered institutions who choose to undertake these improvements in order to avoid those potential reputational costs. In addition, by

---

435 *See infra* section IV.D.1.b(1).

436 As discussed below, the final amendments could result in unnecessary notification, which could lead to customer desensitization. *See infra* section IV.D.1. Unnecessary notification could decrease covered institutions' incentives to invest in customer information safeguards in order to avoid reputational costs if unnecessary notification, for example, desensitizes customers to notices. In that scenario, those reputational costs are themselves reduced as a result of unnecessary notification. *See infra* section IV.D.1.b(4) for a discussion of the effects of unnecessary notification.

revealing when breaches occur, the final amendments will help provide customers with information on the effectiveness of covered institutions' customer information safeguards, further helping customers make better-informed decisions when choosing a covered institution.[437]

To the extent that a covered institution does not have policies and procedures to safeguard customer information and respond to unauthorized access to or use of customer information, it will bear the costs to develop and implement the required policies and procedures for the incident response program.[438] Moreover, transfer agents—who were not subject to any of the customer information safeguard provisions of Regulation S-P prior to this adoption—will 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.[439]

As adopting policies and procedures involves fixed costs, doing so is very likely to impose a proportionately larger compliance cost on smaller covered institutions as compared to larger covered institutions.[440] This may reduce smaller covered institutions' ability to compete with their larger peers, for whom the fixed costs are spread over more customers.[441] However,

---

437 *See infra* section IV.B.

438 *See infra* section IV.D.1 for a discussion of these costs.

439 That is, they will face the compliance costs of the provisions of Regulation S-P not applicable to registered transfer agents before this adoption. *See* 17 CFR 248.30(a). In addition, transfer agents registered with a regulatory agency other than the Commission will face additional compliance costs to develop, implement, and maintain written policies and procedures that address the proper disposal of customer information, as these transfer agents were not subject to the disposal rule before this adoption. *See* 17 CFR 248.30(b); *see also infra* section IV.D.2.b for a discussion of these costs.

440 If both large and small covered institutions were to undertake the same compliance activities, the fixed costs associated with these activities would impose a proportionately larger compliance cost on smaller covered institutions. *See infra* footnote 722. As discussed below, smaller covered institutions may have to undertake additional activities compared to larger covered institutions, which would result in additional burdens. *See, e.g., infra* section IV.D.1.a.

441 *See infra* sections IV.D.1 and IV.E.

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 adoption will significantly alter these challenges. Similarly, although the final amendments may lead to improvements to capital formation, existing state rules are similar in many respects to the amendments, and so we do not expect the amendments to have a significant impact on capital formation vis-à-vis the baseline.[442]

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 final amendments. 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.

B. Broad Economic Considerations

In a market with complete information, customers are able to perfectly observe the quality of the goods and services being provided and the processes and service provider relationships by which they are being provided. Fully-informed customers can then decide what level of quality of good or service to consume, based on their own personal preferences. In this context, one element of a financial service's quality is the customer information safeguards of the firm providing the service, which capture the likelihood of a customer's information being exposed in the event of a breach, as well as the firm's response to such a breach if it were to

[442] We acknowledge, however, that the final amendments could have incremental effects on capital formation, and we discuss these effects below. *See infra* section IV.E.

occur.[443] Under this assumption, a customer is then able to choose a financial firm that offers a service of a quality that meets his or her preferences.[444]

In the context of covered institutions—firms whose services frequently involve custody of highly sensitive customer information—the assumption of complete information is unrealistic. Customers have little visibility into the internal processes of a firm and those of its service providers, so it is impractical for them to directly observe the level of customer information safeguards that a firm is employing.[445] In addition, customers generally do not know how a firm would respond to a breach, including whether and to what extent a firm would inform its customers about such breach.[446] In fact, firms often lack incentives to voluntarily disclose when information breaches occur (and likely have substantial incentives to avoid such disclosures). Hence, customer information could be compromised without the customers being informed or with the customers being only partially informed.[447] As a result, prospective customers have limited ability to choose a covered institution that is offering the service that most closely meets their needs. In addition, current customers may be paying for a service that is of lower quality than they expect.[448] In both cases, customers have limited ability to avoid covered institutions

---

443 The response includes elements such as detection, assessment, recovery, and the communication of the breach to the firm's customers.

444 For example, a customer may be particularly averse to risk and consequently choose a financial firm with a higher level of information safeguards, even if this firm's service is being provided for a higher price.

445 As discussed below, customers already receive some information on covered institutions' customer information safeguards and disclosure of nonpublic personal information to third parties. *See infra* section IV.C.2.c.

446 Even if a firm has been the subject of a breach in the past, it may have changed its procedures since the last breach. In this case, even knowing the firm's response to a previous breach would not be fully informative to customers.

447 Here, customers are "partially informed" if the information they receive about the breach is not sufficient to allow them to take appropriate mitigating actions.

448 It could also be the case that the true quality of the service is higher than what customers expect. In this case, the customers would not be harmed, but the firm would not be fully realizing the benefits from its investment in customer information safeguards.

that fail to protect customer information to the level expected by these customers.[449] Hence, this information asymmetry prevents market forces from penalizing covered institutions that fail to protect customer information, and therefore prevents market forces from yielding economically efficient outcomes. This market failure serves as the economic rationale for this regulatory intervention.

The information asymmetry can lead to three inefficiencies. First, the information asymmetry about specific information breaches that have occurred 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 potential consequences of such breaches. Second, the information asymmetry about covered institutions' efforts at avoiding and limiting the consequences of such breaches can lead to customers choosing financial firms with levels of safeguards different from what they expect, which can result in customers choosing firms that they would not have otherwise chosen if provided with better information. Third, this asymmetry can also reduce covered institutions' incentives to sufficiently safeguard customer information. As a result, they could devote too little effort (i.e., "underspend") toward safeguarding this information, thereby increasing the probability of the

---

449 The release of information about data breaches can lead to loss of customers, reputational harm, litigation, or regulatory scrutiny. *See, e.g.*, U.S. Fed. Trade Comm'n, Press Release, *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach* (July 22, 2019), *available at* https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach. *See also* James Mackay*, 5 Damaging Consequences of Data Breach: Protect Your Assets* (Dec. 15, 2023), *available at* https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach (stating that research has shown that up to a third of customers in retail, finance and healthcare would stop doing business with organizations that have been breached and that 85% would tell others about their experience) and *2019 Consumer Survey: Trust and Accountability in the Era of Data Misuse*, PING IDENTITY, *available at* https://www.pingidentity.com/en/resources/content-library/misc/3464-2019-consumer-survey-trust-accountability.html (last visited Apr. 9, 2024) (describing a survey of more than 4,000 individuals across the U.S., U.K., Australia, France, and Germany which found that 81% of people would stop engaging with a brand online following a data breach; this includes 25% who would stop interacting with the brand in any capacity).

information being compromised in the first place.[450] This scenario is often characterized as a moral hazard problem. When an agent's actions cannot be observed or directly contracted for by the principal, it is difficult to induce the agent to supply the proper amounts of productive inputs.[451] In other words, information asymmetry prevents covered institutions (the agents) that spend more effort on safeguarding customer information from having customers (the principals) recognize their extra efforts and therefore prevents the covered institutions from realizing some of the benefits associated with this additional effort.[452] This reduces the incentives for covered institutions to exert effort towards safeguarding information.[453]

We expect the final amendments may mitigate the inefficiencies described above in several ways. First, by helping facilitate timely and informative notices to customers when their information is compromised, the amendments may mitigate information asymmetries around the

---

450 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), *available at* https://www.iif.com/portals/0/Files/content/cyber_resilience_survey_3.20.2020_print.pdf ("IIF/McKinsey Report"). 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).

451 *See, e.g.*, Bengt Holmstrom, *Moral Hazard and Observability*, 10 BELL J. ECON. 74-91 (1979) ("It has long been recognized that a problem of moral hazard may arise when individuals engage in risk sharing under conditions such that their privately taken actions affect the probability distribution of the outcome […]. The source of this moral hazard or incentive problem is an asymmetry of information among individuals that results because individual actions cannot be observed and hence contracted upon."); Bengt Holmstrom, *Moral Hazard in Teams*, 13 BELL J. ECON. 324-340 (1982) ("Moral hazard refers to the problem of inducing agents to supply proper amounts of productive inputs when their actions cannot be observed and contracted for directly."). In other contexts, moral hazard refers to a party taking on excessive risk when knowing another party will be responsible for negative outcomes. This alternative definition may be viewed as a special case within the broader economic definition associated with the difficulty of contracting for privately taken actions. *See, e.g.*, Adam Carpenter, *Moral Hazard Definition*, U.S. NEWS (Aug. 11, 2022; updated Dec. 8, 2023), *available at* https://money.usnews.com/investing/term/moral-hazard.

452 Such benefits include attracting customers who are willing to pay more for enhanced security, thereby allowing these covered institutions to charge a higher price for their services.

453 This is not to say that firms do not have any incentives to invest in customer information safeguards. As discussed below, firms themselves are hurt by incidents resulting in unauthorized access to or use of customer information and therefore have incentives to invest in safeguards even when these incidents remain unknown to their customers. *See infra* section IV.C.1.

compromise of information and improve customers' ability to take appropriate remedial actions. Second, by revealing when such events occur, the amendments may help customers draw inferences about a covered institution's efforts toward protecting customer information, which might help inform their choice of covered institution and reduce the probability of customers inadvertently choosing a firm that is less likely to meet their preferences or needs.[454] This, in turn, might provide firms with greater incentives to exert effort toward protecting customer information,[455] thereby mitigating the moral hazard problem. And, by imposing a regulatory requirement to develop, implement, and maintain policies and procedures, the final amendments might further enhance firms' cybersecurity preparations and will restrict firms' ability to limit efforts in these areas.

The effectiveness of the final amendments at mitigating these problems will depend on several factors. First, the effectiveness of the amendments will depend on the degree to which breach notification provides customers with sufficient actionable information in a sufficient timeframe to help them mitigate the effects of the compromise of sensitive customer information. Second, it will depend on customers' ability to draw inferences on a covered institution's protection of customer information based on the notifications they receive, or the absence thereof.[456] Third, it will also depend on the degree to which the prospect of issuing such notices—and the prospect of the reputational harm, litigation, and regulatory scrutiny that could

---

454 In the case of transfer agents and funding portals, such effects would usually be mediated through security-issuing firms' choice of transfer agent or funding portal and therefore be less direct. Nonetheless we expect that, all else being equal, firms would prefer to avoid employing the services of transfer agents or funding portals that have been unable to prevent investors' information from being compromised.

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

456 Because breaches can happen even at firms with very high customer information safeguards, and because firms with very low levels of safeguards might never be victim of a breach, customers' ability to draw inferences could be limited.

ensue—helps alleviate underspending on safeguarding customer information.[457] These factors themselves depend on the extent to which covered institutions already have in place processes and practices that satisfy the final requirements and therefore on the extent to which the amendments will induce improvements to existing practices relative to the baseline.[458]

Some commenters supported generally the economic rationale in the Proposing Release.[459] Some of these commenters expressed that the asymmetric information market failure was present in this context.[460] Some commenters stated that this market failure could lead to inefficiencies.[461] One commenter stated that firms "either seek to skirt notification requirements altogether or provide vague or confusing notifications," preventing affected individuals from taking timely actions, and that firms' self-interest could lead them to fail to notify customers

---

457 Although empirical evidence on the effectiveness of notification breach laws (that is, on how such laws help individuals mitigate the effects of a breach and how they prevent such breaches from occurring by influencing firms' levels of safeguards) is quite limited, extant studies suggest that such laws protect consumers from harm. *See* Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT 256 (2011); *see also* Sullivan & Maniff, *supra* footnote 455.

458 This economic analysis presents evidence suggesting that the inefficiencies described above do exist in this context, and therefore suggesting that covered institutions' existing processes and practices can be improved. *See infra* footnote 464 and accompanying text for evidence that some notices do not currently contain sufficient information for customers to take appropriate mitigating actions and *infra* section IV.D.1.b(2) for evidence that such notices are sometimes sent with such delay as to make it difficult for customers to take "timely" mitigating actions; *see also supra* footnote 449 for evidence that customers would modify the firms with which they do business if they learned that this firm was the victim of a breach, suggesting that such customers do draw inferences on firms' customer information safeguards when learning that breaches occur and modify their behavior as a result; *see also infra* section IV.C.1 for evidence that some firms are currently underspending on cybersecurity.

459 *See, e.g.*, Nasdaq Comment Letter; FSI Comment Letter.

460 *See, e.g.*, Better Markets Comment Letter ("But companies will not always disclose data breaches to affected individuals voluntarily. They may be concerned about the damage to their reputation and their bottom line from disclosing a breach."); EPIC Comment Letter ("A company has better visibility than its consumers do into the threats to the privacy and security of consumer data entrusted to that company's custody; and the company's interests are not directly aligned with those of its consumers."); Nasdaq Comment Letter ("Requiring various financial institutions and market entities to address these cybersecurity risks through policies and procedures, incident response programs, third-party management, notifications and/or public disclosures can promote transparency and consistency. Investors, issuers and other market participants benefit from healthy capital markets that promote trust and transparency.").

461 *See, e.g.*, EPIC Comment Letter; Better Markets Comment Letter.

affected by a breach.[462] Another commenter stated its view that firms have a natural tendency to want to avoid making disclosures that could incur liability or lead to a loss of customers.[463] Another commenter stated that beginning in the fourth quarter of 2021, less information started being included in data breach notices and that in 2022, only 34 percent of notices included information about the breaches and their victims.[464] This commenter further added that this lack of actionable information in breach notices prevented individuals from effectively judging the risks they faced and from taking the appropriate actions to protect themselves.[465] One commenter supported the economic rationale of the Proposing Release, stating that stronger notification requirements could effectively incentivize covered institutions to improve their data security practices in order to avoid the reputational harm associated with distributing breach notices.[466]

Other commenters disagreed with the economic rationale in the Proposing Release and stated that covered institutions' level of customer information safeguards and/or breach notification practices were already adequate, and that existing regulation made the amendments unnecessary.[467] We disagree with these commenters that the amendments are unnecessary, even

---

462 *See* EPIC Comment Letter.

463 *See* NASAA Comment Letter.

464 *See* Better Markets Comment Letter, citing IDENTITY THEFT RESOURCE CENTER, DATA BREACH ANNUAL REPORT (Jan 2023), *available at* https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf ("IRTC Data Breach Annual Report").

465 *See* Better Markets Comment Letter.

466 *See* EPIC Comment Letter. This commenter also cited Federal Communications Commission (FCC), *Data Breach Reporting Requirements*, Proposed Rule, FCC 22-102, 88 FR 3953 (Jan. 23, 2023) (stating that the FCC "anticipate[s] that requiring notification for accidental breaches will encourage telecommunications carriers to adopt stronger data security practices and will help us identify and confront systemic network vulnerabilities").

467 *See* ASA Comment Letter (stating that the proposal was not "supported by evidence that brokers are fundamentally failing in their obligations to safeguard investor information and notify government authorities – within applicable Federal and state law – when a significant breach of sensitive information has occurred" and that the Proposing Release did not "provide any discussion about how current broker-dealer cybersecurity and customer notification policies are deficient or in need of a regulatory fix"); ACLI Comment Letter ("The ACLI's members already comply with much of the Proposal's content through state

if some covered institutions may already have policies and procedures in place that satisfy the final amendments' requirements. We have discussed, here and in the Proposing Release, the information asymmetries that prevent customers from knowing whether or how they will be notified of a data breach and from choosing firms based on the level of their customer information safeguards.[468] Furthermore, in addition to describing existing requirements and guidance available to (and potentially adopted by) covered institutions addressing customer information safeguards and customer notification, we have described (here and in the Proposing Release) a variety of practices and state law requirements that could lead to different notification outcomes depending on where the customer resides.[469] In particular, we have described a variety of delays and inconsistencies in notification under existing requirements.[470] Hence, the Proposing Release described in detail the existing regulatory framework and analyzed the benefits and costs of the proposed amendments relative to this framework. In addition, as discussed above, some commenters provided additional evidence of deficiencies in existing practices.[471] Moreover, in response to commenters, we have supplemented the analysis of the amendments' benefits and

---

regulations, such as those that require companies to maintain written cybersecurity policies and procedures, respond to cyber incidents, notify authorities and consumers of certain cyber incidents, and dispose of consumer data. However, we are concerned with the Proposal's shortened notification timeframes and expanded scope."); CAI Comment Letter (stating that "[n]otice currently is given to individuals whose information is reasonably believed to have potentially been affected after the findings of the investigation are determined," that it "believes this current practice is an appropriate and common-sense approach to notification," and that "[t]he new notice requirement proposed under Proposed Rule 30(b) would simply add another layer on top of these existing requirements and would likely go entirely unnoticed by consumers"); Computershare Comment Letter ("Computershare believes Proposed Reg S-P is an unnecessary regulation for transfer agents, as they are already subject, either directly or indirectly, to state, federal or provincial laws designed to protect personal information of securityholders and requiring breach notification."); STA Comment Letter 2 (stating that the proposed amendments would not "meaningfully increase the safeguarding of shareholder information" and instead "cause ambiguity among competing laws.").

468 *See* Proposing Release at section III.B.

469 *See* Proposing Release at section III.C; *see also infra* section IV.C.2.

470 *See* Proposing Release at section III.C.2.a; *see also infra* section IV.C.2.a.

471 *See supra* footnote 460 and accompanying text.

costs, describing in greater detail the changes made by the final amendments over the baseline.[472] We summarize these changes below. We have also supplemented the analysis of the expected benefits and costs of expanding the scope of the safeguards and disposal rules to include transfer agents.[473]

In particular, the variety of practices and state law requirements that could lead to different notification outcomes under existing requirements provides a further rationale for the rule and motivated specific differences in the final amendments relative to state laws. We discuss the effects of these differences in detail below,[474] but for example, the required timing of notification in the final amendments is stricter than under many state laws. The analysis in section IV.D.1.b(2) provides evidence that currently, many customers receive notification long after the event. The amendments are designed to help ensure that customers receive notification in a timely manner. In addition, the notification obligation covers a set of customer information that is broader than in many state laws, thereby covering more data breaches. Moreover, the final amendments require certain information to be included in the notice sent to customers. This requirement will help ensure that customers receive relevant information, allowing them to take appropriate mitigating actions in case of a breach. Hence, while the final amendments contain some requirements that are similar to those in some existing state laws, the final requirements are stricter than many state laws and may therefore lead to customers receiving additional, timelier, and more relevant notices than under existing regulations.[475] In addition, variations in state law

---

472 *See infra* section IV.D.

473 *See infra* section IV.D.2.b.

474 *See infra* section IV.D.1.

475 It is possible that, because of the overlap with state laws, some covered institutions already have policies and procedures in place satisfying the final amendments' requirements. For these institutions and their customers, both the benefits and the costs of the amendments will be limited.

requirements highlight the need for a consistent Federal minimum standard for covered institutions. Such a standard will protect all customers regardless of their state of residence and reduce the potential confusion that could result from customers in one state receiving notice of an incident while customers in another state do not.

Other commenters stated that the analysis in the Proposing Release underestimated the costs of the amendments.[476] Some commenters also stated that the proposed amendments in general would be very costly to implement for smaller covered institutions.[477] As discussed more fully below, we expect some of the changes made to the final amendments to result in lower costs relative to the proposal.[478] For example, the changes made to the service provider provisions of the amendments (requiring that covered institutions oversee service providers instead of requiring written contracts between covered institutions and their service providers, and requiring that the covered institution's policies and procedures be reasonably designed to ensure service providers take appropriate measures to notify covered institutions of an applicable breach in security within 72 hours instead of 48 hours) may reduce some costs relative to the proposal and facilitate their implementation, especially for smaller covered institutions.[479] In addition, in a change from proposal, we are adopting longer compliance periods for all covered institutions, and an even longer compliance period for smaller covered institutions,[480] who are less likely to already have policies and procedures broadly consistent with the final amendments.

---

476 *See, e.g.*, IAA Comment Letter 1 ("We urge the Commission to undertake a more expansive, accurate, and quantifiable assessment of the specific and cumulative costs, burdens, and economic effects that would be placed on advisers by the proposed requirements, as well as of the potential unintended consequences for their clients.").

477 *See, e.g.*, ASA Comment Letter; IAA Comment Letter 1.

478 *See, e.g.*, *infra* sections IV.D.1.c and IV.E.

479 *See supra* section II.A.4; *infra* section IV.D.1.c.

480 *See supra* section II.F.

C. Baseline

The baseline against which the costs, the benefits, and the effects on efficiency, competition, and capital formation of the final amendments are measured consists of current requirements for customer notification and information safeguards, current practice as it relates to customer notification and information safeguards, and the current market structure and regulatory framework. The economic analysis appropriately considers existing regulatory requirements, including recently adopted Commission rules as well as state, federal, and foreign laws and regulations, as part of the economic baseline against which the costs and benefits of the final amendments are measured.[481]

Several commenters requested that the Commission consider interactions between the economic effects of the proposal and other recent Commission proposals.[482] The Commission adopted several of the rules mentioned by commenters, namely the Electronic Recordkeeping

---

481 *See, e.g.*, *Nasdaq* v. *SEC*, 34 F.4th 1105, 1111-15 (D.C. Cir. 2022). This approach also follows SEC staff guidance on economic analysis for rulemaking. *See* SEC Staff, *Current Guidance on Economic Analysis in SEC Rulemaking* (Mar. 16, 2012), *available at* https://www.sec.gov/divisions/riskfin/rsfi_guidance_econ_analy_secrulemaking.pdf ("The economic consequences of proposed rules (potential costs and benefits including effects on efficiency, competition, and capital formation) should be measured against a baseline, which is the best assessment of how the world would look in the absence of the proposed action."); *Id.* at 7 ("The baseline includes both the economic attributes of the relevant market and the existing regulatory structure."). The best assessment of how the world would look in the absence of the proposed or final action typically does not include recently proposed actions, because that would improperly assume the adoption of those proposed actions.

482 *See, e.g.*, IAA Comment Letter 2; IAA Comment Letter 1; CAI Comment Letter; Comment Letter of the Securities Industry and Financial Markets Association, et al. (Mar. 31, 2023) ("SIFMA Comment Letter 1"). *See also* Comment Letter of the Investment Company Institute (Aug. 17, 2023) ("ICI Comment Letter 2") (stating the Commission should analyze the interconnections in related rules).

Adopting Release,[483] the Form N-PX Adopting Release,[484] the Settlement Cycle Adopting Release,[485] the May 2023 SEC Form PF Adopting Release,[486] the Public Company Cybersecurity

---

483 *Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants*, Release No. 34-96034 (Oct. 12, 2022) [87 FR 66412 (Nov. 3. 2022)] ("Electronic Recordkeeping Adopting Release"). One commenter stated that the Proposing Release could create concurrent obligations with Rule 17a-4 and Rule 18a-6. *See* AWS Comment Letter. Rule 17a-4 and Rule 18a-6 were amended in the Electronic Recordkeeping Adopting Release. Those amendments modified requirements regarding the maintenance and presentation of electronic records, the use of third-party recordkeeping services, and prompt production of records. The compliance dates were May 3, 2023, and Nov. 3, 2023. *See* Electronic Recordkeeping Adopting Release, section II.I.

484 *Enhanced Reporting of Proxy Votes by Registered Management Investment Companies; Reporting of Executive Compensation Votes by Institutional Investment Managers,* Release Nos. 33–11131, 34-96206, IC-34745 (Nov. 2, 2022) [87 FR 78770 (Dec. 22, 2022)] ("Form N–PX Adopting Release"). The Form N–PX amendments enhanced the information funds report publicly about their proxy votes, and apply to most registered management investment companies. The effective date is July 1, 2024. Form N-PX Adopting Release, section II.K.

485 *Shortening the Securities Transaction Settlement Cycle,* Release No. 34-96930 (Feb. 15, 2023) [88 FR 13872 (Mar. 6, 2023)] ("Settlement Cycle Adopting Release"). This rule shortens the standard settlement cycle for most broker-dealer transactions from two business days after the trade date to one business day after the trade date. To facilitate orderly transition to a shorter settlement cycle, the rule requires same-day confirmations, allocations, and affirmations for processing transactions subject to the rule, and requires registered investment advisers to make and keep records of each confirmation received, and of any allocation and each affirmation sent or received, with a date and time stamp for each indicating when it was sent or received. With certain exceptions, the rule has a compliance date of May 28, 2024. Settlement Cycle Adopting Release, sections VII, VII.B.3.

486 *Form PF; Event Reporting for Large Hedge Fund Advisers and Private Equity Fund Advisers; Requirements for Large Private Equity Fund Adviser Reporting,* Investment Company Act Release No. 6297 (May 3, 2023) [88 FR 38146 (June 12, 2023)] ("May 2023 SEC Form PF Adopting Release"). The Form PF amendments adopted in May 2023 require large hedge fund advisers and all private equity fund advisers to file reports upon the occurrence of certain reporting events. The compliance dates are Dec. 11, 2023, for the event reports in Form PF sections 5 and 6, and June 11, 2024, for the remainder of the Form PF amendments in the May 2023 SEC Form PF Adopting Release. *See* May 2023 SEC Form PF Adopting Release, section II.E.

Rules,[487] the Money Market Fund Adopting Release,[488] the Investment Company Names Adopting Release,[489] the Beneficial Ownership Adopting Release,[490] the Private Fund Advisers

---

487 Public Company Cybersecurity Rules, *supra* footnote 14. The amendments require current disclosure about material cybersecurity incidents, and periodic disclosures about a registrant's processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks. With respect to Item 106 of Regulation S-K and item 16K of Form 20-F, all registrants must provide disclosures beginning with annual reports for fiscal years ending on or after Dec. 15, 2023. With respect to incident disclosure requirements in Item 1.05 of Form 8-K and in Form 6-K, all registrants other than SRCs were required to begin complying on Dec. 18, 2023; SRCs must begin complying with Item 1.05 of Form 8-K on June 15, 2024. With respect to structured data requirements, all registrants must tag disclosures beginning one year after the initial compliance date: specifically, beginning with annual reports for fiscal years ending on or after Dec. 15, 2024, in the case of Item 106 of Regulation S-K and item 16K of Form 20-F, and beginning Dec. 18, 2024, in the case of Item 1.05 of Form 8-K and Form 6-K. Cybersecurity Disclosure Adopting Release, section II.I.

488 *Money Market Fund Reforms; Form PF Reporting Requirements for Large Liquidity Fund Advisers; Technical Amendments to Form N-CSR and Form N-1*, Release No. 33-11211 (July 12, 2023) [88 FR 51404 (Aug. 3, 2023)] ("Money Market Fund Adopting Release"). The amendments are designed to improve the resilience and transparency of money market funds by increasing minimum liquidity requirements to provide a more substantial buffer in the event of rapid redemptions; removing provisions that permitted a money market fund to temporarily suspend redemptions, and removing the regulatory tie between the imposition of liquidity fees and a fund's liquidity level; requiring certain money market funds to implement a liquidity fee framework that will better allocate the costs of providing liquidity to redeeming investors; and enhancing certain reporting requirements. The Money Market Fund Adopting Release has compliance dates of Oct. 2, 2024, for implementing mandatory liquidity fees and of Apr. 2, 2024, for discretionary liquidity fees; a compliance date of Apr. 2, 2024, for minimum liquidity requirements and weighted average maturity calculations; a compliance date of June 11, 2024, for certain form amendments and website reporting requirements; and an effective date of Oct. 2, 2023, for other provisions. Money Market Fund Adopting Release, section II.H.

489 *Investment Company Names*, Release No. 33-11238 (Sept. 20, 2023) [88 FR 70436 (Oct. 11, 2023)], as amended by *Investment Company Names; Correction*, Release No. 33-11238A (Oct. 24, 2023) [88 FR 73755 (Oct. 27, 2023)] ("Investment Company Names Adopting Release"). The amendments broaden the scope of the requirement for certain funds to adopt a policy to invest at least 80 percent of the value of their assets in accordance with the investment focus that the fund's name suggests; require enhanced prospectus disclosure for terminology used in fund names; impose related notice, recordkeeping, and reporting requirements. The compliance date for the final amendments is Dec. 11, 2025, for larger entities and June 11, 2026, for smaller entities. *See* Investment Company Names Adopting Release, sections II.H, IV.D.3.

490 *Modernization of Beneficial Ownership Reporting,* Release No. 33-11253 (Oct. 10, 2023) [88 FR 76896 (Nov. 7, 2023)] ("Beneficial Ownership Adopting Release"). Among other things, the amendments generally shorten the filing deadlines for initial and amended beneficial ownership reports filed on Schedules 13D and 13G, and require that Schedule 13D and 13G filings be made using a structured, machine-readable data language. The amendments are effective Feb. 5, 2024. The new filing deadline for Schedule 13G will not be required before Sept. 30, 2024, and the rule's structured data requirements have a one-year implementation period ending Dec. 18, 2024. Beneficial Ownership Adopting Release, section II.G.

Adopting Release,[491] the Securitizations Conflicts Adopting Release,[492] and the February 2024 Form PF Adopting Release.[493] These adopted rules are part of the baseline against which this economic analysis considers the benefits and costs of the final amendments. In response to commenters, this economic analysis also considers potential economic effects arising from the extent to which there is any overlap between the compliance period for the final amendments and the compliance periods for these other adopted rules.[494]

---

491 *Private Fund Advisers; Documentation of Registered Investment Adviser Compliance Reviews*, Release No. IA-6383 (Aug. 23, 2023) [88 FR 63206 (Sept. 14, 2023)] ("Private Fund Advisers Adopting Release"). The Commission adopted five new rules and two rule amendments as part of the reforms. The compliance date for the quarterly statement rule and the audit rule is Mar. 14, 2025, for registered private fund advisers. For the adviser-led secondaries rule, the preferential treatment rule, and the restricted activities rule, the Commission adopted staggered compliance dates that provide for the following compliance periods: for advisers with $1.5 billion or more in private funds assets under management, a 12-month compliance period (ending on Sept. 14, 2024) and for advisers with less than $1.5 billion in private funds assets under management, an 18-month compliance period (ending on Mar. 14, 2025). The amended Advisers Act compliance provision for registered investment advisers had a Nov. 13, 2023, compliance date. *See* Private Fund Advisers Adopting Release, sections IV, VI.C.1.

492 *Prohibition Against Conflicts of Interest in Certain Securitizations*, Release No. 33-11254 (Nov. 27, 2023) [88 FR 85396 (Dec. 7, 2023)] ("Securitizations Conflicts Adopting Release"). The new rule prohibits an underwriter, placement agent, initial purchaser, or sponsor of an asset-backed security (including a synthetic asset-backed security), or certain affiliates or subsidiaries of any such entity, from engaging in any transaction that would involve or result in certain material conflicts of interest. The compliance date for securitization participants to comply with the prohibition is Jun. 9, 2025. Securitizations Conflicts Adopting Release, section II.I.

493 *Form PF: Reporting Requirements for All Filers and Large Hedge Fund Advisers*, Release No. IA-6546 (Feb. 8, 2024) [89 FR 17984 (Mar. 12, 2024)] ("February 2024 Form PF Adopting Release"). The Form PF amendments are designed to enhance the Financial Stability Oversight Council's ability to monitor systemic risk as well as bolster the SEC's regulatory oversight of private fund advisers and investor protection efforts. The compliance date for the rule is Mar. 12, 2025. February 2024 Form PF Adopting Release, section II.F.

494 *See infra* sections IV.D and IV.E. In addition, commenters indicated there could be overlapping compliance costs between the final amendments and proposals that have not been adopted. *See, e.g.*, IAA Comment Letter 2, Exhibit A; IAA Comment Letter 1; CAI Comment Letter; FSI Comment Letter. Proposed rules that commenters mentioned included *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, Release No. 33-11028 (Feb. 9, 2022), 87 FR 13524 (Mar. 9, 2022); *Enhanced Disclosures by Certain Investment Advisers and Investment Companies About Environmental, Social, and Governance Investment Practices*, Release No. 33-11117 (Oct. 7, 2022) [87 FR 63016] (Oct. 18, 2022)]; *Open-End Fund Liquidity Risk Management Programs and Swing Pricing; Form N-PORT Reporting*, Release No. 33-11130 (Nov. 2, 2022), [87 FR 77172 (Dec. 16, 2022)]; *Safeguarding Advisory Client Assets*, Release No. IA-6240 (Feb. 15, 2023), [88 FR 14672 (Mar. 9, 2023)]; and *Cybersecurity Risk Management 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*

The parties directly affected by the final amendments, the "covered institutions,"[495] include every broker-dealer (3,476 entities),[496] every funding portal (92 entities),[497] every investment company (13,766 distinct legal entities),[498] every investment adviser (15,565 entities) registered with the Commission,[499] and every transfer agent (315 entities) registered with the Commission or another appropriate regulatory agency.[500] In addition, the final amendments will affect current and prospective customers of covered institutions as well as certain service providers to covered institutions.[501] The final amendments will impact hundreds of millions of customers. For example, as discussed in more detail in subsequent sections, carrying broker-

---

Transfer Agents, Release No. 34-97142 (Mar. 15, 2023) [88 FR 20212 (Apr. 5, 2023)]. To the extent those proposals are adopted, the baseline in those subsequent rulemakings will reflect the existing regulatory requirements at that time.

495 *See infra* section IV.C.3.

496 Of these, 303 are dually registered as investment advisers. *See infra* section IV.C.3.a. These numbers exclude notice-registered broker-dealers, who will be deemed in compliance with the final provision through the substituted compliance provisions of Regulation S-P. *See supra* section II.B.3. For this release, the number of broker-dealers dually registered as investment advisers was estimated based on FOCUS filings for broker-dealers during the third quarter of 2023, Form BD filings as of Sept. 2023, and Form ADV filings for investment advisers as of Oct. 5, 2023. The Proposing Release cited a figure of 502 as of Dec. 2021. The correct number of broker-dealers dually registered as investment advisers as of Dec. 2021 in the Proposing Release should be 328. This change would not have affected the Commission's assessment of economic effects at Proposal as these assessments were focused primarily on effects at the level of individual covered institutions and their customers.

497 *See infra* section IV.C.3.b.

498 *See infra* section IV.C.3.d, in particular Table 4, for statistics on the different types of investment companies. 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 (although BDCs and ESCs are not grouped in families, *see* Form N-2 and Form 40-APP). *See infra* footnote 660. We estimate there are 313 such families. *See infra* section IV.C.3.d. For this release, the number of families was estimated by counting unique family names in Form N-CEN filings as of Sept. 30, 2023. The Proposing Release cited a figure of 1,093 using 2021 N-CEN filings. The correct number of distinct fund families using 2021 N-CEN filings in the Proposing Release should be 327. This change would not have affected the Commission's assessment of economic effects at Proposal as these assessments were focused primarily on effects at the level of individual covered institutions and their customers.

499 *See infra* section IV.C.3.c.

500 *See infra* section IV.C.3.e.

501 *See infra* section IV.C.3.f.

dealers report a total of 233 million customer accounts,[502] registered investment advisers report a total of more than 51 million individual clients,[503] and transfer agents report around 250 million individual accounts.[504]

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. This trend has also applied to the financial services industry.[505] Alongside this progress, the industry has observed increased exposure to cyberattacks that threaten not only the financial firms themselves, but also their customers. Hence, the trend toward digitization has increasingly turned the problem of safeguarding customer records and information into one of cybersecurity.[506] Cyber threat intelligence surveys find the financial sector to be a highly attacked industry,[507] making the problem of cybersecurity particularly acute for financial firms. The customer records and information in their possession can be quite

---

502 *See infra* section IV.C.3.a.

503 *See infra* section IV.C.3.c.

504 *See infra* section IV.C.3.e.

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

506 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 Apr. 9, 2024); 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 Apr. 9, 2024).

507 *See, e.g.*, IBM, *X-Force Threat Intelligence Index 2022* (Feb. 2022), *available at* https://www.ibm.com/downloads/cas/ADLMYLAZ.

sensitive (e.g., personal identifying information, bank account numbers, financial transactions) and their compromise could lead to substantial harm.[508]

Certain recent changes in the industry, including changes discussed by commenters, have continued the trend toward digitization and the importance of cybersecurity. For example, the shift to remote work has brought new cybersecurity challenges. One commenter stated that 91 percent of data security professionals saw negative risk implications from remote and hybrid work.[509] The same commenter cited a report finding that in 2022, the cost of a data breach was on average nearly $1 million higher when remote work was a factor in the breach and more than $1 million higher in organizations with a share of employees working remotely between 80 percent and 100 percent compared with organizations where less than 20 percent of employees worked remotely.[510] Remote work arrangements have significantly expanded following the onset of the COVID-19 pandemic in the United States in 2020,[511] and a recent study found the financial services industry to be the fifth most flexible industry in terms of work location flexibility.[512]

---

508 *See, e.g.*, David W. Opderbeck, *Cybersecurity and Data Breach Harms: Theory and Reality*, 82 MD. L. REV. 1001 (2023) ("A criminal actor can use stolen PII in true identity theft to open new lines of credit in the victim's name, including new credit cards, personal loans, business loans, or mortgages. Criminal actors also employ true identity theft to file for tax refunds, welfare, insurance, or pension benefits in the victim's name.").

509 *See* Better Markets Comment Letter, citing Hugo Guzman, *Remote Work Leading to Big Data-Loss Problems*, LAW.COM (Mar. 7, 2023).

510 *See* Better Markets Comment Letter citing IBM, *Cost of a Data Breach Report 2022* (July 2022) ("2022 IBM Cost of Data Breach Report"), *available at* https://www.ibm.com/downloads/cas/3R8N1DZJ. The 2023 version of the same report does not address remote work specifically.

511 Census 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.

512 *See* THE FLEX INDEX, Q3 2023 FLEX REPORT, *available at* https://www.flex.scoopforwork.com/reports/flex-report-2023-q3 (last visited Apr. 9, 2024).

The financial sector is one of the biggest spenders on cybersecurity measures: a recent survey found that financial firms spent an average of approximately 13.6 percent of their technology budget on cybersecurity in 2023, compared to an overall average across industries of 11.6 percent.[513] 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 percent of financial firms self-reported "underspending" on cybersecurity measures.[514] In addition, some covered institutions increasingly use third-party vendors to provide a wide range of functions, which may implicate a review of those service providers' cybersecurity controls.[515]

Before adopting these amendments, the Commission did not require covered institutions to notify customers (or the Commission) in the event of a data breach, and so statistics relating to data breaches that occurred at covered institutions were not readily available. However, data compiled from notifications required under various state laws indicate that in 2022 the number of data breaches reported in the U.S. was 1,802—a 3 percent decrease over 2021, but a 63 percent increase over 2020.[516] Of these, 268 (15 percent) were reported by firms in the financial services

---

513 *See* James Rundle, *Cybersecurity Budgets Grow, But at a Slower Pace*, WALL ST J. (Sept. 29, 2023), *available at* https://www.wsj.com/articles/cybersecurity-budgets-grow-but-at-a-slower-pace-89ce3d3c. One commenter agreed that total cybersecurity costs are significant. *See* Better Markets Comment Letter ("While the magnitude of dollar losses is difficult to estimate, it is clear that companies must expend significant resources to prevent breaches, detect breaches that do occur, contain the damage from breaches, prevent future breaches, and in some cases make customers whole.").

514 *See* IIF/McKinsey Report, *supra* footnote 450.

515 *See*, *e.g.*, FINRA, *Regulatory Notice 21-29: Vendor Management and Outsourcing* (Aug. 13, 2021), *available at* https://www.finra.org/sites/default/files/2021-08/Regulatory-Notice-21-29.pdf (encouraging firms that "use – or are contemplating using – Vendors to review […] obligations and assess whether their supervisory procedures and controls for outsourced activities or functions are sufficient to maintain compliance with applicable rules"). *See also infra* section IV.C.3.f for a discussion of different types of covered institutions' reliance on service providers.

516 *See* IRTC Data Breach Annual Report.

industry.[517] However, the report estimating these statistics states that the 1,802 breaches reported are a minimum estimate and states that in the U.S., the number of breach notices issued per business day in 2022 (7 notices) was much lower than in the European Union (356 notices) in 2021 (the last year for which data is available).[518] One commenter cited a report stating that nearly half of U.S. consumers had been affected by data breaches where a firm holding their personal data was hacked, compared to a global average of 33 percent of consumers.[519]

The average total cost of a data breach for a U.S. firm in 2023 was estimated to be $9.48 million by one report.[520] While the report does not provide estimates for U.S. financial services firms specifically, it estimated that world-wide, the cost of a data breach for financial services firms averaged $5.90 million, and that average costs for U.S. firms were approximately twice the world-wide average.[521] Hence, we can estimate that for U.S. financial firms, the cost of a data breach was about $12 million. The bulk of these costs is attributed to detection and escalation (36 percent), lost business (29 percent), and post-breach response (27 percent); customer notification is estimated to account for only a small fraction (8 percent) of these costs.[522] For the U.S. financial industry as a whole, this implies an estimate of aggregate notification costs under

---

517 *See id.*

518 *See id. See also* Better Markets Comment Letter. The report suggests that this disparity may be related to the fact that in the European Union, enforcement officials, together with the organization affected by a breach, make the determination that the breach puts individuals or businesses at risk and therefore requires notification. *See also infra* section IV.D.1.b(4).

519 *See* EPIC Comment Letter, citing THALES, 2022 THALES CONSUMER DIGITAL TRUST INDEX (Sept. 2022).

520 *See* IBM, COST OF A DATA BREACH REPORT 2023 (July 2023) ("2023 IBM Cost of Data Breach Report"), *available at* https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700077723822555&p5=p&&msclkid=45aa555fae8d1f62fb9c3066eddb719a&gclid=45aa555fae8d1f62fb9c3066eddb719a&gclsrc=3p.ds.

521 The 2023 IBM Cost of Data Breach Report estimates that the global average cost of a data breach is $4.45 million. One commenter, citing the 2022 IBM Cost of Data Breach Report, stated that the average cost of a data breach in 2022 was $4.35 million, which is a global average. *See* Better Markets Comment Letter. In the Proposing Release, we also cited the 2022 IBM Cost of Data Breach Report and stated that the cost of a data breach was $9.44 million, which applies to U.S. firms specifically.

522 *See* 2023 IBM Cost of Data Breach Report.

the baseline of between $200 million and $250 million.[523] Because these estimates are based on data breach incidence rates for all firms, and because financial firms are part of one of the most attacked industries,[524] the actual aggregate notification costs are likely higher than this estimated range.

Some commenters supported the Proposing Release's assessment that data breaches are an important risk currently faced by covered institutions and their customers.[525] One commenter cited an article describing a data breach at a financial institution that had cost that institution more than $150 million.[526] Commenters also mentioned additional types of risks. One commenter stated that in addition to the financial costs imposed on firms by data breaches, individuals whose sensitive information is compromised also suffer harms, both financial and psychological, as many become victims of identity theft.[527] Another commenter stated that the consequences of these breaches were staggering and that the Commission's proposals to establish minimum standards for incident response and breach notification could help with mitigation.[528] The same commenter cited a report by the Government Accountability Office indicating that past victims of identity theft, which can be a consequence of data breaches, have

---

523 The $200 million figure is based on 8% (the customer notification portion) of an average cost of $9.48 million multiplied by 268 data breaches. The $250 million figure is based on the same calculation but using $12 million instead of $9.48 million. *See supra* footnotes 516 and 520 and accompanying text.

524 *See supra* footnotes 507-512 and accompanying text.

525 *See, e.g.*, Better Markets Comment Letter; Nasdaq Comment Letter.

526 *See* Better Markets Comment Letter, citing Emily Flitter & Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, N.Y. TIMES (July 29, 2019), *available at* https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.

527 *See* Better Markets Comment Letter. Citing the IRTC Data Breach Annual Report, the same commenter also stated that globally, organizational data compromises impacted over 392 million individual victims in 2022.

528 *See* EPIC Comment Letter.

"lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft."[529]

2. Regulations and Guidelines

Two features of the existing regulatory framework are most relevant to the amendments: existing regulations that require covered institutions to notify customers in the event that their information is compromised; and existing regulations and guidelines that affect covered institutions' practices for safeguarding customers' information. While the relevance of the former is obvious, the latter is potentially more significant: regulations aimed at improving firms' practices for 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 as well as existing annual notice delivery requirements.

a. State Law Customer Notification Requirements

(1) Scope of 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 (46), a notification obligation is triggered only when there is unauthorized acquisition, while a handful of states (5) require notification whenever there is unauthorized access.[530]

---

529 *See* EPIC Comment Letter citing U.S. Government Accountability Office, GAO-14-34, *Agency Responses to Breaches of Personally Identifiable Information Need to be More Consistent* (Dec. 2013), *available at* http://www.gao.gov/assets/660/659572.pdf.

530 *See, e.g.*, notification requirements in California (Cal. Civ. Code § 1798.82(a)) and Texas (Tex. Bus. & Com. Code § 521.053) triggered by the unauthorized acquisition of certain information, as compared to

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 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.[531] A typical enhanced definition includes 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.[532] Enhanced definitions also trigger notification requirements 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.[533] Most states (37) adopt some form of enhanced definition, while a minority (14) adopt a basic definition.

One commenter stated that all states provided an exception to the notification requirement if the data compromised were encrypted.[534] We found that states may include an

---

notification requirements in Florida (Fla. Stat. § 501.171) and New York (N.Y. Gen. Bus. Law § 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 Sept. 2023 versions of state codes.

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

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

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

534 *See* SIFMA Comment Letter 2 ("Note that all U.S. state data breach notification laws provide an encryption

explicit encryption or redaction exception in their definition of personal information,[535] in their definition of breach,[536] or in the determination that notification of affected individuals is necessary.[537] Multiple states include at least two of these exceptions. States vary, however, in the whether and how they define encryption or redaction.[538]

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").[539] Twenty of these states do not have a presumption of notification and instead require notification only if, for example, an investigation reveals a risk of harm or misuse.[540] Although the types of harms vary by state, they most commonly include: "harm" generally (13), identity theft or other fraud (10), or misuse of personal information (8). Figure 1 plots the frequency of the various types of harms referenced in states' no-harm exceptions.

---

safe harbor."); *see also* Liisa M. Thomas, THOMAS ON DATA BREACH: A PRACTICAL GUIDE TO HANDLING DATA BREACH NOTIFICATIONS WORLDWIDE (Feb. 2023), at § 2:45 ("Thomas 2023").

535 *See, e.g.*, Kan. Stat. § 50-7a01(g) (defining "personal information" to include a consumer's first name or first initial and last name linked to any one or more of the specified data elements that relate to the consumer, when the data elements are neither encrypted nor redacted); Wyo. Stat. § 40-12-501 (defining "personal identifying information" to exclude redacted data elements).

536 *See, e.g.*, Ariz. Code § 18-551 (defining "breach" to include unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and unredacted computerized personal information).

537 *See, e.g.*, Minn. Stat. § 325E.61(a) (requiring notification of a breach to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person).

538 We considered a safe harbor from the notification requirements for encrypted information. *See infra* section IV.F.3.

539 *See, e.g.*, Fla. Stat. § 501.171(4)(c) and N.Y. Gen. Bus. Law § 899-AA(2)(a). Eight states, including California and Texas, do not have a no-harm exception and require notification even in the cases where there is no risk of harm.

540 *See, e.g.*, N.C. Stat. § 75-61(14) and Utah Code 13-44-202(1).

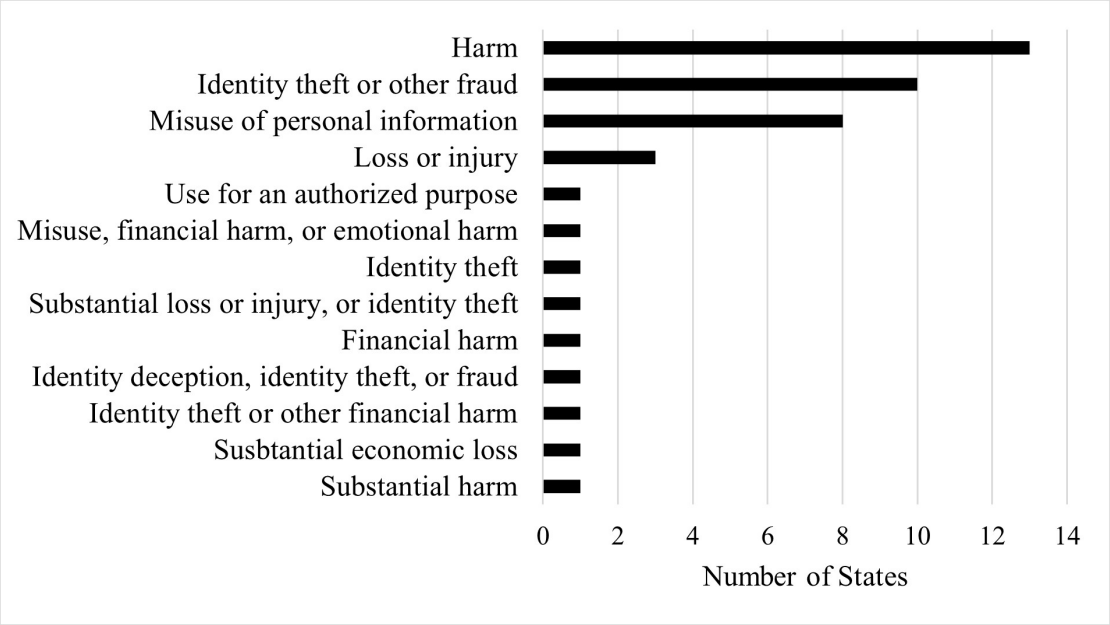

Figure 1: Frequency of types of harms referenced by state laws with no-harm exceptions to notification requirements. Data source: State law in 2023.

(2) Timing, Content, and Method of Notification

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").[541] 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).[542] All states allow for a delay if it is requested by a law enforcement

---

541 *See, e.g.*, Cal. Civ. Code § 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).

542 *See, e.g.*, Colo. Rev. Stat. § 6-1-716(2)(a) (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. § 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).

agency.[543] Additionally, some states allow for a delay if necessary to determine the nature and scope of the breach or to restore the reasonable integrity of the information system.[544] Figure 2 plots the frequency of different notification deadlines in state laws. For states with specific deadlines, the figure distinguishes between states that allow an exception to determine the nature and scope of the breach or to restore the reasonable integrity of the information system, and those that do not.[545]

---

543 *See, e.g.*, Ala. Stat. § 8-38-5(c) ("If a federal or state law enforcement agency determines that notice to individuals required under this section would interfere with a criminal investigation or national security, the notice shall be delayed upon the receipt of written request of the law enforcement agency for a period that the law enforcement agency determines is necessary."); Ark. Code § 4-110-105(c) ("The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation."); Conn. Stat. § 36a-701b.(d) ("Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed."); Md. Comm. Code § 14-3504(d)(1) (notice may be delayed if "a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security"); N.C. Stat. § 75-65(c) ("The notice required by this section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation.").

544 *See, e.g.*, Tex. Bus. & Com. Code § 521.053 (notice to be made "without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system").

545 We conducted this supplemental analysis to help analyze and respond to comments, and also to provide additional context for our analysis of the possible effects of the final amendments. *See infra* section IV.D.1.b(2).

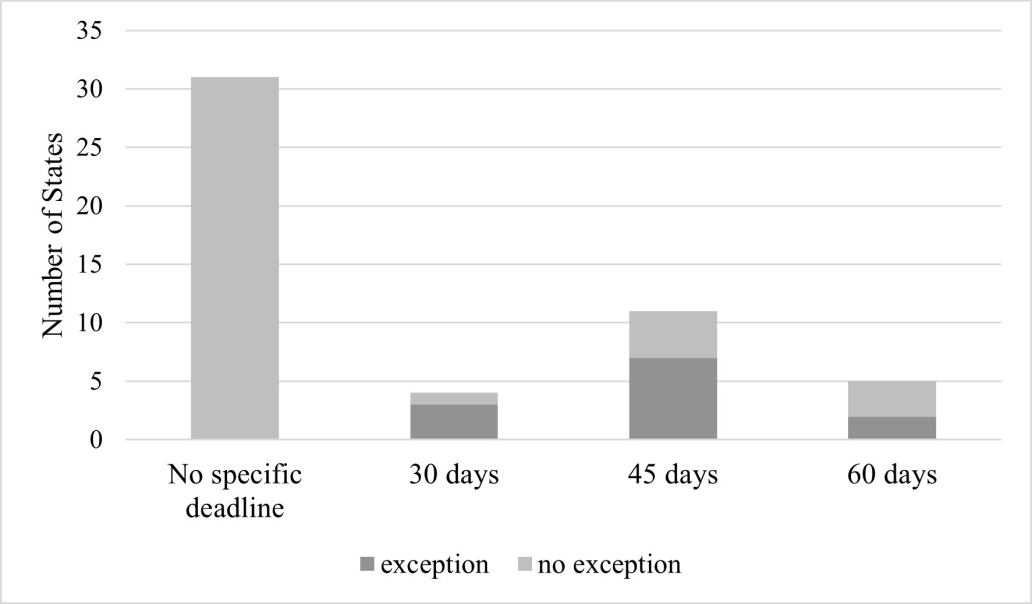

Figure 2: Frequency of notification deadlines in state laws. "Exception" states allow an exception to determine the nature and scope of the breach or to restore the reasonable integrity of the information system. Data source: State law in 2023.

One commenter stated that, where state laws have a 30-day notice requirement, the 30-day periods generally do not begin to run until a determination has been made that the incident affected residents of that state that will require notice, and that the Commission's proposed 30-day requirement would be triggered much sooner in the process.[546] The same commenter also stated that notices are currently sent to individuals whose information is reasonably believed to have potentially been affected after the findings of an investigation are determined.[547] To help analyze and respond to these comments, and also to provide additional context for our analysis of

[546] *See* CAI Comment Letter ("While the Commission correctly notes in the S-P Proposing Release that some existing state laws also include a 30-day notice requirement, those requirements generally do not begin to run until a determination has been made that the incident affected residents of that state that will require notice."). In the final amendments, as in the proposal, the beginning of the 30-day outside timeframe is a covered institution "becoming aware" that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred. *See* proposed rule 248.30(b)(4)(iii); final rule 248.30(a)(4)(iii).

[547] *See* CAI Comment Letter.

the possible effects of the final amendments,[548] we conducted supplemental analysis of the frequency of different triggers for the specific deadline requirement in the 20 states that specify such a deadline. The results of this analysis are in Figure 3 and demonstrate variation in triggering events. For example, state laws specify that the notification of customers be made "not later than sixty days from the discovery of the breach,"[549] or "no later than 30 days after the determination of a breach or reason to believe a breach occurred."[550] Many of these triggers use words such as "determination" or "confirmation," which, consistent with the commenter's observation, suggests investigation that might cause the specific deadline to be triggered later than the Commission's proposed or adopted notification trigger, although "discovery of breach"—used in five states—could potentially be earlier.[551]

---

548 *See infra* section IV.D.1.b(2).

549 *See* La. Rev. Stat. § 51:3074.

550 *See* Fla. Stat. § 501.171(4)(a).

551 *See infra* section IV.D.1.b(2).

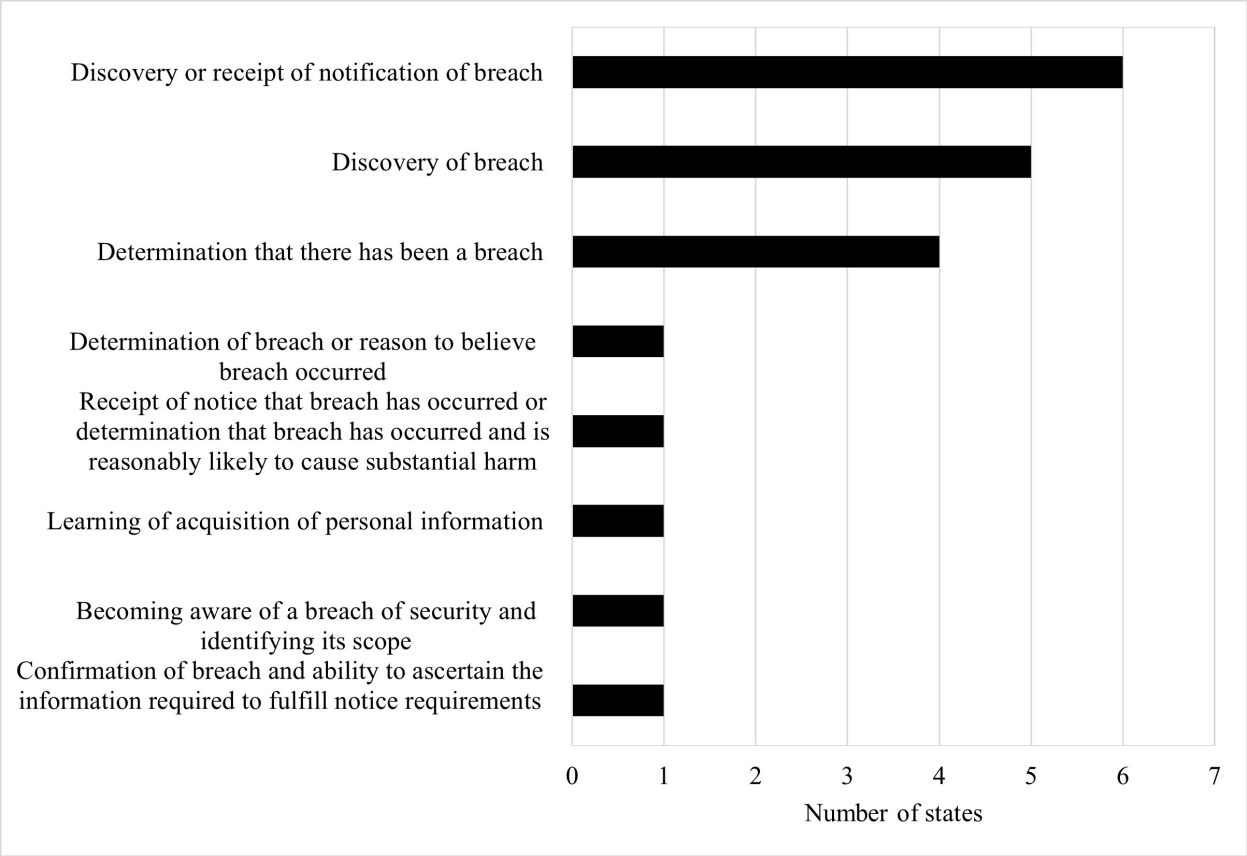

Figure 3: Frequency of triggers of notification deadline, for the 20 states that specify such a deadline. Data source: State law in 2023.

One commenter stated that most state data breach notification laws did not specify a number of days to report a breach, and that of the states that did have a specific timeframe, many had an exception allowing for compliance with the GLBA in lieu of adherence to their timeframes.[552] To help analyze and respond to this comment, and also to provide additional context for our analysis of the possible effects of the final amendments, we conducted supplemental analysis of the overlap between states that have a specific deadline and states that

[552] *See* SIFMA Comment Letter 2.

include a GLBA exception.[553] We found that of the 20 states that have a specific deadline, 10 do not include a GLBA exception.[554]

Additionally, one commenter stated the establishment of a Federal minimum standard for data breach notification would satisfy state notice laws that provide exemptions for firms subject to such a requirement.[555] To help analyze and respond to this comment, and also to provide additional context for our analysis of the possible effects of the final amendments,[556] we conducted supplemental analysis of this question. We have found that some states excuse entities from individual notification under state law if the entities comply with the notification requirements of a Federal regulator or, in some cases, another state. Some states allow these substitute notifications to replace their own state-specific requirements on notice content and timing,[557] while others only allow it if the provisions are at least as protective as state law.[558]

Some commenters stated that different state laws currently have different requirements as to what content must be included in a notice to customers.[559] One of these commenters further

---

553 *See infra* section IV.D.1.b(1).

554 We discuss this exception and the states where it applies in section IV.D.1.b(1).

555 *See* IAA Comment Letter 1.

556 *See infra* section IV.D.1.b.

557 *See*, *e.g.*, Fla. Stat. § 501.171(4)(g) ("Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to be in compliance with the notice requirement in this subsection …."); Va. Code. Ann. § 18.2-186.6(H) ("An entity that complies with the notification requirements … established by the entity's primary or functional state or federal regulator shall be in compliance with this section."). According to Thomas 2023, approximately 15 states allow compliance with a primary regulator to replace their own state's required notification in some circumstances; *see also* ICI Comment Letter 1 ("Today, approximately 13 states provide an exemption or exclusion from the state's breach notice requirements if the entity experiencing the breach has a duty under federal law to provide notice of the breach."). *See also infra* section IV.D.1.b(1) on GLBA safe harbor provisions, which are similar but distinct.

558 *See*, *e.g.*, Colo. Rev. Stat. 6-1-716(3)(b) ("In the case of a conflict … the law or regulation with the shortest timeframe for notice to the individual controls."); Iowa Code § 715C.2(7)(b) (exempting in the case of compliance "with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section").

559 *See, e.g.*, IAA Comment Letter 1.

stated that, as a result, covered institutions may, when they experience a data breach incident today, send different notification letters to residents of different states for the same incident.[560] To help analyze and respond to these comments, and to provide additional context for our analysis of the possible effects of the final amendments,[561] we conducted supplemental analysis of the frequency at which different items are currently required by state laws to be included in notices to customers. This analysis, shown in Figure 4, supports commenters' observation that different states have different requirements. While half of the states do not have such requirements, many states (25) provide minimum content to be included in the notices sent to individuals whose information has been affected by a breach. The most common required items include the type of information affected, contact information for consumer reporting agencies, and the date of the breach. Figure 4 plots the frequency of different items required by state laws to be included in the notices.

---

560 *See* ICI Comment Letter 1 ("In discussing breach notices with our members, we understand it is not uncommon for their current breach response programs to include separate notification letters depending upon the state the individual resides in."). One benefit of the final amendments will be to help ensure that all customers receive a minimum level of information regarding a given breach. *See infra* section IV.D.1.b(5).

561 *See infra* section IV.D.1.b(5).

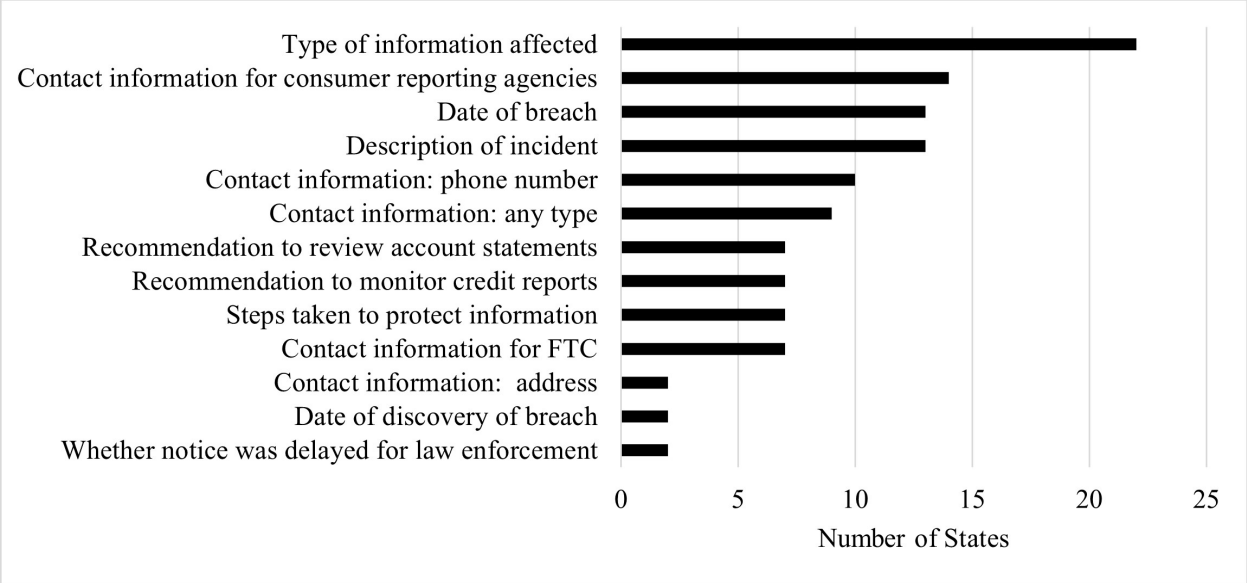

Figure 4: Frequency of different items required by state laws to be included in the notices to affected individuals. Date source: State law in 2023.

States also differ in their requirements regarding the method that must be used to notify affected individuals.[562] While all states allow for a written notification, most states impose conditions if the notice is sent electronically. For example, 37 states provide that a notice can be sent electronically only if the notice is consistent with the Electronic Signatures in Global and National Commerce Act.[563] Fifteen states have as a condition that a primary method of communication between the entity and the affected residents be by electronic means.[564] Five states impose no condition for electronic notices,[565] and 2 states only require that the notifying

[562] We conducted this supplemental analysis to help analyze and respond to comments, and also to provide additional context for our analysis of the possible effects of the final amendments. *See infra* section IV.D.1.b(5).

[563] 15 U.S.C. 7001, et seq. *See, e.g.*, Cal. Civ. Code § 1798.82(j); Conn. Stat. § 36a-701b.(e); Ga. Code § 10-1-911(4); Tex. Bus. & Com. Code § 521.053(e).

[564] *See. e.g.*, Colo. Rev. Stat. § 6-1-716(1)(F); Del. Code Tit. 6 § 12B-101(5); Tenn. Code Ann. § 47-18-2107(e).

[565] *See, e.g.*, Ala. Code § 8-38-5(d); Fla. Stat. § 501.171(4)(d); Va. Code. Ann. § 18.2-186.6(A).

institution have the email address of the affected individuals.[566] In addition, 26 states allow for the notice to be made over the phone.[567] Of these 26 states, 7 provide that a condition for a telephonic notice is that contact is made directly with the affected individuals.[568]

All states allow, under some conditions, for substitute notification instead of the required methods of notification discussed above. The most common conditions include a specified large number of individuals to notify and/or a minimum dollar cost to notify the affected individuals. These conditions vary widely across states.[569] In most states, a substitute notice consists of all of the following elements: email notification to the affected individuals, a notice on the institution's website, and notification to major statewide media.[570] However, other states have fewer requirements.[571]

(3) Notification by Service Providers

Some data breach incidents involve service providers. Covered institutions may use service providers to perform certain business activities and functions, such as trading and order

---

566 *See* Ariz. Code § 18-552(F); Ind. Code 24-4.9-3-4.

567 *See. e.g.*, Conn. Stat. § 36a-701b.(e); N.Y. Gen. Bus. Law § 899-AA(5); 73 Pa. Stat. § 2302.

568 *See, e.g.*, Ariz. Code § 18-552(F); Mo. Stat. 407.1500 § 2(6); 9 Vt. Stat. Ann. § 2435(b)(6)(A).

569 For example, some states allow for a substitute notice if the number of affected individuals is above 1,000 or 5,000 or if the cost of providing notice is above $5,000 or $10,000, while many states have a threshold of 500,000 affected individuals or a cost threshold of $250,000. *See, e.g.*, Maine Rev. Stat. Tit. 10 § 1347(4); Miss. Code § 75-24-29(6); N.H. Rev. Stat. § 359-C:20(III); Cal. Civ. Code § 1798.82(j); Fla. Stat. § 501.171(4)(f); N.Y. Gen. Bus. Law § 899-AA(5).

570 *See, e.g.*, D.C. Code § 28-3851(2); La. Rev. Stat. § 51:3074(G); N.J. Stat. § 56:8-163(d).; Va. Code. Ann. § 18.2-186.6(A).

571 *See, e.g.*, Ala. Code § 8-38-5(e) ("Substitute notice shall include both of the following: 1. A conspicuous notice on the Internet website of the covered entity, if the covered entity maintains a website, for a period of 30 days. 2. Notice in print and in broadcast media, including major media in urban and rural areas where the affected individuals reside."); Fla. Stat. § 501.171(4)(f) ("Such substitute notice shall include the following: 1. A conspicuous notice on the Internet website of the covered entity if the covered entity maintains a website; and 2. Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside."); Tex. Bus. & Com. Code § 521.053(f) (requiring that under certain conditions, "the notice may be given by: (1) electronic mail, if the person has electronic mail addresses for the affected persons; (2) conspicuous posting of the notice on the person's website; or (3) notice published in or broadcast on major statewide media").

management, information technology functions, and cloud 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 general, state laws require persons and entities that maintain computerized data for other entities, but do not own or license that data, to notify the data-owning entity in the event of a data breach (so as to allow that entity to notify affected individuals).[572] However, 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.[573] In addition, some states impose the responsibility of notifying affected individuals on entities that maintain or possess the data even if they do not own or license it.[574]

Some commenters opposed the proposed provision that would have required service providers to notify covered institutions of a breach of sensitive customer information within 48 hours.[575] A commenter further stated that our analysis of the effects of this requirement was

---

572 *See, e.g.*, Cal. Civ. Code § 1798.82(b); D.C. Code § 28-3852(b); N.Y. Gen. Bus. Law § 899-AA(3); Tex. Bus. & Com. Code § 521.053(c).

573 *See, e.g.*, Fla. Stat. § 501.171(6)(b); Ala. Code § 8-38-8. We do not have information on the frequency of such arrangements.

574 *See, e.g.*, Ky. Rev. Stat. 365.732(2) ("Any information holder shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of Kentucky whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."); Maine Rev. Stat. Tit. 10 § 1348(1)(B). ("If any other person who maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the person shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur."). *See also* Thomas 2023, at § 2:21.

575 *See, e.g.*, ACLI Comment Letter.

incomplete.[576] We conducted supplemental analysis of the notification timeframe required by state laws for entities that do not own or license the compromised data to help analyze and respond to these comments, and to provide additional context for our analysis of the possible effects of the final amendments.[577]

In general, state laws provide a window for notification of the entity that owns or licenses the data by the entity that maintains the data.[578] Ten states provide a specific deadline of either 24 hours (one state),[579] 10 days (four states),[580] 45 days (four states),[581] or 60 days (one state).[582]

---

576 *See* Microsoft Comment Letter ("The cost-benefit analyses of the Proposed Rules do not identify why a 48-hour or shorter reporting period is optimal."). *See also supra* section II.A.4 for a discussion of the length of notification period.

577 *See infra* section IV.D.1.c.

578 A small number of states do not require such a notification. For example, Rhode Island does not distinguish between entities that own or license the data and those entities that do not, requiring all entities to notify customers directly (R.I. Gen. Laws § 11-49.3-4(a)(1) ("Any municipal agency, state agency, or person that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information shall provide notification as set forth in this section of any disclosure of personal information, or any breach of the security of the system, that poses a significant risk of identity theft to any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity."). Similarly, South Dakota does not have a provision for persons or businesses that do not own or license computerized personal data (SDCL §§ 22-40-19 through 22-40-26).

579 *See* Ga. Code § 10-1-912(b) ("Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own shall notify the information broker or data collector of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.").

580 *See, e.g.*, Md. Comm. Code § 14-3504(c) ("Except as provided in subsection (d) of this section, the notification required under paragraph (1) of this subsection shall be given as soon as reasonably practicable, but not later than 10 days after the business discovers or is notified of the breach of the security of a system.").

581 *See, e.g.*, Tenn. Code Ann. § 47-18-2107(c) ("Any information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of system security if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement, as provided in subsection (d).").

582 *See* La. Rev. Stat. § 51:3074(E) ("The notification required pursuant to Subsections C and D of this Section shall be made in the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach, consistent with the legitimate needs of law enforcement, as provided in Subsection F of this Section, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.").

Thirty-eight states provide instead a general principle such as "as soon as practicable" or "without unreasonable delay."[583] In particular, 24 states require the notification to take place immediately after the discovery of the breach or the determination that a breach has occurred.[584] Figure 5 plots the frequency of these different provisions across state laws. This variation across state laws in timelines for (1) notification of the entity that owns or licenses the data by the entity that maintains the data and (2) notification of the affected individuals by the entity that owns or licenses the data can result in widely different lengths of time between the discovery of a breach and the time the affected individuals are notified. In addition, variations in these state laws could result in residents of one state receiving notice while residents of another receive no notice for the same data breach incident.[585]

---

583 *See, e.g.*, Miss. Code § 75-24-29(4) ("Any person who conducts business in this state that maintains computerized data which includes personal information that the person does not own or license shall notify the owner or licensee of the information of any breach of the security of the data as soon as practicable following its discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes."); Va. Code. Ann. § 18.2-186.6(D) ("An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system").

584 *See, e.g.*, Ark. Code § 4-110-105(b), N.C. Stat. § 75-65(b), and Utah Code 13-44-202(3). For many of these states, this immediate notification can be delayed if the delay is requested by a law enforcement agency.

585 *See supra* footnote 578 on South Dakota. In addition, 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 § 75-24-29(4) (requiring notification if the information was or is reasonably believed to have been acquired by an unauthorized person for fraudulent purposes); Colo. Rev. Stat. § 6-1-716(2)(b) (requiring notification if misuse of personal information about a Colorado resident occurred or is likely to occur).

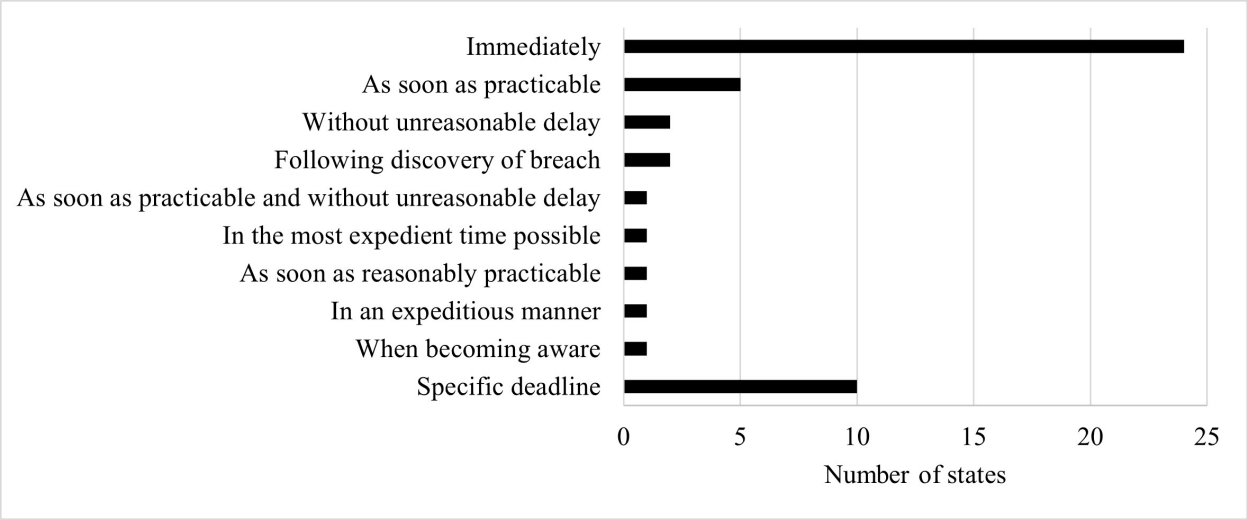

Figure 5: Frequency of timeline requirements for notification of entities that own or license data by entities that maintain but do not own or license data in case of breach in state laws. Data source: State law in 2023.

Some of the service providers that will be affected by the final amendments are covered institutions themselves.[586] Also, some entities that are covered institutions but not service providers under the final amendments could, under state law, be entities that maintain but do not own or license that data, meaning they may have an obligation under state law to notify the data owner.[587] In particular, commenters stated that transfer agents were generally considered service providers of the securities issuers under state laws.[588] State laws typically require transfer agents to notify the securities issuers in case of security breach, which in turn must notify the affected customers. One commenter stated that transfer agents were, in addition, often required by contract to notify their securities issuer clients in case of data breach.[589] Another commenter

586 *See supra* section II.A.3.a.

587 This could be the case, for example, of transfer agents providing services only to publicly traded companies that are not covered institutions.

588 *See, e.g.*, Computershare Comment Letter ("It is also contrary to privacy laws that deem the issuer to be the 'controller' or 'business' with respect to securityholders and their data and deem the transfer agent based on its role to be the 'processor' or 'service provider.'").

589 *See* STA Comment Letter 2.

stated that it was not uncommon for covered institutions to require, by contract or agreement, that their service providers, including transfer agents, notify them in case of security breach.[590] Hence, we expect that all or almost all covered institutions and their service providers are already complying with one or more notification requirements, pursuant to either state law or contract.[591]

b. Customer Information Safeguards

Regulation S-P, prior to the adoption of the amendments, required all covered institutions to adopt written policies and procedures reasonably designed to: "(i) insure [sic] 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."[592] In addition, Regulation S-P established limitations on how covered institutions may disclose nonpublic personal information about a consumer to nonaffiliated third parties.[593] It also established limitations on the further disclosure of nonpublic personal information received by a covered institution from a nonaffiliated financial institution, as well as limitations on the further disclosure of nonpublic personal information disclosed from a covered institution to a nonaffiliated third party.[594] Before this adoption, Regulation S-P did not

---

590 *See* ICI Comment Letter 1.

591 Even if a state does not have specific requirements for entities that do not own or license computerized personal or protected information (such as South Dakota, *see supra* footnote 578), it is unlikely, by the nature of the transfer agent business, that a transfer agent would have access to customer information of individuals residing in this state only.

592 17 CFR 248.30. *See also* 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 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); *see also supra* section II.B.2 explaining that prior to these final amendments, the safeguards rule did not apply to any transfer agents, and the disposal rule applied only to transfer agents registered with the Commission.

593 *See* 17 CFR 248.10.

594 *See* 17 CFR 248.11.

include specific provisions for how covered institutions were to satisfy their obligations to safeguard customer records and information when utilizing service providers.

Covered institutions that hold transactional accounts for consumers may also be subject to Regulation S-ID.[595] 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.[596]

In addition, broker-dealers that operate alternative trading systems exceeding specified volume thresholds are SCI entities subject to Regulation SCI and required, among other things, to have certain policies and procedures reasonably designed to ensure that their market systems have adequate levels of capacity, integrity, resiliency, availability, and security and take appropriate corrective action when "SCI events" occur.[597] SCI entities are required to disseminate information to their members or participants about certain types of SCI events.[598] Upon the SCI entity having a reasonable basis to conclude that a certain type of SCI event (such as a "systems intrusion" that is not de minimis) has occurred, it is generally required to promptly

---

595 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, funding portals, investment companies, and some registered investment advisers. *See* 17 CFR 248.201; *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"); *see also* 17 CFR 227.403(b).

596 In a 2017 Risk Alert, the SEC Office of Compliance Inspections and Examinations (now called the Division of Examinations) noted that, based on observations from examinations of 75 registrants, nearly all examined broker-dealers and most of the examined 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. In addition, affected entities must also periodically update their identity theft programs. *See* 17 CFR 248.201. 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).

597 Regulation SCI is codified at 17 CFR 242.1000 through 1007.

598 17 CFR 242.1002(c).

disseminate information about the SCI event to those members and participants that the SCI entity has reasonably estimated may have been affected. If such "SCI event" is "major," the information disseminated must be to all of the entity's members or participants.[599] When required, the notification must include a summary description of the systems intrusion, including a description of the corrective action taken by the SCI entity and when the systems intrusion has been or is expected to be resolved, unless the SCI entity determines that dissemination of such information would likely compromise the security of the SCI entity's SCI systems or indirect SCI systems, or an investigation of the systems intrusion, and documents the reasons for such determination.[600] Therefore, information about an "SCI event" caused by a cybersecurity incident may be required to be disseminated to some or all an SCI entity's members or participants pursuant to Regulation SCI.

The safeguards rule of Regulation S-P did not, before this adoption, apply to transfer agents. In addition, the disposal rule did not apply to transfer agents registered with a regulatory agency other than the Commission.[601] Thus, for these institutions, the final amendments create new requirements to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information and to take reasonable measures to protect against unauthorized access to or use of consumer information and customer information in connection with its disposal.[602] Some transfer agents registered with a regulatory agency other than the Commission may already be subject to some of the Federal regulation described below. In addition, many states impose requirements regarding the safeguarding and

---

599 17 CFR 242.1002(c)(3).

600 17 CFR 242.1002(c).

601 *See supra* section II.B.2.

602 *See* final rule 240.30(a)(1) and 240.30(b).

the disposal of customer information.[603] Hence, many transfer agents are likely to already have policies and procedures in the areas covered by these new requirements.

Some covered institutions may also be subject to other regulators' rules and guidelines implicating customer information safeguards. Transfer agents supervised by one of the Banking Agencies may be subject to the Banking Agencies' Incident Response Guidance and to the Banking Agencies' Safeguards Guidance, for example.[604] The Banking Agencies' Incident Response Guidance requires covered financial institutions to develop a response program covering assessment, notification to relevant regulators and law enforcement, incident

---

603 Twenty states have customer information safeguard requirements, and 30 states have customer information disposal requirements. *See, e.g.*, Cal. Civ. Code § 1798.81.5 ("A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."); Del. Code Tit. 6 § 12B-100 ("Any person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business."); Fla. Stat. § 501.171(2) ("Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information."). *See also, e.g.*, Cal. Civ. Code § 1798.81 ("A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means."); La. Rev. Stat. § 51:3074(B) ("Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information shall take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means."); N.J. Stat. § 56:8-162 ("A business or public entity shall destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means.").

604 *See* Banking Agencies' Incident Response Guidance and Banking Agencies' Safeguards Guidance; *see also* Computershare Comment Letter ("Many registered transfer agents like Computershare US and Computershare Canada entities are banks or trust companies, and therefore already subject to state, federal, or provincial banking laws, rules, regulations and inter-agency guidelines." The commenter also refers to "Title V, Subtitle A, of the Gramm–Leach–Bliley Act, 15 U.S.C. 6801–6809; 12 CFR 30, Appendix B to Part 30 - Interagency Guidelines Establishing Information Security Standards; and New York State Department of Financial Services Cybersecurity Regulation, 23 NYCRR Part 500.").

containment, and customer notice.[605] These guidelines require customer notification if a financial institution determines that misuse of sensitive customer information "has occurred or is reasonably possible."[606] 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."[607] 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."[608] 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.[609] The Banking Agencies' Safeguards Guidance directs every financial institution covered by the guidelines 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.[610] In addition, the Banking Agencies' Incident Response Guidance directs that an institution's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the financial

---

605 *See* Banking Agencies' Incident Response Guidance at Supplement A, section II.A.

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

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

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

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

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

institution's customer information, including notification to the institution as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.[611]

The Banking Agencies' Safeguards Guidance requires certain financial institutions to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the entity and the nature and scope of its activities.[612] This guidance requires that the information security program be designed to (1) ensure the security and confidentiality of customer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and (4) ensure the proper disposal of customer information and consumer information.[613]

Private funds may be subject to the FTC's recently amended FTC Safeguards Rule, which contains data security requirements to protect customer financial information.[614] The FTC Safeguards Rule generally requires financial institutions to develop, implement, and maintain a comprehensive information security program,[615] defined as 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.[616] The rule also

---

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

612 *See* Banking Agencies' Safeguards Guidance, at section II.A.

613 *See id.*, at section II.B.

614 The FTC Safeguards Rule applies to financial institutions of certain types "that are not otherwise subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6805." *See* 16 CFR 314.1(b). Private funds that are able to rely on section 3(c)(1) or 3(c)(7) of the Investment Company Act are not subject to Regulation S-P but they may be subject to the FTC Safeguards Rule. *See supra* footnote 2. Investment advisers registered with the Commission, including those that are advisers to private funds, are covered institutions for the purposes of the final amendments.

615 *See* 16 CFR 314.3(a).

616 *See* 16 CFR 314.2(i).

requires that the comprehensive information security program contain various elements, including an incident response plan.[617] 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 to require those service providers by contract to implement and maintain such safeguards.[618] Since the date of our proposal, the FTC Safeguards Rule has been updated to require financial institutions to notify the FTC as soon as possible, and no later than 30 days after discovery, of a security breach involving the unencrypted information of at least 500 consumers.[619] Although the FTC Safeguards Rule does not contain a customer notification requirement, the FTC indicated that it "intends to enter notification event reports into a publicly available database" unless a law enforcement official requests delay.[620]

In addition, many entities covered by this rule may be subject to other, more general information protection requirements.[621] In particular, companies operating in foreign jurisdictions may need to comply with information protection requirements in their foreign markets. For example, the GDPR requires entities that process the personal data of EU citizens or residents to, among other things, do so in a manner that ensures appropriate security, integrity, and

---

617 *See* 16 CFR 314.4(h).

618 *See* 16 CFR 314.4(f). The FTC Safeguards Rule does not contain a requirement that financial institutions require their service providers to notify them in case of a breach resulting in customer information being compromised.

619 The amendments are effective May 13, 2024. *See Standards for Safeguarding Customer Information*, 88 FR 77499 (Nov. 13, 2023); *see also* FTC Press Release, *FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches* (Oct. 27, 2023), *available at* https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-amends-safeguards-rule-require-non-banking-financial-institutions-report-data-security-breaches.

620 88 FR at 77506. *See also* 16 CFR 315.4(j)(vi) (effective May 13, 2024), describing the conditions for a delay in notifying the public of the breach, if requested by law enforcement.

621 *See supra* Section I (discussing other requirements); footnotes 245, 257 (examples of other regimes); *see also* Microsoft Comment Letter.

confidentiality.[622] Other recent regulations in foreign jurisdictions may subject covered institutions to further rules intended to address cybersecurity risk management by financial institutions and some of their service providers.[623] Hence, we expect that some of the entities covered by the final amendments, or their service providers, already have customer information safeguards in place because of other information protection regimes.

A variety of guidance is available to institutions seeking to address information security risk, particularly through the development of policies and procedures. These include NIST and CISA voluntary standards, both of which include assessment, containment, and notification elements similar to those included in these amendments.[624] 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, and no commenter suggested such data. However, past Commission examination sweeps of broker-dealers and investment advisers suggest that such practices are widespread.[625] Thus, we expect that

---

622 GDPR, *supra* footnote 245, at Art. 5(1)(f); *see also What is GDPR, the EU's New Data Protection Law?*, *available at* https://gdpr.eu/what-is-gdpr/ (last visited Apr. 8, 2024). The GDPR places data protection obligations on organizations that process the personal data of EU citizens and residents. Among these are provisions requiring notification in the case of a breach: Art. 34(1), for example, requires a personal data breach to be "communicated to the data subject without undue delay" when the breach is likely to result in a high risk to the rights and freedoms of natural persons, unless certain exceptions (including an encryption exception) apply.

623 *See, e.g.*, *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations*, OFFICIAL J. OF THE EURO. UNION (2022), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554 ("DORA").

624 *See* NIST Special Publication 800-61, Revision 2 (Aug. 2012) ("NIST Computer Security Incident Handling Guide"), *available at* https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final and CISA, Cybersecurity Incident & Vulnerability Response Playbooks (Nov. 2021) ("CISA Incident Response Playbook"), *available at* https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

625 *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 examined broker-dealers (82%) and the examined advisers (51%), discuss mitigating the effects of a cybersecurity incident and/or outline the plan to recover from such an incident.

institutions seeking 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.

c. Annual Notice Delivery Requirement

Under the baseline,[626] a broker-dealer, funding portal, 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.[627] 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.[628]

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.[629] The privacy notices also must describe the type of information the institution collects, how it protects the confidentiality and security of nonpublic personal

---

Similarly, most of the examined broker-dealers (88%) and many of the examined advisers (53%) reference published cybersecurity risk management standards.).

626 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* FAST Act, Pub. L. 114-94, § 75001, adding section 503(f) to the GLBA, codified at 15 U.S.C. 6803(f).

627 17 CFR 248.4 and 248.5.

628 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 with a new nonaffiliated third party that was adequately disclosed in the prior privacy notice.

629 *See* 17 CFR 248.6(a)(2) through (5) and 248.6(a)(9).

information, a description of any opt out right, and certain disclosures the institution makes under the FCRA.[630]

3. Market Structure

The final amendments will affect five categories of covered institutions: broker-dealers other than notice-registered broker-dealers, funding portals, 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

Broker-dealers include both brokers (persons engaged in the business of effecting transactions in securities for the account of others),[631] as well as dealers (persons engaged in the business of buying and selling securities for their own accounts).[632] Most brokers and dealers maintain customer relationships, and are thus likely to come into the possession of sensitive

---

630 *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).

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

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

customer information.[633] 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.[634] 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) 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 and Form BD filings, there were 3,476 registered broker-dealers during the third quarter of 2023.[635] Of these, 303 were dually registered as investment advisers.[636] There were over 233 million customer accounts reported by carrying brokers.[637] However, the majority of broker-dealers are not "carrying broker-dealers" and

---

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

634 *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.

635 The numbers in this section exclude notice-registered broker-dealers. *See supra* section II.B.3.

636 *See supra* footnote 496.

637 FOCUS filings and Form X-17A-5 Schedule I, Item I8080. For this release, the number of customer accounts reported by carrying brokers was estimated based on FOCUS filings during the third quarter of 2023 and Form X-17A-5 Schedule I, Item I8080 for 2022. The Proposing Release cited a figure of 72 million as of July 1, 2022. The correct number of customer accounts reported by carrying brokers as of July 1, 2022, in the Proposing Release should be 220 million. This change would not have affected the Commission's assessment of economic effects at Proposal as these assessments were focused primarily on effects at the level of individual covered institutions and their customers.

therefore do not report the numbers of customer accounts.[638] Therefore, we expect that this figure of 233 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.[639] 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. Funding Portals

Funding portals act as intermediaries in facilitating securities-based crowdfunding transactions that are subject to Regulation Crowdfunding.[640] Securities-based crowdfunding involves using the Internet to raise capital through small individual contributions from a large number of people. The crowdfunding transaction must be conducted through an intermediary registered with the Commission, but a statutory exemption allows that intermediary to forgo registration as a broker-dealer. Therefore some, but not all, crowdfunding intermediaries are registered broker-dealers while others are funding portals.

Funding portals are registered with the Commission and are members of FINRA.[641] They must provide investors with educational materials, take measures to reduce the risk of fraud,

---

638 *See* General Instructions to Form CUSTODY (as of Sept. 30, 2022).

639 This information includes name, address, age, and tax identification or Social Security number. *See* FINRA Rule 4512.

640 *See* 17 CFR part 227.

641 *See* Regulation Crowdfunding, Release No. 33-9974, (Oct. 30, 2015) [80 FR 71388 (Nov. 16, 2015)] ("Regulation Crowdfunding Adopting Release"). An entity raising funds through securities-based crowdfunding typically seeks small individual contributions from a large number of people. Individuals interested in the crowdfunding campaign—members of the "crowd"—may share information about the project, cause, idea or business with each other and use the information to decide whether to fund the campaign based on the collective "wisdom of the crowd." The JOBS Act established a regulatory structure for startups and small businesses to raise capital through securities offerings using the Internet through

make information available about the issuer and the offering, and provide communication channels to permit discussions about offerings on the funding portal's platform, among other related services.[642] In facilitating crowdfunding transactions, funding portals may come into possession of investors' sensitive customer information, as investors are required to open an account with the funding portal before the funding portal may accept an investment commitment from them.[643] Funding portals may have possession of sensitive customer information but, unlike broker-dealers, funding portals are statutorily prohibited from holding, managing, possessing, or handling investor funds or securities.[644] These funding portals are required to direct investors to transmit money or other consideration for the securities directly to a qualified third party that has agreed in writing to hold the funds for the benefit of investors and the issuer and to promptly transmit or return the funds to the person entitled to the funds.[645]

As of December 31, 2023, there were 92 registered funding portals that were members of FINRA (excluding funding portals that had withdrawn their registration and FINRA

---

crowdfunding. *See id*. at section I.A. Securities Act section 4(a)(6) provides an exemption from registration for certain crowdfunding transactions. 15 U.S.C. 77d(a)(6). A company issuing securities in reliance on rules established by the Regulation Crowdfunding Adopting Release (17 CFR part 227, "Regulation Crowdfunding") is permitted to raise a maximum of $5 million in a twelve-month period and is required to conduct the transaction exclusively through an intermediary registered with the Commission, either a broker-dealer or a funding portal. *See* 17 CFR 227.100(a).

642 *See* Regulation Crowdfunding Adopting Release at section II.

643 *See* 17 CFR 227.302(a)(1). Regulation Crowdfunding Rule 302 does not prescribe specific information that a funding portal must collect as part of opening an account.

644 *See* 15 U.S.C. § 78c(a)(80)(D).

645 *See* 17 CFR 227.303(e)(2), which defines a "qualified third party" as (i) a registered broker or dealer that carries customer or broker or dealer accounts and holds funds or securities for those persons or (ii) a bank or credit union (where such credit union is insured by National Credit Union Administration) that has agreed in writing either to hold the funds in escrow for the persons who have the beneficial interests therein and to transmit or return such funds directly to the persons entitled thereto when so directed by the funding portal as described in paragraph (e)(3) of the rule, or to maintain a bank or credit union account (or accounts) for the exclusive benefit of investors and the issuer.

membership).[646] The crowdfunding intermediary market is highly concentrated.[647] For example, based on staff analysis from May 16, 2016 (inception of Regulation Crowdfunding) through December 31, 2023, five intermediaries accounted for 70 percent of all initiated offerings, including one funding portal accounting for 29 percent of all initiated offerings.[648]

c. 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.[649] Although advisers engaged in any of these activities are likely to possess sensitive customer information, the degree of sensitivity will vary widely across advisers. Some advisers may only hold the customer's address, payment details, and the customer's overall financial condition, while others may hold account numbers, tax identification numbers, access credentials to brokerage accounts, and other highly sensitive information.

Based on Form ADV filings received up to October 5, 2023, there are 15,565 investment advisers registered with the Commission with a total of more than 51 million individual clients and $114 trillion in assets under management.[650] Practically all (97 percent) of these advisers reported providing portfolio management services to their clients.[651] Over half (57 percent)

---

646 *See* FINRA, "Funding Portals We Regulate," at https://www.finra.org/about/funding-portals-we-regulate.

647 The crowdfunding intermediary market includes all funding portals and some registered broker-dealers who may also serve as intermediaries of Regulation Crowdfunding transactions. *See* 17 CFR 227.300(a).

648 Based on staff analysis of EDGAR filings under Regulation Crowdfunding as of December 31, 2023. This includes all initiated offerings facilitated by either funding portals or registered broker-dealers.

649 *See* Form ADV.

650 Form ADV, Items 5D(a-b) (as of Oct. 5, 2023). Broadly, regulatory assets under management capture 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.

651 Form ADV, Items 5G(2-5) (as of Oct. 5, 2023).

reported having custody of clients' cash or securities either directly or through a related person,[652] with client funds in custody totaling $43 trillion.[653]

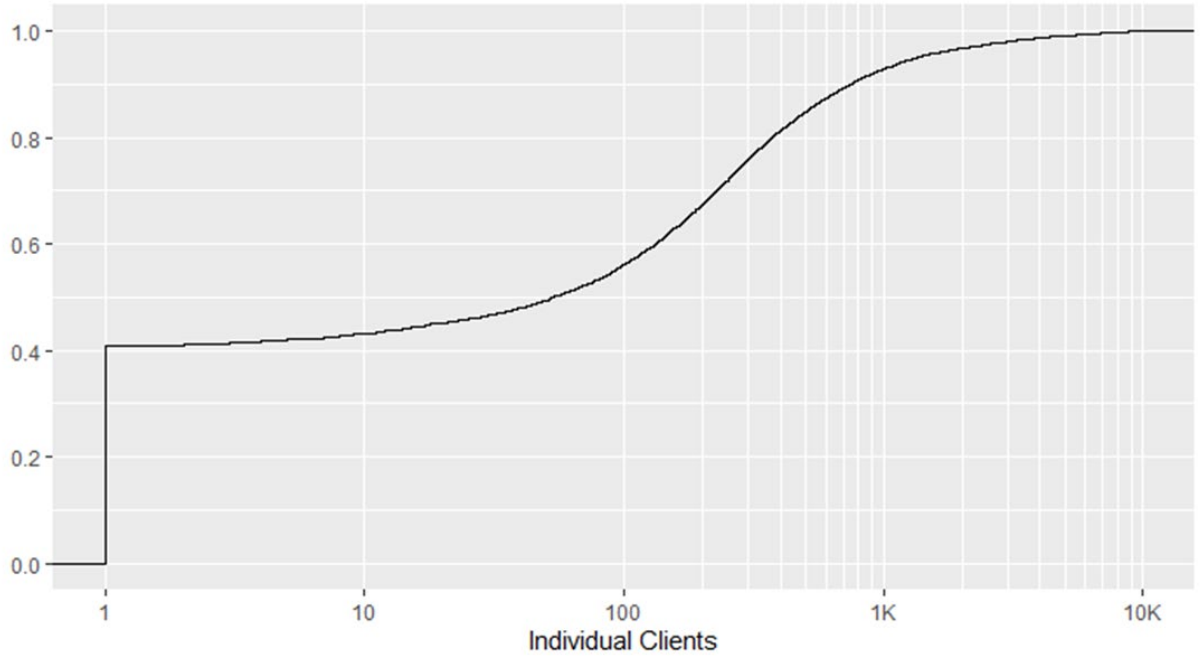

Figure 6: Cumulative distribution of the number of clients across investment advisers. Data source: Form ADV, Items 5D(a-b) (as of Oct. 5, 2023).

Figure 6 plots the cumulative distribution of the number of individual clients handled by investment advisers registered with the Commission. The distribution is highly skewed: 13 advisers each reported having more than one million clients while 95 percent of advisers reported having fewer than 2,000 clients. Many such advisers are quite small, with half reporting fewer than 62 clients.[654]

652 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).

653 Form ADV, Items 9A and 9B (as of Oct. 5, 2023).

654 Form ADV, Items 5D(a) and (b) (as of Oct. 5, 2023).

Similarly, most investment advisers registered with the Commission are limited geographically. These advisers must generally make a "notice filing" with a state in which they have a place of business or six or more clients.[655] Figure 7 plots the frequency distribution of the number of such filings. Based on notice filings, 57 percent of investment advisers registered with the Commission operated in fewer than four states, and 37 percent operated in only one state.[656]

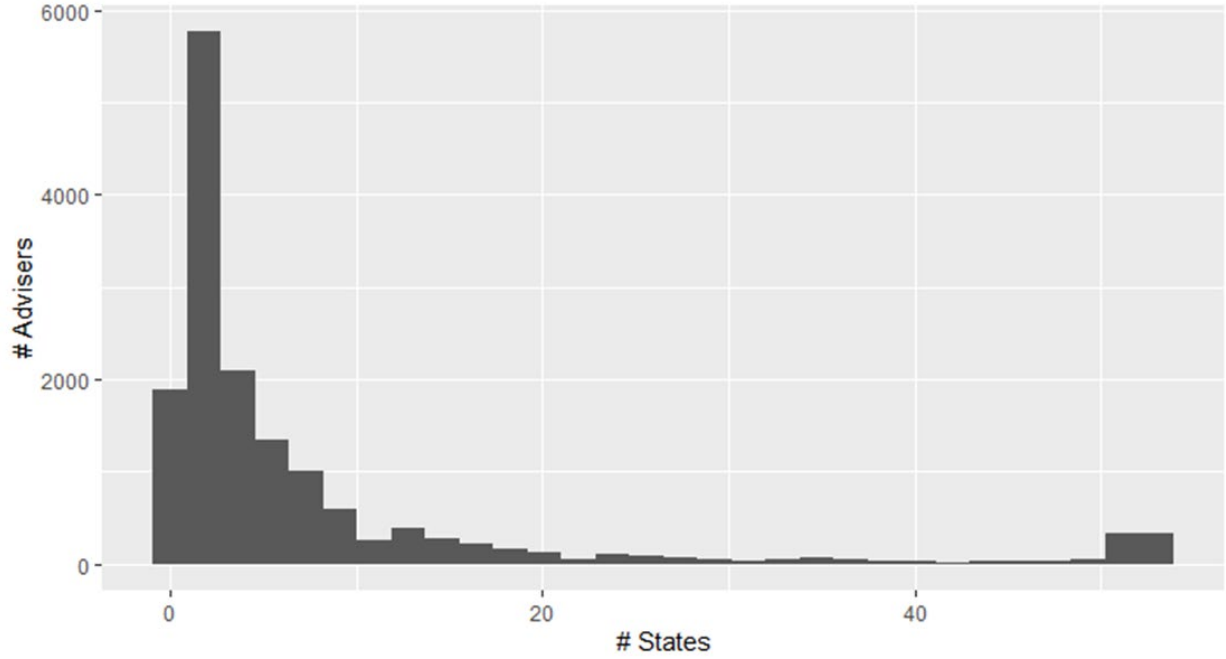

Figure 7: Frequency of number of state notice filings by SEC-registered investment advisers. Data source: Form ADV, Item 2.C (as of Oct. 5, 2023).

d. 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 subject to the final

655 *See* General Instructions to Form ADV (as of Oct. 5, 2023).

656 Form ADV, Item 2.C (as of Oct. 5, 2023). This includes 1,887 advisers who do not make any notice filings.

amendments include registered open-end and closed-end funds, business development companies ("BDCs"), Unit Investment Trusts ("UITs"), employee securities' companies ("ESCs"), and management company separate accounts ("MCSAs"). 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.[657]

Table 4 summarizes the investment company universe that will be subject to the final amendments. In total, as of September 30, 2023, there were 13,766 investment companies, including 12,183 open-end management investment companies, 682 closed-end managed investment companies, 702 UITs,[658] 141 BDCs,[659] approximately 43 ESCs, and 15 MCSAs. Many of the investment companies that will be subject to the final amendments are part of a "family" of investment companies.[660] Such families often share infrastructure for operations (e.g., accounting, auditing, custody, legal), and potentially marketing and distribution. We expect that many of the compliance costs and other economic costs discussed in the following sections will likely be borne at the family level.[661] We estimate that there were up to 1,131 distinct

---

657 The definition of "customer information" in the final amendments includes information about investment companies' investors. *See* final rule 248.30(d)(5)(i) and § 248.3(t).

658 For this release, the number of UITs includes N-4, N-6, N-8B-2, and S-6 filers as of Sept. 30, 2023. The Proposing Release cited a figure of 662 UITs using 2021 N-CEN filings. The correct number of UITs using 2021 N-CEN filings in the Proposing Release should be 703. This change would not have affected the Commission's assessment of economic effects at Proposal as these assessments were focused primarily on effects at the level of individual covered institutions and their customers.

659 For this release, the number of BDCs was estimated using London Stock Exchange Group ("LSEG") BDC Collateral data as of Sept. 2023.

660 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).

661 For example, each investment company in a family is likely to share common policies and procedures.

operational entities (families and unaffiliated investment companies) in the investment company universe.[662]

Table 4: Investment Companies, summary statistics. For each type of fund, this table presents estimates of the number of investment companies and investment company families. Data sources: 2023 N-CEN filings,[a] LSEG BDC Collateral (2023).[b]

Fund Type	# Inv. Co.	# Families[c]	# Unaffiliated[d]	# Entities[e]
Open-End[f]	12,183	212	251	463
Closed-End[g]	682	87	153	240
UIT[h]	702	106	229	335
BDC[i]	141	-	-	141
ESC[j]	43	-	-	43
MCSA[k]	15	1	1	2
Total[l]	13,766	313	634	1,131

a Year 2023 Form N-CEN (as of Sept. 2023).
b LSEG BDC Collateral (as of Sept. 2023).
c Number of families calculated from affiliation reported by registrants on Item B.5 of form N-CEN. The total number of families represents the number of distinct families; summing over the number of families across different fund types will double count some fund families.
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). The grand total is the sum of distinct families (313), total unaffiliated registrants (634), BDCs (141), and ESCs (43).
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 UITs are comprised of (1) Variable annuity separate accounts organized as UITs, which are series, or classes of series, of trusts registered on Form N-4; (2) Variable life insurance separate accounts organized as UITs, which are series, or classes of series, of trusts registered on Form N-6; (3) ETFs organized as UITs, which are series, or classes of series, of trusts registered on Form N-8B-2 / S-6 (Non-separate-account UITs register in the first instance on form N-8B-2, and then their subsequent filings are on Form S-6); and Non-ETF UITs are trusts registered on Forms N-4 or N-6.
i Form N-2 filers classified as BDCs.
j Form 40-APP filers [not classified as BDCs].
k Trusts registered on Form N-3.
l Cells do not sum to totals as investment company families may span multiple investment company types.

662 For this release, the number of unaffiliated entities was estimated using N-CEN filings as of Sept. 30, 2023. The Proposing Release cited a figure of 476 using 2021 N-CEN filings. The correct number of the unaffiliated entities using 2021 N-CEN filings in the Proposing Release should be 609. This change would not have affected the Commission's assessment of economic effects at Proposal as these assessments were focused primarily on effects at the level of individual covered institutions and their customers.

e. 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 securities registered in the U.S. 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 who maintains records of the claims of the various brokers.[663] 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, as only the broker holds this information.

Despite the prevalence of securities held in street name, a large number of individuals nonetheless hold securities directly through a 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 the DRS.

---

[663] In the U.S., this owner is generally Cede & Co., a partnership organized by the Depository Trust & Clearing Corporation.

In 2023, there were 251 transfer agents registered with the Commission, with an additional 64 registered with the Banking Agencies.[664] As discussed above,[665] differences in the baseline regulation of these transfer agents affect their current notification obligations.[666] Among the 315 transfer agents, 132 are considered small entities.[667] By registration, 100 of these small transfer agents are registered with the Commission and 32 are registered with the Banking Agencies.[668]

On average, each transfer agent reported around 1 million individual accounts, with the largest reporting 61 million.[669] Figure 8 plots the cumulative distribution of the number of individual accounts reported by registered transfer agents. Approximately one third of registered

---

664 Form TA-1 (as of Sept. 30, 2023).

665 *See supra* footnotes 601 and 604 and accompanying text.

666 *See infra* sections IV.D.2.b and IV.E (discussing benefits and costs, and competitive effects, relative to the baseline).

667 *See infra* section VI.C. 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 collected by the Commission as of Sept. 30, 2023.

668 *Id*.

669 Form TA-2 Items 5(a) (as of Sept. 30, 2023). This analysis is limited to the 265 transfer agents that filed form TA-2. For the 205 transfer agents registered with the Commission that filed form TA-2, the average number of individual accounts is 1.2 million; for the 60 transfer agents registered with the Banking Agencies that filed form TA-2, the average number of individual accounts is 69 thousand.

transfer agents reported no individual accounts,[670] and 58 percent reported fewer than ten thousand individual accounts.[671]

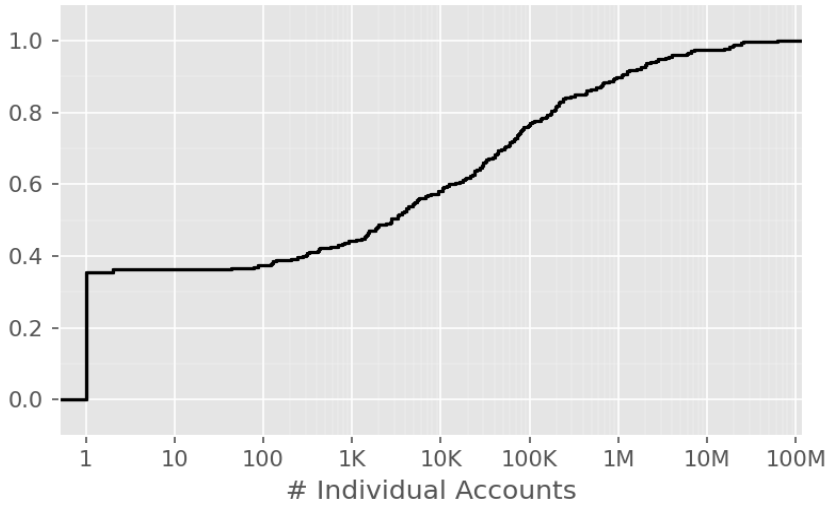

Figure 8: Cumulative distribution of the number of individual accounts (logarithmic scale) across registered transfer agents. Data source: Form TA-2, Items 5(a) (as of Sept. 30, 2023).

f. Service Providers

The final amendments require that a covered institution's incident response program include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers. These policies and procedures must be reasonably designed to ensure service providers take appropriate measures to protect against unauthorized access to or use of customer information and to notify covered institutions of an applicable breach in security.[672] These requirements on a covered institution will affect a service provider that "receives, maintains,

670 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).

671 Form TA-2, Items 5(a) (as of Sept. 30, 2023).

672 *See* final rule 248.30(a)(5).

processes, or otherwise is permitted access to customer information through its provision of services directly to [the] covered institution."[673]

Covered institutions' relationships with a wide range of service providers will be affected. Specialized service providers with offerings geared toward outsourcing of covered institutions' core functions will generally fall under the requirements. Those offering 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) will likely fall under the requirements. Some of these specialized service providers will be themselves covered institutions.[674] In addition, various less-specialized service providers might potentially fall under the requirements. Service providers offering Software-as-a-Service (SaaS) solutions for email, file storage, and similar general-purpose services might potentially be in a position to receive, maintain, or process 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) will in many cases be "otherwise [] permitted access to customer information" and might fall under the provisions.

In the Proposing Release, we stated that the financial services industry is increasingly relying on service providers through various forms of outsourcing.[675] We also stated that we were unable to quantify or characterize in much detail the structure of the relevant service provider markets due to data limitations.[676] One commenter stated that this resulted in an analysis that

---

673 Final rule 248.30(d)(10).

674 For example, many investment companies rely on third-party investment advisers and transfer agents.

675 *See* Proposing Release at section III.C.3.e; *see also* Bank for International Settlements, *Outsourcing in Financial Services* (Feb. 15, 2005), *available at* https://www.bis.org/publ/joint12.htm.

676 *See* Proposing Release at section III.C.3.e.

fails to meaningfully address the associated costs.[677] While this commenter did not identify any additional data sources, in response we have conducted a further review of industry literature.[678] While we continue to find certain data limitations, we also have identified certain additional informative data points on covered institutions' reliance on service providers.[679] A recent notice issued by FINRA states that FINRA's members, which include broker-dealers, "are increasingly using third-party vendors to perform a wide range of core business and regulatory oversight functions," a trend that has accelerated with the COVID-19 pandemic.[680] One report describes the results of a 2022 survey of 248 advisers and independent broker-dealers.[681] The survey found that 32 percent of the registered investment advisers and 50 percent of the independent broker-dealers that responded to the survey reported outsourcing investment management functions, and that while these proportions had not changed significantly in the past decade, half of the respondents who do outsource some of these functions reported an increase in their use of service providers. In addition, a different recent report finds that 33 percent of asset managers surveyed outsource their entire back-office function and 20 percent outsource their entire middle-

677 *See* IAA Comment Letter 1.

678 In addition, in response to this commenter, we have added further details on the current regulatory framework, in particular with respect to the obligations of covered institutions regarding their service providers and the notification obligations of service providers. *See supra* section IV.C.2. Also, we have supplemented the analysis of the benefits and costs of the final amendments' service provider requirements. *See infra* section IV.D.1.c. The supplemental review described here is designed to help us analyze and respond to commenters, and also to provide additional context for this analysis.

679 Potential service providers include a wide range of firms fulfilling a variety of functions. The internal organization of covered institutions, 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 and investment advisers' reliance on third parties for recordkeeping), we are unaware of any data sources that provide detail on the reliance of covered institutions on service providers.

680 *See* FINRA, *Regulatory Notice 21-29, supra* footnote 515.

681 *See* FlexShares, *The Race to Scalability 2022* (July 2022).

office function.[682] By the nature of their business models, most of the operations of investment companies are carried out by service providers.[683] Finally, many transfer agents outsource many functions.[684] Hence, all types of covered institutions affected by the final amendments commonly retain service providers to some extent.

D. Benefits and Costs of the Final Rule Amendments

The final amendments can be divided into four main components. First, they create a requirement for covered institutions to adopt policies and procedures for the protection of customer information. The policies and procedures must include an incident response program to address unauthorized access to or use of customer information, including by providing notification to individuals affected by an incident during which their sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. The response program must also include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight of service providers, including to ensure service providers take appropriate measures to protect against unauthorized access to or use of customer information. Second, the amendments define the information covered by the safeguards rule and the disposal rule,[685] and extend the application of the safeguards rule to transfer agents. Third, the amendments require covered institutions (other than

---

682 *See* Cerulli Associates, *Asset Managers Turn to Outsourcing Providers for Operating Model Sustainability* (Nov. 22, 2022), *available at* https://www.cerulli.com/press-releases/asset-managers-turn-to-outsourcing-providers-for-operating-model-sustainability ("Cerulli Report").

683 *See* Investment Company Institute, *How US-Registered Investment Companies Operate and the Core Principles Underlying Their Regulation* (May 2022), available at https://www.ici.org/system/files/2023-06/us-reg-funds-principles.pdf.

684 *See supra* footnote 670. *See also Interagency Guidance on Third-Party Relationships: Risk Management*, 88 FR 37920, 37937 (June 9, 2023), which may cover some transfer agents registered with a regulatory agency other than the Commission.

685 *See* final rule 248.30(a)(1), 248.30(b), 248.30(d)(1), and 248.30(d)(5).

funding portals) to maintain and retain records documenting compliance with the amended rules.[686] Fourth, they incorporate into regulation an existing statutory exemption for annual privacy notices. Below we discuss the benefits and the costs of each component in turn.

Some commenters criticized, generally, the discussion of benefits and costs in the Proposing Release. One commenter stated that the Commission should "undertake a more expansive, accurate, and quantifiable assessment of the specific and cumulative costs, burdens, and economic effects that would be placed on investment advisers by the proposed requirements, as well as of the potential unintended consequences for their clients."[687] Another commenter stated a need for more in-depth analysis of how the proposed amendments might impact transfer agents, their customers (issuers of securities), and securityholders.[688] Other commenters did not directly disagree with the analysis in the Proposing Release, but stated that the proposed amendments would place a high overall burden on covered institutions, including smaller institutions.[689]

In response to these commenters, we have supplemented the analysis of the benefits and the costs of the final amendments regarding the timing requirement for notification of customers affected by a breach, including by providing more details on how the requirements differ from the baseline;[690] different elements required to be included in a notice to affected individuals;[691]

---

686 As discussed above, funding portals are not subject to the recordkeeping obligations found under Rule 17a-4. Funding portals are instead obligated, pursuant to Rule 404 of Regulation Crowdfunding, to make and preserve all records required to demonstrate their compliance with Regulation S-P for five years, the first two years in an easily accessible place. *See supra* footnote 385; *see also* 17 CFR 227.404(a)(5).

687 *See* IAA Comment Letter 1.

688 *See* STA Comment Letter 2.

689 *See, e.g.*, SIFMA Comment Letter 2; ASA Comment Letter.

690 *See infra* section IV.D.1.b(2); *see also supra* section IV.C.2.a(2).

691 *See infra* section IV.D.1.b(5); *see also supra* section IV.C.2.a(2).

different requirements relating to service providers;[692] and the extension of the rule's scope to include all transfer agents.[693] As discussed below, we have also made changes to the final amendments that will reduce compliance costs for all covered institutions, including those that are smaller in size.[694]

Several commenters stated that the Commission should consider the cumulative costs of implementing the proposed amendments and other recent Commission rules and proposed rules.[695] Specifically, one commenter stated that "there can be no doubt that the costs of compliance—direct and indirect—rise with each regulation and directly impact the ability of [covered institutions] to invest in other aspects of their businesses" and that the Commission should "consider the cumulative effects that" the final amendments and other adopted rules will have on covered institutions' "operational limitations and, more importantly, resource constraints, in determining the compliance dates."[696] That commenter and others mentioned proposals which culminated in several adopted rules.[697]

Consistent with its long-standing practice, the Commission's economic analysis in each adopting release considers the incremental benefits and costs for the specific rule—that is, the benefits and costs stemming from that rule compared to the baseline. The Commission acknowledges the possibility that complying with more than one rule may entail costs that could exceed the costs if the rules were to be complied with separately. Four of the rules identified by commenters have compliance dates that occur before the effective date of the final

---

692 *See infra* section IV.D.1.c; *see also supra* sections IV.C.2.a(3) and IV.C.3.f.

693 *See infra* section IV.D.1.b; *see also supra* section IV.C.2.a(3).

694 *See infra* footnote 1058 and accompanying text.

695 *See supra* footnote 482.

696 *See* IAA Comment letter 2.

697 *See supra* footnotes 483-493.

amendments,[698] such that there is no overlap in compliance periods. The compliance periods for the other rules overlap in part, but the compliance dates adopted by the Commission in recent rules are generally spread out over an approximately three-year period from 2023 to 2026,[699] which could limit the number of implementation activities occurring simultaneously. Where overlap in compliance periods exists, the Commission acknowledges that there may be additional costs on those covered institutions subject to one or more other rules as well as implications of those costs, such as impacts on entities' ability to invest in other aspects of their businesses.[700]

Covered institutions subject to the final amendments in this rulemaking may be subject to one or more of the other adopted rules commenters named depending on whether those institutions' activities fall within the scope of the other rules. Specifically, the rules and amendments in the February 2024 Form PF Adopting Release, and those rules and amendments in the Private Fund Advisers Adopting Release for which the compliance dates have not already passed, apply to advisers to private funds: as private fund advisers are a subset of the covered institutions affected by the amendments, only a subset of covered institutions face compliance costs associated with these recent rules and amendments.[701] The Public Company Cybersecurity Rules apply only to public companies, not all covered institutions.[702] The amendments adopted in

---

698 The compliance dates for the Electronic Recordkeeping Adopting Release occurred in 2023, and the compliance date for the Settlement Cycle Adopting Release is May 28, 2024. The compliance dates for the May 2023 SEC Form PF Adopting Release and the Form N-PX Adopting Release are June 11, 2024, and July 1, 2024, respectively.

699 *See supra* section IV.C. In addition, we adopted longer compliance periods for all covered institutions relative to the proposal, and an even longer compliance period for smaller covered institutions. *See supra* section II.F.

700 *See*, *e.g.*, IAA Comment letter 2 (describing the types of implementation activities, such as updating internal controls, and training).

701 *See* Private Fund Advisers Adopting Release, at section VI.C.1; February 2024 Form PF Adopting Release, at section IV.B.2.

702 *See* Public Company Cybersecurity Rules, at section IV.B.2. One commenter also suggested the Commission should consider the relationship between reporting obligations in the proposed amendments

the Money Market Fund Adopting Release place a compliance burden on money market funds and certain liquidity fund advisers registered with the Commission, which are also a subset of covered institutions.[703] The Investment Company Names Adopting Release amended requirements for those registered investment companies and BDCs with names with terms suggesting that the fund has particular characteristics, which are a subset of the funds affected by the final amendments.[704] The Beneficial Ownership Adopting Release amended disclosure requirements that apply only to persons who beneficially own more than five percent of a covered class of equity securities.[705] The rule adopted in the Securitization Conflicts Adopting Release affects only certain entities (and their affiliates and subsidiaries) that participate in securitization transactions.[706] We acknowledge that covered institutions subject to multiple rules may still experience increased costs associated with implementing multiple rules at once as well as implications of those costs, such as impacts on those institutions' ability to invest in other aspects of their businesses.

1. Written Policies and Procedures

In this section, we discuss the effects of written policies and procedures requirements in the final amendments, focusing on those relating to the incident response program required under the final amendments. Specifically, while the final amendments require covered institutions to develop, implement, and maintain written policies and procedures that address administrative,

---

and the Public Company Cybersecurity Rules. *See* ASA Comment Letter. We modified the final amendments, relative to the proposal, to align with the Public Company Cybersecurity Rules with regard to disclosure delays for national security or public safety reasons. *See supra* section II.A.(d)(2).

703 *See* Money Market Fund Adopting Release, at section IV.B.

704 *See* Investment Company Names Adopting Release, at section IV.C.

705 *See* Beneficial Ownership Adopting Release, at section IV.B.3.

706 *See* Securitization Conflicts Adopting Release, at section IV.B.2.

technical, and physical safeguards for the protection of customer information,[707] general written policies and procedures to protect customer information are already part of the baseline.[708] The primary new requirements pertain to written policies and procedures that must include an incident response program to address unauthorized access to or use of customer information.

We expect that requiring written policies and procedures for the response program will improve the effectiveness of response programs in multiple ways, which will benefit covered institutions and their customers. Written policies and procedures are a practical prerequisite for organizations to implement standard operating procedures and have been recognized as effective at improving outcomes in critical environments.[709] We expect that this will also be the case for response programs for data breach incidents. Written policies and procedures can help ensure that the covered institution's personnel know what corrective actions to take and when in the event of a data breach. Written policies and procedures can also help ensure that the incident is handled in an optimal manner. Moreover, 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. This may also lead to covered

---

707 *See* final rule 248.30(a)(1).

708 Prior to this adoption, Regulation S-P already required covered institutions to adopt policies and procedures reasonably designed to protect customer information. *See supra* section IV.C.2.b. Transfer agents were not previously covered by the safeguards rule and were not, before this adoption, required by the Commission to have such written policies and procedures in place. We analyze the benefits and costs that are specific to transfer agents in section IV.D.2.b.

709 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; 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* Joseph Alex, 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). We are not aware of any studies that assess the efficacy of written policies and procedures specifically in the context of financial regulation, and no commenter provided such sources.

institutions improving their customer information safeguards, which could reduce the likelihood of unauthorized access to or use of customer information in the first place.[710]

We do not anticipate that the final requirement for written policies and procedures will 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. As stated above,[711] all states and the District of Columbia generally require businesses to notify their customers when certain customer information is compromised. States do not typically require the adoption of written policies and procedures for the handling of such incidents.[712] 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 for assessment, containment, and notification.[713] Given the 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 that covered institutions that have already developed written policies and procedures for incident response have based such policies and

---

710 *See infra s*ection IV.D.1.b(3) for examples of how covered institutions could enhance their customer information safeguards.

711 *See supra* section IV.C.2.

712 Some states do, however, require businesses to have procedures to protect personal information. *See, e.g.*, Cal. Civil Code § 1798.81.5 and N.Y. Gen. Bus. Law. § 899-BB.

713 Various industry guidebooks, frameworks, and government recommendations share many common elements, including the ones included in the final amendments. *See, e.g.*, NIST Computer Security Incident Handling Guide and CISA Incident Response Playbook.

procedures on common cyber incident response frameworks (e.g., NIST Computer Security Incident Handling Guide, CISA Cybersecurity Incident Response Playbook),[714] generally accepted industry best practices, or other applicable regulatory guidelines,[715] these large covered institutions' written policies and procedures are likely to include the elements of assessment, containment, and notification, and to be substantially consistent with the requirements of the final amendments. Thus, we do not anticipate that the final requirement for written policies and procedures will result in substantial new benefits from its application to these institutions.

For the same reasons, this requirement is unlikely to impose significant new costs for these institutions. As discussed below, we estimate that certain costs associated with developing and implementing policies and procedures to comply with the final amendments will be, on average, $15,445 per year per covered institution.[716] Here, we expect the main costs associated with the final requirement to be the costs of reviewing, and possibly updating, existing policies and procedures to ensure that they satisfy the new requirements. Hence, we expect these reviews and updates will result in these covered institutions incurring direct compliance costs generally smaller than the costs of developing and implementing new policies and procedures. If covered institutions respond to this requirement by improving their customer information safeguards

---

714 *See supra* footnote 625.

715 For example, the Banking Agencies' Incident Response 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 footnote 605.

716 This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $5,425 per year per covered institution. *See infra* section V. We expect that for some institutions, the actual costs might be lower than these estimates. For example, there may be some portability between funds belonging to the same family of investment companies, which could mitigate costs per investment company. *See supra* section IV.C.3.d. We estimate that these costs will be higher for transfer agents because transfer agents were not, before this adoption, covered by the safeguards rule. In addition, transfer agents registered with a regulatory agency other than the Commission were not, before this adoption, covered by the disposal rule. *See infra* footnote 1003 and accompanying text.

beyond what is required by the final amendments, they will incur additional costs.[717] We expect that the costs incurred by these covered institutions as a result of this requirement will ultimately be passed on to customers of these institutions.[718]

We expect that the final written policies and procedures requirements will 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. Before this adoption, some of these covered institutions may have had lower incentives to develop and implement written policies and procedures for a response program and may therefore have been less likely to have such policies and procedures in place for several reasons. First, the incentives to develop and implement policies and procedures for a response program may vary for covered institutions of different sizes. Some smaller covered institutions may already prioritize response programs, for example because the firm views reputational costs of a cybersecurity breach or other type of unauthorized access to or use of customer information as posing the potential for serious harm to the firm. However, for other smaller covered institutions, the firm and its managers may view response programs as lower priority because, for example, the potential reputational cost of an unauthorized access to or use of customer information may be relatively smaller than it would be for a larger firm. This would be the case to the extent that the firm and its managers perceive that the firm has a lower franchise value (the present value of the future profits that a firm is expected

---

717 Because covered institutions could decide to enhance their customer information safeguards in many different ways, we are unable to quantify expected costs resulting from such enhancements. *See infra* section IV.D.1.b(3) for examples of how covered institutions could enhance their customer information safeguards as a result of the final amendments.

718 Costs incurred by larger covered institutions as a result of the final amendments will generally be passed on to their customers in the form of higher fees. However, smaller covered institutions—which are likely to face higher costs relative to their size—may not be able to do so. *See infra* section IV.E.

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 may be perceived to be lower than at larger firms. Moreover, the cost of developing and implementing written policies and procedures for a response program is proportionately large compared to larger covered institutions since it involves fixed costs.

Second, some covered institutions could potentially have, before this adoption, complied effectively with the relevant state data breach notification laws without adopting written policies and procedures to deal with customer notification: they may only have needed to consider—on an ad hoc basis—the notification requirements of the small number of states in which their customers reside.[719] Hence, for such covered institutions, the cost of developing policies and procedures will be relatively larger, but the benefits for the customers of these institutions will also be larger.

We expect that for such covered institutions, the final amendments will likely impose additional compliance costs related to written policies and procedures for safeguarding customer information.[720] Certain costs associated with developing and implementing policies and procedures to comply with the final amendments are estimated to be $15,445 generally per year per covered institution, but may vary depending on the size of the institution and the current state

---

[719] As discussed above, many registered investment advisers have clients in only a few states. *See supra* section IV.C.3.c.

[720] The existing policies and procedures were already required under Regulation S-P before this adoption; *see* 17 CFR 248.30. The final amendments may also generate additional costs to covered institutions who decide to improve their customer information safeguards to avoid the potential reputational harm associated with the customer notification requirements. However, one commenter stated that the FTC has often noted that reasonable security measures are a relatively low cost. *See* EPIC Comment Letter. Such improvements in customer information safeguards would also provide potential benefits to customers in addition to reducing the risk of reputational harm for the covered institutions.

of their existing policies and procedures.[721] Furthermore, as for larger covered institutions, if these covered institutions respond to this requirement by improving their customer information safeguards beyond what is required by the final amendments, they will incur additional costs. While these smaller covered institutions might potentially pass some of the costs resulting from the final amendments 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 across which to spread costs.[722] In addition, covered institutions that improve their customer notification procedures in response to the final amendments might suffer reputational costs resulting from the additional notifications.[723]

Some commenters stated that many covered institutions already had policies and procedures in place.[724] These commenters also stated that these policies and procedures would need to be reviewed and updated to comply with the amendments, but to different extents. On the one hand, one commenter stated that its members already complied with much of the proposal's content through state regulations, such as the requirements that companies maintain written cybersecurity policies and procedures, respond to cyber incidents, notify authorities and

---

721 This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $5,425 per year per covered institution. *See infra* section V. We expect that for some institutions, the actual costs might be lower than these estimates. For example, there may be some portability between funds belonging to the same family, which could mitigate costs. *See supra* section IV.C.3.d.

722 *See supra* section IV.C.3. Developing and implementing written policies and procedures for a response program involves fixed costs. Larger institutions can spread these costs over a larger number of customers, resulting in a smaller increase in the price that each customer pays. Smaller institutions must spread these costs over a smaller number of customers, resulting in a larger price increase per customer. This could result in smaller institutions losing more customers as a result of the increase in price. Hence, smaller institutions could decide to absorb more of the costs compared to large institutions in order to avoid losing customers.

723 *See supra* section IV.B; *see also infra* section IV.D.1.b.

724 *See, e.g.*, IAA Comment Letter 1; SIFMA Comment Letter 2.

consumers of certain cyber incidents, and dispose of consumer data.[725] A second commenter stated that the customer notification requirements would need to be incorporated into existing policies and procedures.[726] These commenters' perspectives are consistent with our view that the final rules will impose a fairly limited burden for covered institutions bringing existing policies and procedures into compliance with the new requirements. On the other hand, a different commenter stated that written incident response program policies and procedures and recordkeeping requirements would need to be created and implemented,[727] indicating higher potential burden. Hence, we continue to expect that the policies and procedures requirements will potentially have different effects on different covered institutions.[728] In a change from the proposal and after considering commenters' concerns, we are now adopting a longer compliance period for all covered institutions relative to the proposal, and an even longer compliance period of 24 months for smaller covered institutions, which are less likely to already have policies and procedures broadly consistent with the final amendments.[729]

Two commenters discussed how the proposed amendments would affect an entity that is dually registered as an investment adviser and broker-dealer. One commenter stated that it appreciated the approach of the proposal, which applies uniformly to the two types of covered institutions and would allow for streamlining of processes.[730] Another commenter stated that

---

725 *See* ACLI Comment Letter.

726 *See* SIFMA Comment Letter 2.

727 *See* IAA Comment Letter 1.

728 For example, some covered institutions, such as transfer agents, may not have existing notification procedures since they may not have been required, under state law, to notify customers in case of a breach. *See supra* section IV.C.2.a(3); *infra* section IV.D.2.b.

729 The compliance period for larger institutions under the final amendments is 18 months from the date of publication in the Federal Register. The proposed compliance period for all covered institutions was 12 months from the effective date of the final amendments. *See supra* section II.F.

730 *See* FSI Comment Letter.

bringing both sides of the entity into compliance with the proposed amendments would impose a significant burden and require a dual registrant to modify both sides of the entity' compliance frameworks.[731] We do not expect a significant burden, because we expect that these institutions could generally implement a single set of procedures to comply with many of the provisions of the final amendments, which would limit these additional burdens.[732] To the extent entities registered as more than one category of covered institution arrange their business such that there are separate policies and procedures for each category, those entities may encounter additional cost burden when complying with the final amendments. For example, an entity that creates two different incident response programs for its advisory and broker-dealer operations could bear as much as twice the cost burden as the same entity would bear when creating one incident response program,[733] although there may be efficiencies to the extent that development of one program informs the other. The final amendments, however, do not prevent that entity from using the same incident response program across its categories of covered institutions.

In the remainder of this section, we first consider the benefits and costs associated with requiring covered institutions to have a response program generally. We then analyze the benefits and the costs of the notification requirements vis-à-vis the notification requirements already in force under the various existing state laws. We conclude this section with an analysis of the benefits and costs of the response program's service provider provisions.

---

731 *See* Cambridge Comment Letter.

732 For example, we expect that these institutions will be able to implement a single set of procedures to satisfy the customer notification requirements.

733 For example, annual average costs of $30,890 associated with preparation of written policies and procedures instead of annual average costs of $15,445. *See, e.g.*, *infra* footnote 856 and accompanying text.

a. Response Program

The final amendments require covered institutions' written policies and procedures to include a response program "reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures."[734] The response program must address incident assessment, containment, as well as customer notification and oversight of service providers.[735]

The question of how best to structure the response to an incident resulting in unauthorized access to or use of customer information 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.[736] While the emphasis of these reports varies, certain key components are common across many 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.[737] The assessment, containment, and notification prongs of the final policies and procedures requirements correspond to the latter three phases of the NIST recommendations. Similar analogues are found in other reports, recommendations, and other regulators' guidelines.[738] Thus, the required 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.

---

[734] Final rule 248.30(a)(3).

[735] *See* final rule 248.30(a)(3).

[736] *See supra* section IV.C.1.

[737] *See* NIST Computer Security Incident Handling Guide.

[738] *See supra* text accompanying footnote 604.

While some commenters suggested that some specific provisions of the amendments be better aligned with existing regulation,[739] other commenters stated that the Commission's proposal would generally align the amendments with other regulatory frameworks such as the Banking Agencies' Incident Response Guidance.[740] One of these commenters stated that consistency across regulatory requirements facilitates firms' operations, provides for efficiencies in their operations, and better serves customers.[741] In the final amendments, we have revised some requirements from the proposal to better align them with existing regulatory framework. For example, one commenter stated that a 72-hour deadline would improve alignment with other existing requirements and that this would significantly reduce complexity and compliance burdens for covered institutions and their service providers.[742] Consistent with other regulatory frameworks,[743] the final amendments require that covered institutions ensure that their service providers take appropriate measures to provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred.[744]

Similar to the written policies and procedures requirement, we expect the benefits and the costs of the response program requirements to vary across covered institutions. In general, costs will be larger for entities that do not have any related incident response programs or related policies and procedures. For those entities, costs may include needing to familiarize themselves with the new requirements, initial set up costs for new systems to monitor when customers need

---

739 *See* SIFMA Comment Letter 2; Computershare Comment Letter.

740 *See, e.g.*, ICI Comment Letter 1; Nasdaq Comment Letter.

741 *See* ICI Comment Letter 1.

742 *See* Microsoft Comment Letter; *see also supra* footnote 245 and accompanying text.

743 *See supra* footnote 257 and accompanying text.

744 The proposed amendments instead had a requirement of 48 hours. *See* Proposing Release at section II.A.3.

to be notified, new notification systems, and development and implementation of new policies and procedures associated with response programs. Therefore, on the one hand, the effects of the requirements are likely to be small for covered institutions with a national presence who are likely to already have such programs in place.[745] For such institutions, we expect direct compliance costs to be largely limited to reviews and, if needed, updates of existing policies and procedures.[746] On the other hand, we expect greater benefits and costs for smaller, more geographically limited covered institutions since they are less likely to have an existing incident response program. The benefits ensuing from these 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. The response program requirements might potentially provide substantial benefit in a specific incident, for example in the case of a data breach at an institution that does not currently have an incident response program and is unprepared to promptly respond in keeping with law and best practice. Such an institution will also bear the full costs associated with adopting and implementing procedures complying with the final amendments.[747]

In addition to helping ensure that customers are notified when their data are breached,[748] having reasonably designed strategies for incident assessment and containment ex ante might

---

745 In addition, as discussed above, private funds may be subject to the FTC Safeguards Rule, which requires an incident response plan. *See supra* footnotes 614 and 617 and accompanying text. Hence, we expect that private funds advisers that are registered with the Commission may already have an incident response plan in place.

746 We expect these reviews and updates will result in entities incurring costs generally smaller than the costs of adopting and implementing new procedures. *See supra* section IV.D.1.

747 *See supra* footnote 721 and accompanying text for a discussion of certain quantified costs associated with developing and implementing policies and procedures. *See also infra* section V.

748 The benefits and costs specific to the notification requirements are analyzed in detail in section IV.D.1.b

reduce the frequency and scale of breaches through more effective intervention and improved managerial awareness, providing further indirect benefits. Any such improvements to covered institutions' processes will benefit their customers (e.g., by reducing harms to customers resulting from data breaches), as well as the covered institutions themselves (e.g., by reducing the expected costs of handling data breaches), representing further indirect benefits of the rule.

We lack data on efficacy of incident assessment, incident containment, or customer notification that would allow us to quantify the economic benefits of the final requirements, and no commenter suggested such data. Similarly, we lack data, and no commenter suggested such data, that would allow us to quantify the indirect economic costs, such as reputational cost of any potential increase in the frequency of customer notification or the indirect costs of customer information protection improvements that may be undertaken to avoid such reputational costs. In the aggregate, however, considering the amendments in the context of the baseline, these benefits and costs are likely to be limited. As we have discussed above,[749] all states have previously enacted data breach notification laws with substantially similar aims and, therefore, we think it likely that many institutions have response programs to support compliance with these laws. In addition, we anticipate that larger covered institutions with a national presence—which account for the bulk of covered institutions' customers—have already developed written incident response programs consistent with the proposed requirements in most respects.[750] Thus, the benefits and costs of requiring written incident response programs will be the most significant for smaller covered institutions without a national presence—institutions whose policies affect relatively few customers.

---

below.

749 *See supra* section IV.C.2.a.

750 *See supra* footnote 713 and accompanying text.

In support of the proposed response program requirement, some commenters stated that response programs had benefits beyond the notification of affected individuals. One commenter stated that effective cybersecurity practices and system safeguards, including incident response and notification, were critical for the financial markets and services industry and the regulators tasked with oversight of this sector.[751] Another commenter stated that the costs associated with the incident response programs and more robust notification regime served an important forcing function for entities that might otherwise not adequately invest in safeguards on the front end.[752] This commenter also cited a report stating that having an incident plan is one of the steps organizations can take to protect their data.[753] In addition, in support of the Proposing Release, commenters cited sources offering additional context and evidence of the benefits of incident response programs. A report cited by a commenter states that businesses with an incident response team that tested their incident response plan saw an average of $2.66 million lower breach costs compared to organizations without an incident response team and that did not test their incident response plan.[754] A more recent version of the same report states that businesses which both had an incident response team and tested their incident response plan took 54 fewer days to identify and contain a data breach, compared to businesses that did not have a response

---

751 *See* Google Comment Letter.

752 *See* EPIC Comment Letter. Potential reputational costs, and the associated potential loss of customers, that could result from customer notification will incentivize covered institutions to spend more on information safeguards. However, additional costs associated with the required response program are unlikely to provide such incentives. Once informed, the customers will have the possibility to stop doing business with covered institutions they wish to avoid.

753 *See* EPIC Comment Letter, citing Internet Society's Online Trust Alliance, *2018 Cyber Incident & Breach Trends Report* (July 9, 2019), *available at* https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf.

754 *See* Better Markets Comment Letter. The commenter cited the 2022 IBM Cost of Data Breach Report which finds that the cost of a data breach for organizations without an incident response team and that did not test their incident response plan was $5.92 million, while the costs for organizations with an incident response team that tested its incident response plan was $3.26 million. Equivalent numbers are not available in the 2023 version of the report.

team nor test their incident response plan (252 days as compared to 306 days).[755] This information generally supports our view that incident response programs will have benefits for both covered institutions and their customers. However, because the amendments' requirements differ from those analyzed in these reports, we are unable to use these estimates to precisely quantify the benefits of the amendments in terms of prevention of and response to data breach incidents involving customer information. Nevertheless, to the extent that different reasonably designed incident response programs yield benefits of similar magnitudes, the final amendments will have benefits of similar magnitude for the covered institutions that do not currently have an incident response program in place, with associated benefits for the customers of these institutions.

b. Notification Requirements

The final requirements provide for a Federal 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),[756] regardless of their state of residence. The information value 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 how and 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.[757]

---

755 *See* 2023 IBM Cost of Data Breach Report.

756 *See* final rule 248.30(d)(5)(i).

757 Commenters agreed that a breach notification allows customers to take mitigating actions limiting the negative effects of a breach. *See, e.g.*, EPIC Comment Letter. One commenter also stated that the value of

These customers will also be better able to make informed decisions about whether to continue to do business with institutions that have been unable to prevent their information from being compromised. Similarly, non-customers who learn of a data breach, for example from individuals notified as a result of the final amendments, might use this information to evaluate their potential use of a covered institution.

As discussed above, all 50 states and the District of Columbia already have data breach notification laws that apply, in varying ways, to compromises of their residents' information.[758] Thus, the benefits of the adopted Federal minimum standard for notification of customers (vis-à-vis the baseline) will vary depending on each customer's state of residence, with the greatest benefits accruing to customers that reside in states with the least informative customer notification requirements.[759]

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 on a state-by-state basis the benefits of the adopted Federal minimum standard to customers residing in the various states. In considering the benefits of the final notification requirement, we limit consideration to the "strength" of individual provisions of the final amendments vis-à-vis the corresponding provisions under state laws and consider the number of customers that might potentially benefit from each.

---

any required disclosure depended largely on the extent to which it conveyed clear, comprehensible, and usable information. *See* Better Markets Comment Letter.

758 *See supra* section IV.C.2.a. In addition, some covered institutions may be required to share information with certain individuals about certain events under other Federal regulations such as Regulation SCI or the Banking Agencies' Incident Response Guidance. *See supra* section IV.C.2.b.

759 In some cases, large benefits could also accrue to customers that reside in states with broader and more informative breach notification laws if they reside in states where such laws are not applicable to entities in compliance with the GLBA. *See infra* section IV.D.1.b(1).

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 the final amendments will be greater for covered institutions whose customers reside in states with less informative customer notification laws than for those whose customers reside in states with broader and more informative notification laws. In particular, smaller covered institutions whose customers are concentrated in states where state data breach laws result in less informative customer notification are likely to face higher costs since they may have to issue additional notices to comply with the amendments. The costs associated with notice issuance comprise both administrative costs and reputational costs. Certain costs arising from notice issuance are covered in the Paperwork Reduction Act analysis in section V and are estimated to be on average $5,178 per year per covered institution.[760] We lack data, and no commenter suggested such data, that would allow us to quantify the reputational cost resulting from any potential increase in the frequency of customer notification or the indirect costs of customer information protection improvements that may be undertaken by covered institutions to avoid such reputational costs.

Although some commenters stated that a Federal notification requirement was not needed given existing state law requirements,[761] other commenters supported this proposed provision.[762] One commenter stated that a significant advantage would be that in several states, it would

---

760 This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $3,862 per year per covered institution. *See infra* section V.

761 *See, e.g.*, CAI Comment Letter (stating that the proposed amendments' requirements "would simply add another layer on top of these existing requirements and would likely go entirely unnoticed by consumers, while complicating compliance efforts for covered institutions and raising additional compliance and legal risk"). We disagree with these commenters and discuss in detail in the subsections below the benefits of different provisions of the notification requirements over the baseline.

762 *See, e.g.*, ICI Comment Letter 1; IAA Comment Letter 1.

relieve covered institutions from having to issue state-specific breach notices under state law.[763] Another commenter further stated that a Federal breach notification requirement "would satisfy state notice laws that provide exemptions for firms subject to such a requirement, which will help to a degree to reduce the confusion and notification burdens arising from the patchwork of state data breach notification requirements."[764] Another commenter stated that the benefits of a Federal minimum standard would outweigh the burden of the new notification requirements.[765]

In the rest of this section, we consider key provisions of the final notification requirements, their potential benefits to customers (vis-à-vis existing state notification laws), and their costs.

(1) GLBA Safe Harbors

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, funding portals, investment companies, or transfer agents. The final amendments will 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 19 states provide a GLBA Safe Harbor.[766] Together, these states account for 24 percent of the U.S. population, or approximately

---

763 *See* ICI Comment Letter 1.

764 *See* IAA Comment Letter 1; *see also supra* footnote 557 and accompanying text. Another commenter stated that the proposed notification requirements would not replace state law requirements and that covered institutions would continue to have to comply beyond the Federal minimum standard for at least 20 states. *See* FSI Comment Letter.

765 *See* FSI Comment Letter.

766 States with exceptions that specifically mention the GLBA include Arizona, Connecticut, the District of Columbia, Delaware, Iowa, Kentucky, Maryland, Minnesota, Missouri, Nevada, New Mexico, Oregon, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Virginia, and Wisconsin. Additional states

17 million potential customers who may benefit from this provision.[767] 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.[768] We estimate that there are 679 such advisers, representing 4.4 percent of the registered adviser population, and that these advisers represent in total more than 97,000 clients.[769] 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, many covered institutions have customers residing in states without a GLBA Safe Harbor and we therefore expect them to have existing procedures for notifying customers under state law. Additionally, some jurisdictions require notification policies or actual notification as condition of the safe harbor.[770] However, covered institutions whose customer base is limited to GLBA Safe Harbor states may not have implemented any procedures to notify customers in the event of a data breach. These covered institutions may face higher costs than entities with some notification procedures already in place, but the customers of these institutions will benefit the most from the final amendments by receiving notice they may not have otherwise received.

---

have exceptions for compliance with a primary Federal regulator, as discussed *supra*.

767 Estimates of the numbers of potential customers are based on state population adjusted by the percentage of households reporting direct stock ownership (21%). *See* U.S. CENSUS BUREAU, APPORTIONMENT REPORT (2020)*, available at* https://www2.census.gov/programs-surveys/decennial/2020/data/apportionment/apportionment-2020-table01.xlsx (last visited Apr. 12, 2024); *see also* Federal Reserve Board*, Survey of Consumer Finances* (2022), *available at* https://www.federalreserve.gov/econres/scfindex.htm (last visited Apr. 9, 2024).

768 Based on Form ADV, Item 2.C as of Oct. 5, 2023*; see also supra* footnote 655.

769 Based on Form ADV, Item 5.D as of Oct. 5, 2023; *see also supra* footnote 650.

770 *See, e.g.*, D.C. Code § 28-3852(g).

One commenter agreed that some state laws provided exemptions from their notice requirements under the GLBA but disagreed that this implied benefits for the amendments, stating that the proposed amendments would not preempt state notification requirements and would instead add another variation on existing requirements to be accounted for by covered institutions, with limited real benefits to affected individuals.[771] The final amendments will create new and to various extents different notification requirements for covered institutions with customers residing in states without GLBA exemptions. However, we disagree with this commenter's assertion that benefits to affected individuals will be limited. As discussed above, state laws vary in detail from state to state.[772] We discuss below how the final amendments will impose a Federal minimum standard for customer notification and how we expect this standard to benefit customers.

(2) Accelerated Timing of Customer Notification

The final amendments require covered institutions to provide notice to customers in the event of some data breaches 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.[773] As discussed in section IV.C.2.a, existing state laws vary in terms of notification timing. Most states (31) do not include a specific deadline for notifying customers, but rather require that the notice be given in an expedient manner and/or that it be provided

---

[771] *See* CAI Comment Letter ("Although some state laws do provide exemptions from their state specific notice requirements where a notice is provided consistent with requirements under the Gramm-Leach Bliley Act (GLBA), most do not. This proposed new requirement would not serve to preempt those generally applicable state notice requirements, and would not establish a new singular standard. It would just be another variation on existing requirements to be accounted for, with limited real benefit to affected individuals.").

[772] *See supra* section IV.C.2.a.

[773] *See* final rule 248.30(a)(4)(iii).

without unreasonable delay. These states account for 60 percent of the U.S. population, with approximately 42 million potential customers residing in these states.[774] Four states have a 30-day deadline; we estimate that close to 8 million potential customers reside in these states. The remaining 16 states provide for longer notification deadlines. For the estimated 20 million potential customers residing in these 16 states, the final amendments' 30-day outside timeframe might tighten the notification timeframes.[775] In addition, the 30-day outside timeframe is likely to tighten notification timeframes for the approximately 42 million potential customers residing in states with no specific deadline.

Even though the timing language in state laws without specific deadlines generally suggests that notices must be prompt, we have evidence that the notices are frequently sent significantly later than 30 days after the affected institution learns of the breach. The Proposing Release references data from California and Washington, which we explain in more detail below. California requires that such notice be given "in the most expedient time possible and without unreasonable delay."[776] Nevertheless, data from the California Office of the Attorney General, regarding notices sent to more than 500 California residents for any one incident, indicate that for the notices for which these data are available, the average time from discovery to notification was 144 days in 2022, and 91 percent of these notices were sent later than 30 days after the discovery of the breach.[777] Hence, we expect that the aggregate effects of a 30-day notification

---

774 *See supra* Figure 2; *see also supra* footnote 767.

775 State deadlines are either 30, 45, or 60 days, but differ in terms of triggers of those deadlines; s*ee supra* Figure 3.

776 *See* Cal. Civil Code § 1798.82.

777 This analysis was performed using data from the 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 Apr. 8, 2024). California law requires that a sample copy of a breach notice sent to more than 500 California residents be provided to the California Attorney General. Four-hundred fifty-six such notices were reported in the year of 2022. Of those notices, 164 (36%)

outside timeframe might be significant for the 42 million potential customers residing in states with no specific deadline.[778]

In addition, because the final amendments will not provide for broad exceptions to the 30-day notification requirement,[779] in many cases the amendments will tighten notification timeframes even for the 8 million potential customers residing in states with a 30-day deadline. For example, in Washington, the state law requires that the notice be given "without unreasonable delay, and no more than thirty calendar days after the breach was discovered."[780] However, the law also allows for a delay "at the request of law enforcement" or "due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[781] Data from the Washington Attorney General's Office indicate that for the notices for which these data are available, the average time from discovery to notification was 137 days in 2022 and the median time was 93 days.[782] Eighty-seven percent of these notices

---

included both the date of the discovery of the breach and the date the notice was sent to affected individuals. For those 164 notices, the average number of days between discovery and notice was 144 and the median number of days was 107. One hundred fifty of these notices (91%) were sent more than 30 days after discovery. The minimum number of days was 0 and the maximum was 538. The Proposing Release cited an average number of days between discovery and notice of 197 (for calendar year 2021). The correct number should be 97. This change would not have affected the Commission's assessment, in the Proposing Release, that there would be substantial economic benefits from a new notification deadline in an amended Regulation S-P, as both estimates are substantially larger than 30 days.

778 The final amendments' 30-day notification timeframe starts when a covered institution becomes aware that unauthorized access to or use of customer information has occurred or is likely to have occurred. *See* final rule 248.30(a)(4)(iii). The analysis performed here relies instead on an entity's description of when it discovered or became aware of a breach, which could refer to a different point in time.

779 *See supra* footnote 544 and accompanying text.

780 *See* RCW 19.255.010(8).

781 *See* RCW 19.255.010(8).

782 This analysis was performed using data from the Washington State Office of the Attorney General, *Data Breach Notifications*, *available at* https://www.atg.wa.gov/data-breach-notifications (last visited Apr. 8, 2024). Washington law requires that any business, individual, or public agency that is required to issue a security breach notification to more than 500 Washington residents as a result of a single security breach shall electronically submit a single sample copy of that security breach notification. One hundred and eighty-five such notices were reported in the year 2022. For 121 (65%) of those notices, data is available for both the date of the discovery of the breach and the date the notice was sent to affected individuals. For

were sent later than 30 days after the discovery of the breach, presumably as a result of these exceptions.[783] Hence, we expect that the timing requirements of the final amendments will result in many notices being sent earlier even in some states with a 30-day deadline.

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.[784] Based on the data from the California Office of the Attorney General, the average number of days between the start of a breach and its discovery was 46 days in 2022, with a median of 7 days and a standard deviation of 126 days.[785] In addition, data from the Washington Attorney General's Office show that in 2022, there were on average 94 days between the time a breach occurred and its discovery, with a median of 10 days

---

those 121 notices, the average number of days between discovery and notice was 137 and the median number of days was 93. One hundred four notices (87%) were sent more than 30 days after discovery. The minimum number of days was 4 and the maximum was 651.

783 These numbers should be interpreted with care, since what different firms describe as the time at which they "discover" a breach could vary. *See also supra* footnote 778.

784 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 versus 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., generally change over time).

785 *See supra* footnote 777 describing the methodology. Many breaches, for example in the case of ransomware attacks or compromises of physical equipment, are discovered on the day that they happen or shortly thereafter.

and a standard deviation of 319 days.[786] This suggests that time to discovery is likely to prevent issuance of timely customer notices in many but not all cases. As plotted in Figure 9, while some firms take many months—even years—to discover a data breach, others do so in a matter of days: 66 percent of firms were able to detect a breach within 2 weeks and 77 percent were able to do so within 30 days.[787] Thus, while the adopted 30-day notification outside timeframe may not always substantially improve the timeliness of customer notices, in many cases it may improve timeliness.

---

[786] *See supra* footnote 782 describing the methodology. A few factors could influence the estimated length of time between a breach and its discovery by the notifying entity. First, the two states discussed here (California and Washington) require firms to report the date on which the breach started. In instances where firms do not know this information, they could report the discovery date instead. This would result in an underestimate of the time between when a breach occurs and its discovery. Second, as discussed above, different firms could interpret the meaning of discovery differently. *See supra* footnote 783. Third, the discovery date used for this estimate is the date on which the notifying entity discovers the breach. If the breach happened at a service provider, it is possible that the service provider discovered the breach earlier and notified its client later. Hence, the numbers reported here likely overestimate the amount of time the affected entity took to discover the breach when the breach affected an entity different from the notifying entity. For comparison, according to IBM, in 2023 it took an average of 207 days to identify a data breach. *See* 2023 IBM Cost of Data Breach Report.

[787] Based on data from the State of California Department of Justice, Office of the Attorney General. *See supra* footnote 777; footnote 785 and accompanying text. The equivalent numbers for Washington are 56% and 73%, based on data from the Washington State Office of the Attorney General. *See supra* footnote 782; footnote 786 and accompanying text.

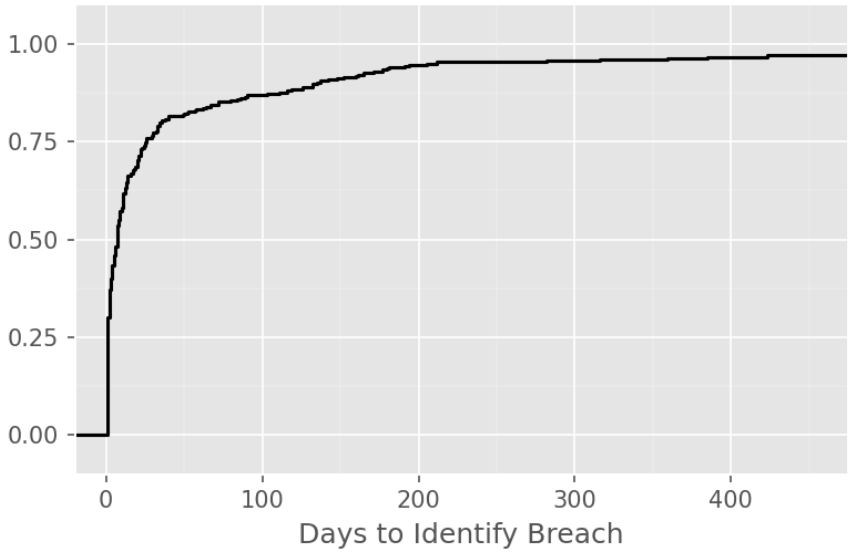

Figure 9: Cumulative distribution of the number of days between a breach and its discovery based on breaches reported in California in 2022. Data source: State of California Department of Justice, Office of Attorney General.

While we do not expect that the 30-day outside timeframe for customer notification will impose significant direct costs relative to a longer timeframe (or relative to having no fixed timeframe), the shorter outside timeframe might potentially lead to indirect costs arising from notification potentially interfering with incident containment efforts. Based on data from the Washington Attorney General's Office for the fiscal year of 2022, "containment" of data breaches generally occurs quickly—7.6 days on average.[788] However, according to IBM's study for 2022, it takes an average of 70 days to "contain" a data breach.[789] The discrepancy suggests

[788] 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 the exposure of consumer data, after discovering the breach." *See supra* footnote 782.

[789] 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* 2022 IBM Cost of Data Breach Report. We use the 2022 average here (70 days) to align with the date of the Washington and California state data, but note that IBM reports for 2021 and 2023 reported averages of 75 and 73 days, respectively. *See* Proposing Release at n.466; 2023 IBM Cost of Data Breach Report. Some of the discrepancy may be due to variation in how entities report the date at which the breach started in the data for Washington; *see supra* footnote 786.

that there exists some ambiguity in the interpretation of "containment," raising the possibility that the 30-day notification outside timeframe might require customer notification to occur before some aspects of incident containment have been completed and potentially interfering with efforts to do so.[790]

Some commenters opposed the proposed timeframe for customer notifications.[791] One commenter stated that the proposed outside timeframe of 30 days after becoming aware of a breach was insufficient time to provide a meaningful notification to impacted individuals, particularly in complex cases.[792] Another commenter stated that the proposed 30-day outside timeframe was "unjustified and arbitrary" and that it was "likely to be insufficient for proper investigation and notification."[793] Another commenter stated that the proposed timing requirement was overly rigid and did not account for the wide variety and complexity of cybersecurity incidents, and that 30 days after becoming aware of a possible incident was not enough time to accomplish the many steps required to be able to issue notifications to affected individuals.[794] This commenter detailed these steps as "needing to respond to and remediate the security incident directly, conduct a forensic investigation to determine what information may have been affected, analyze the affected data to determine what sensitive customer information is contained in affected data, extract or obtain the information needed to make notification to affected users, hire vendors and arrange identity protection services for affected individuals, and

---

790 For example, the notice may prompt the attacker to accelerate efforts to obtain or use sensitive information before the vulnerability can be completely contained.

791 *See, e.g.*, ACLI Comment Letter; IAA Comment Letter 1.

792 *See* ACLI Comment Letter. *See also* Cambridge Comment Letter; IAA Comment Letter 1.

793 *See* Federated Comment Letter.

794 *See* CAI Comment Letter.

actually send the notifications."[795] These commenters, as well as other commenters, suggested longer or less specific timeframes.[796]

A different commenter instead stated that the final required timeframe should not be longer than 30 days, citing an article stating that "an analysis of the current state data breach notification laws shows that requiring notification within thirty days of a breach to affected consumers would be appropriate."[797] This article further adds that a "thirty-day time limit will give an organization ample time to conduct a full investigation" and "ensure that consumers are notified of a breach in a timely manner so they can take the proper steps to mitigate any losses and protect their personal information from further exposure to cybercriminals through credit freezes, credit monitoring, and the like." The same commenter suggested that the deadline be shortened to 14 days after becoming aware of an incident.[798]

After considering these comments, we are adopting the notification timeframe as proposed. Under the final amendments, covered institutions will be required to provide notice to affected customers 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. Commenters stated that this notification timeframe may result in customers

---

795 *See* CAI Comment Letter.

796 *See, e.g.*, FSI Comment Letter ("We recommend that the notification requirement under Reg S-P be revised from 'as soon as practicable, but not later than 30-days' to 'as soon as practicable, but not later than 60-days' after a firm becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to occur."); Cambridge Comment Letter ("A period of, for example, 60 days would be more realistic, while achieving the Proposals' same goals."); IAA Comment Letter 1 ("We recommend a 45-day rather than a 30-day notification requirement to provide a more reasonable amount of time for advisers to perform investigation and risk assessments, collect the information necessary to include in client notices, and provide notices in complex cases.").

797 *See* Better Markets Comment Letter, citing Gregory S. Gaglione Jr., *The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America*, 67 Buff. L. Rev. 1133 (2019).

798 *See* Better Markets Comment Letter.

receiving notices that are less accurate or receiving some notices that are unnecessary. The final amendments' notification timeframe may, in some cases, result in customers receiving less informative notices than they would have received under a longer notification timeframe, since covered institutions will have less time to understand the incident before sending the notice. This 30-day timeframe may also result in instances where a notification will be sent but, had the covered institution been able to fully investigate the breach in the prescribed timeframe, the covered institution would have been able to determine that notification was not required.[799] If unnecessary notifications are sent, as commenters suggest could occur, these instances may result in customers taking unnecessary mitigating actions, and the costs of these actions will be a cost of the final amendments.[800] These instances will also result in additional costs associated with customer notification, such as administrative costs related to preparing and distributing notices and potential reputational costs (including indirect costs of customer information protection improvements that may be undertaken to avoid such reputational costs) for covered institutions; we have accounted for these additional costs associated with notification in our estimates of some of the costs arising from notice issuance.[801] However, the 30-day notification timeframe preserves the benefits of the proposed, relatively short notification timeframe and allows customers to take rapid and effective mitigating actions.[802]

---

799 Longer investigations are likely to correlate with more complicated incidents and are less likely to result in a determination that notice is not required. We therefore do not expect that a longer notification outside timeframe would have led to significantly fewer required notices.

800 *See infra* section IV.D.1.b(4) for a discussion of the effect of unnecessary notification.

801 Certain costs arising from notice issuance are covered in the Paperwork Reduction Act analysis in section V and are estimated to be on average $5,178 per year per covered institution. This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $3,862 per year per covered institution. *See infra* section V. We have increased these estimates from the proposal in response to commenters. *See infra* section V.

802 We have further reviewed, in response to commenters, evidence that customers prefer an early notification. A survey of U.S. individuals found that notifying customers immediately was one of main steps the

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.[803] It could also make other threat actors aware of vulnerabilities in a covered institution's systems, which they could then try to exploit. The final amendments allow a covered institution to delay notification of customers if the Attorney General determines that the notice required poses a substantial risk to national security or public safety and notifies the Commission of such determination in writing.[804] The main benefit of this delay is to decrease the likelihood of the potential situations described above where law enforcement is hindered. The delay might, in some cases, lead to a better protection of national security and public safety. Another benefit of the delay is that it might give covered institutions more time to assess the scope of the incident and gather the information to be included in the notice to customers in particularly complex cases. However, the delay provisions might also, in some cases, result in customers being notified later, which would decrease the benefits of such notification, as described above.[805] Where investigations do not rise to the level of meeting the prescribed conditions for delayed notification, customer notification could alert attackers that their intrusion has been detected and could potentially impact law enforcement's investigation.

Because we do not have data on the frequency with which an investigation will rise to the level of meeting the final amendments' conditions for delayed notification, and because we do

---

respondents would recommend to firms after a data breach, providing evidence that extending the timeframe is likely to therefore reduce the benefits of the notification requirement. *See* Lillian Ablon et al., *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, RAND Corporation (2016), *available at* https://www.rand.org/pubs/research_reports/RR1187.html. Customers who receive notices faster are better able to take appropriate mitigating actions.

803 The attacker could then work to remove evidence on the covered institution's systems, thereby making the identity of the attacker harder to uncover by law enforcement.

804 *See* final rule 248.30(a)(4)(iii).

805 *See supra* text following footnote 783.

not have data on the scope of the effect on national security or public safety of breaches being revealed to the attackers, nor did commenters identify such data, we are unable to precisely estimate the costs and benefits of this provision. However, we expect that such events will be relatively rare.[806]

(3) Broader Scope of Information Triggering Notification

In the final amendments, "sensitive customer information" is defined more broadly than in most state laws, yielding a customer notification trigger that is broader in scope than the various state law notification triggers included under the baseline.[807] The broader scope of information triggering the notice requirements will cover more data breaches impacting customers than the notice requirements under the baseline. This broader scope might benefit customers who will be made aware of more cases where their information has been compromised. At the same time, the broader scope might lead to false alarms—cases where the "sensitive customer information" divulged does not ultimately harm the customer. Such false alarms might be problematic if they reduce customers' responsiveness to data breach notices. In addition, the scope will also likely imply additional costs for covered institutions, which may

---

806 *See* SIFMA comment letter 2 ("The Commission should be aware that under present practice and experience, the number of cases where delay is requested or mandated by other government entities, or court orders, is quite limited—so the SEC need not assume or fear that notification delays would become routine or be otherwise abused."). In addition, the state of California requires that, if a notice sent to individuals affected by a breach was delayed at the request of law enforcement agency, the notice mention such delay. *See* Cal. Civil Code § 1798.82. Of the 456 notices reported in 2022, only 4 indicated that they were delayed at the request of law enforcement. *See supra* footnote 777 for a description of these data. Because the final amendments' conditions for a notification delay are stricter than those under California law, we expect that the frequency at which covered institutions will delay notifications for national security and public safety reasons will be even lower.

807 *See* final rule 248.30(d)(9) and *supra* section IV.C.2.a(1).

need to adapt their processes for safeguarding information to encompass a broader range of customer information and may need to issue additional notices.[808]

In the final amendments, "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."[809] The 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 will thus potentially require a covered institution to notify customers under the final 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. Basic definitions are used by 14 states, which account for 21 percent of the U.S. population.[810] 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 financial account number combined with an access code. For the estimated 15 million potential

---

808 Estimates of certain costs related to notice issuance are discussed in section V.

809 Final rule 248.30(d)(9).

810 *See supra* section IV.C.2.a(1).

customers residing in these states,[811] 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.[812] Such compromises could nonetheless lead to substantial harm or inconvenience. Thus, the final amendments will 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.[813] These definitions 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).[814] For the estimated 55 million potential customers residing in the states with enhanced definitions,[815] the benefits from the final amendments will be somewhat more limited. However, even for these customers, the amendments will tighten the effective notification requirement. There are many pieces of information not covered by the enhanced definitions whose compromise might 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. Under many such state laws, the compromise of information such as

---

811 *See supra* footnote 767.

812 *See supra* text accompanying footnote 532.

813 *See supra* section IV.C.2.a(1).

814 *See id*.

815 *See supra* footnote 767.

a customer's name, combined with his or her transaction history, account balance, or other information not specifically enumerated would not necessarily trigger the notice requirement.

The broader scope of information triggering a notice requirement under the final amendments will benefit customers. As discussed above, many pieces of information not covered under state data breach laws could, when compromised, cause substantial harm or inconvenience. Under the amendments, data breaches involving such information might 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.[816] A large number of such unnecessary notices might undermine the effectiveness of the notice regime.[817]

The broader minimum standard for notification is likely to result in higher costs for covered institutions. There will be increased administrative costs related to preparing and distributing notices for covered institutions who will send out additional notices as a result of the scope of information triggering a notice requirement under the final amendments. As discussed below, we estimate that certain costs associated with the preparation and distribution of notices will be, on average, $5,178 per year per covered institution.[818]

---

816 This may be the case even though the amendments include 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 notify, or it could investigate but not reach a conclusion that satisfied the terms of the exception.

817 *See infra* section IV.D.1.b(4) for a discussion of the effects of notification specifically.

818 This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $3,862 per year per covered institution. *See infra* section V.

In addition, it is possible that 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.[819] 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 adopted minimum standard might not have a significant prophylactic effect and might lead to an increase in reputation and litigation costs for covered institutions resulting from more frequent breach notifications.

Furthermore, because the definition of sensitive customer information is based on a determination that the compromise of this information could create a "reasonably likely risk of substantial harm or inconvenience to an individual identified with the information,"[820] it could increase costs related to incident evaluation, outside legal services, and litigation risk. While we lack data, and no commenter suggested such data, that would allow us to quantify all of these

---

819 We lack data, and no commenter suggested such data, that would allow us to quantify the indirect costs resulting from any potential upgrade to customer information safeguards that covered institutions could choose to implement as a result of the final amendments in order to avoid potential reputational costs associated with customer notification following a breach.

820 Final rule 248.30(d)(9). *See supra* section II.A.3.c; *infra* section IV.D.1.b(4).

costs, we discuss below certain costs associated with developing and implementing policies and procedures to comply with the final amendments, including costs for internal and external counsel.[821] This subjectivity could reduce consistency in the propensity of covered institutions to provide notice to customers, reducing the utility of such notices in customers' inferences about covered institutions' safeguarding efforts.

Some commenters opposed the proposed amendments' definition of sensitive customer information, suggesting either a better alignment with existing regulation,[822] or that the final amendments specify a list of customer information included in the definition.[823] Covered institutions will have to devote some resources determining what specific pieces of information are included in the scope of the final notification requirements. However, different types of covered institutions may keep different types of customer information, the information collected by covered institutions might change in the future, and the type of information that could create a reasonably likely risk of substantial harm or inconvenience to an individual might also change in the future. Thus, having a wide and general range of sensitive customer information trigger the amendments' notice requirement will provide benefits to the affected customers, who may not receive a notice under the baseline. In addition, as discussed above, existing regulations adopt widely different definitions of customer information triggering a breach notification, making alignment difficult.[824]

---

821 *See infra* section V.

822 *See* Computershare Comment Letter; ICI Comment Letter 1; SIFMA Comment Letter 2.

823 *See* CAI Comment Letter; SIFMA Comment Letter 2.

824 *See supra* section IV.C.2.a(1).

(4) Notification Trigger

The final amendments include a 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, unless, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, the covered 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.[825] As discussed above, the final amendments reflect a presumption of notification: a covered institution must provide a notice unless it determines notification is not required following a reasonable investigation.[826] Moreover, if the covered institution is unable to determine which customers are affected by a data breach, a notice to all potentially affected customers is required.[827] The resulting presumptions of 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 or to estimate the potential for such information to be used in a way that is likely to cause harm.[828] Because of this, it may not be feasible to establish the likelihood of sensitive customer information being used in a manner that would result in substantial harm or inconvenience or of

---

825 *See* final rule 248.30(a)(4)(i).

826 *See supra* section II.A.3. A covered institution's determination that there is no risk of harm or inconvenience may also take into consideration whether the compromised data was encrypted. *See supra* section II.A.3.b. We expect that this could mitigate the risk of unnecessary notification. We considered a safe harbor from the definition of sensitive customer information for encrypted information. *See infra* section IV.F.3.

827 *See* final rule 248.30(a)(4)(ii); *see also supra* section II.A.3.a.

828 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.

sensitive customer information pertaining to a specific individual being accessed or used without authorization. Consequently, in the absence of the presumptions of notification, it may be possible for covered institutions to avoid notifying customers in cases where it is unclear what information was compromised or whether sensitive customer information was or is reasonably likely to be used in a manner that would result in substantial harm or inconvenience.

Currently, 20 states' notification laws do not include a presumption of notification.[829] We do not have data with which to estimate reliably the effect of these presumptions on the propensity of covered institutions to issue customer notifications, and no commenter suggested such data. However, we expect that for the estimated 20 million potential customers residing in the 20 states without a presumption of notification,[830] some notifications that will be required under the final amendments would not occur under the baseline. Thus, we anticipate that the final amendments will improve these customers' ability to take actions to mitigate the effects of data breaches. In addition, the final amendments' presumptions for notification rest on a concept of "substantial harm or inconvenience" that is likely to be wider than the equivalent concept of "harm" used in some state laws.[831] Hence, we also expect that the presumptions of notification will have potential benefits even for the customers residing in some of the states with a presumption of notification.

The increased sensitivity of the notification trigger resulting from the presumptions of notification will result in additional costs for covered institutions, who will bear higher

---

829 *See supra* section IV.C.2.a(1).

830 *See id.*; *see also supra* footnote 767.

831 *See supra* section II.A.3.c for a discussion of the concept of "substantial harm or inconvenience." Some states use a narrower definition of harm, for example including only fraud or financial harm. *See supra* section IV.C.2.a(1); *see also* Fla. Stat. § 501.171(4)(c) and Iowa Code § 715C.2(6) for examples of states with a presumption for notification but a narrower concept of harm.

reputational costs (including indirect costs of customer information protection improvements that may be undertaken to avoid such 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. While we are unable to quantify all of these additional costs,[832] we estimate that certain costs associated with the preparation and distribution of notices will be, on average, $5,178 per year per covered institution.[833]

Some commenters disagreed with the proposed requirement that if a covered institution were unable to determine which customers were affected by a data breach, it would have had to notify all individuals whose sensitive customer information resided in the customer information system that was, or was reasonably likely to have been, accessed or used without authorization.[834] One commenter stated that this would result in significant over-notification of individuals, and that this would unnecessarily disturb and frighten individuals who likely were not affected.[835] The commenter also stated that the proposed requirements would significantly increase costs and litigation risk for covered institutions and possibly their service providers and other financial institutions whose information resides on the system.[836] Another commenter stated that this proposed provision would create reputational risks for transfer agents and that it believed resources would be better spent investigating the incident and determining the impacted

---

832 As stated above, we do not have data with which to estimate reliably the effect of these presumptions on the propensity of covered institutions to issue customer notifications, and no commenter suggested such data. In addition, as stated above, we lack data, and no commenter suggested such data, that would allow us to quantify the indirect economic costs, such as reputational cost of any potential increase in the frequency of customer notification. *See supra* section IV.D.1.a.

833 This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $3,862 per year per covered institution. *See infra* section V.

834 *See, e.g.*, CAI Comment Letter; IAA Comment Letter 1.

835 *See* CAI Comment Letter.

836 *See* CAI Comment Letter.

securityholders.[837] Another commenter stated that this proposed requirement would be unnecessarily burdensome for covered institutions and that it could have negative consequences for clients, noting that there would be a risk that too much information could be overwhelming and lead to desensitization.[838]

Another commenter disagreed with the proposed requirement that a covered institution would have had to notify customers whose information was compromised unless the covered institution could determine that the event would not result in a risk of substantial harm or inconvenience for these individuals, suggesting instead that the standard be harmonized further with the Banking Agencies' Incident Response Guidance and with many state laws so as to require notification only if the covered institution affirmatively could find risk of harm.[839] This commenter stated that the proposed presumption of notification could lead to excessive and unnecessary notifications to consumers where a low likelihood of harm were present, which could result in consumers spending time and effort needlessly monitoring accounts or taking actions such as instituting a credit freeze, and simultaneously desensitize consumers to a notification for an actual breach where significant harm could result.[840]

After considering these comments, we have determined that the presumptions of notification should be included in the final amendments. On the one hand, we acknowledge, as commenters stated,[841] that unnecessary notifications could occur and negatively affect covered institutions and their customers as a result of these presumptions. Unnecessary notifications will

---

837 *See* Computershare Comment Letter.

838 *See* IAA Comment Letter 1.

839 *See* SIFMA Comment Letter 2.

840 *See* SIFMA Comment Letter 2.

841 *See supra* footnotes 834-840 and accompanying text.

result in costs for covered institutions, including the costs associated with notification such as administrative costs related to preparing and distributing notices as well as reputational costs, litigation risk, or diversion of resources identified by commenters. [842] More broadly, as stated by commenters,[843] unnecessary notification could reduce customers' responsiveness to data breach notices, for example by decreasing customers' ability to discern which notices require action. Unnecessary notification could also desensitize customers to notices, thereby leading to a decrease in the reputational costs of notification. This could decrease covered institutions' incentives to invest in customer information safeguards in order to avoid such reputational costs.[844] However, the risks of unnecessary notification reducing the benefits of the rule are mitigated by the fact that notification is not required in cases where the covered institution can determine, after a reasonable investigation, that there is no risk of substantial harm or inconvenience for the customers whose information has been compromised. In addition, in a change from the proposal, the final amendments explicitly provide that a covered institution need not provide notice to an individual whose sensitive customer information resides in the customer information system that was, or was reasonably likely to have been, accessed or used without authorization if the covered institution reasonably determines that this individual's sensitive customer information was not accessed or used without authorization.[845]

On the other hand, adopting these presumptions of notification will allow potentially affected customers to take appropriate mitigating actions. In support of the proposed

---

842 *Id*.

843 *See* IAA Comment Letter 1; SIFMA Comment Letter 2.

844 Estimates of certain costs related to notice issuance are discussed above. *See supra* footnote 833 and accompanying text.

845 *See* final rule 248.30(a)(4)(ii).

presumption of notification, another commenter stated that any risk that a presumption to notify individuals could lead to a volume of notices that would inure affected individuals to the notices and result in their not taking proactive action would be outweighed by the risk that individuals would not be notified at all and would not have the opportunity to decide for themselves whether to take action.[846] To support this statement, this commenter referenced a study stating that requiring a determination of misuse to trigger disclosure permits additional discretion to the breached entity which, coupled with the existence of a disclosure disincentive,[847] might bias an institution's investigation of a data leak and might lead to a conclusion that consumer notification was not required.[848] We agree with this commenter. In addition, as discussed above, allowing covered institutions to conduct a full investigation before determining whether customers need to be notified could significantly reduce the benefits of such notification, and thus of the final amendments, by delaying the notice.[849]

(5) Content and Method of Notice

The proposed amendments included a list of information that would have had to be included in a customer notice.[850] Many of these content requirements remain in the final amendments.[851] While some commenters agreed generally with the proposed notice content

---

846 *See* Better Markets Comment Letter.

847 *See supra* section IV.B.

848 *See* Better Markets Comment Letter, citing Paul M. Schwartz and Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 939 (2007). In addition, a report cited by the same commenter discusses the frequency of notification and how it relates to specific notification trigger. The report links higher frequency of notification to a requirement that a government official participate in the determination that a data breach creates risk for the affected parties, and therefore that notification is required. *See* IRTC Data Breach Annual Report; *see also supra* footnote 518 and accompanying text.

849 *See supra* section II.A.3.a; *see also supra* section IV.D.1.b(2) for a discussion of the benefits of timely notification.

850 *See* proposed rule 248.30(b)(4)(iv).

851 *See* final rule 248.30(a)(4)(iv).

requirements,[852] other commenters disagreed with the proposed inclusion of some elements and stated that our analysis of these requirements in the Proposing Release was insufficient.[853] In response to these commenters, we conducted supplemental analysis of the frequency at which different items are required in existing state laws, and are including a supplemental analysis of the costs and benefits of each of the required elements vis-à-vis this baseline.[854]

The main benefit of requiring specific content to be included in the notice is to help ensure that customers residing in different states receive similar information when their information is compromised in the same breach. Because state law requirements differ in terms of required content, covered institutions may send different notices to different individuals.[855] The final amendments will help ensure that all customers receive a minimum of information regarding a given breach affecting their information and are therefore equally able to take appropriate mitigating actions.

The final amendments provide that the notice must include a description of the incident, including the information that was breached and the approximate date at which it occurred, as well as contact information where customers can inquire about the incident. In addition, the notice must include information on recommended actions affected customers can take. We expect that these required items will help customers take appropriate mitigating action to protect themselves from further effect of the breach. Including these elements might require some

---

852 *See, e.g.*, Better Markets Comment Letter.

853 *See, e.g.*, CAI Comment Letter.

854 *See supra* section IV.C.2.a(2).

855 *See* ICI Comment Letter 1 ("In discussing breach notices with our members, we understand it is not uncommon for their current breach response programs to include separate notification letters depending upon the state the individual resides in.").

covered institutions to modify their existing processes for notification, which will incur some costs.[856] We expect that these costs will be passed on to customers.

The first required item is a general description of the incident and the type of sensitive customer information that was or is reasonably believed to have been accessed or used without authorization.[857] We received no comment on this specific requirement. Obtaining this information is crucial for customers as it will allow them to assess the level of risk and to take appropriate mitigating actions. This will also allow them to avoid spending time and resources on mitigating actions related to information that was not affected by the breach. We expect that most covered institutions who already have notification processes already include this information, since 22 states require that the notice describe the type of information affected by the breach and 13 states require a description of the incident to be included.[858] As a result, we expect that the benefits will be the greatest for customers of institutions who do not operate nationally and operate only in states without such requirements. We estimate that there are approximately 51 million potential customers residing in the 38 states that do not require a description of the incident, and 35 million potential customers residing in the 29 states that do not require the type of customer information compromised to be included in the notice.[859] We expect the costs to be the highest for the covered institutions operating only in those states.

---

856 These costs are included in the policies and procedures costs discussed in section IV.D.1 above. As discussed below, we estimate that certain costs associated with developing and implementing policies and procedures to comply with the final amendments will be, on average, $15,445 per year per covered institution. This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $5,425 per year per covered institution. *See infra* section V.

857 *See* final rule 248.30(a)(4)(iv)(A).

858 *See supra* section IV.C.2.a(2).

859 *See supra* footnote 767.

The second item required by the final amendments is the date of the incident, the estimated date of the incident, or the date range within which the incident occurred, if the information is reasonably possible to determine at the time the notice is provided.[860] One commenter disagreed with this proposed requirement, stating that it would imply that covered institutions subject to both Regulation S-P and the Banking Agencies' Incident Response Guidance would have to revise their long-standing breach notices to add the information.[861] This commenter also stated that the Proposing Release did not detail a basis for this inclusion. Including the date of the breach, even if it is the approximate date, will provide useful information to the affected customers and help them make better decisions about the mitigating actions to take. In particular, customers could review their account statements back to the date where the breach happened.[862] An additional benefit of this inclusion will be to provide information to customers about how effectively a covered institution was able to detect and assess a breach. This will help reduce the information asymmetry about a covered institution's customer information safeguards and help customers be better informed when deciding which covered institutions to retain for their financial services needs.

There are 13 states requiring the notice to include an approximate date (or date range) for the breach, and 38 states without such a requirement.[863] These 38 states account for 70 percent of the U.S. population and 49 million estimated potential customers.[864] For these customers, the final amendments might result in their receiving information they would not have otherwise

---

860 *See* final rule 248.30(a)(4)(iv)(B).

861 *See* ICI Comment Letter 1.

862 *See supra* footnote 210 and accompanying text.

863 *See supra* section IV.C.2.a(2).

864 *See supra* footnote 767.

received. Because 13 states already require that the notice include an approximate date, we expect that the costs will be minimal for the covered institutions that operate nationally. For the covered institutions that do not operate nationally, the final amendments might require them to adapt their procedures to include additional information in the notices to customers.

The third item required by the final amendments is "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." [865] One commenter disagreed with this proposed requirement, stating that it was unclear what purpose or benefit this requirement would have for the affected individuals and adding that it would place significant burdens on the internal operations of the covered institution.[866] Another commenter also disagreed with this proposed requirement, stating that covered institutions should have flexibility in determining the contact information to provide, based on how they normally interact with their customers, and suggesting that the final amendments only require one of the listed contact methods.[867] The requirement to include multiple contact methods provides valuable options for affected customers, who may have differing preferences and aptitudes in their use of contact methods.[868] We do not expect that this requirement will overly burden covered institutions, even for those

---

865 Final rule 248.30(a)(4)(iv)(C).

866 *See* CAI Comment Letter.

867 *See* SIFMA Comment Letter 2.

868 In addition, the final amendments will not preclude a covered institution from providing the contact information of a third-party service provider. *See supra* footnote 211.

institutions that will need to adapt their processes to the new requirements.[869] In addition, nothing in this requirement prevents a covered institution from providing additional contact methods.

The final amendments also require the notice to include a recommendation that the customer review account statements and immediately report suspicious activity to the covered institution (if the individual has an account with the covered institution); an explanation of what a fraud alert is and how an individual may place one; a recommendation that the individual periodically obtain credit reports; an explanation of how the individual may obtain a credit report free of charge; and information about the availability of online guidance from the FTC and usa.gov regarding steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the FTC, and the FTC's website address.[870] One commenter supported these proposed requirements, stating that the proposed notice requirements avoided common problems with the content of many data breach notifications, such as confusing language, a lack of details, and insufficient attention to the practical steps customers should take in response.[871] We expect that these additional elements will provide useful information to affected customers regarding potential mitigating actions to take and help ensure that these customers are able to react appropriately to the notice. We expect that while these requirements will impose costs on covered institutions whose notification

---

869 Ten states require the notice to include a phone number as contact information while two states require the notice to include a physical address. *See supra* section IV.C.2.a(2).

870 *See* final rule 248.30(a)(4)(iv)(D) through (H).

871 *See* Better Markets Comment Letter.

process does not already include these elements,[872] these costs will be limited and passed on to the customers.[873] We received no comments opposing these requirements.

The proposed amendments included a provision that would have required the notice to include a description of what has been done by the covered institution to protect the sensitive customer information from further unauthorized access or use. One commenter disagreed with this proposed requirement, stating that it "would be extremely useful to threat actors and not particularly useful to clients."[874] After considering this comment, we have decided to exclude this provision from the final amendments.[875] In addition to reducing the perceived risk of providing a roadmap for threat actors, we expect that this change will accelerate the process of preparing the notice, thereby reducing the associated costs.

The final amendments require that notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing.[876] Some commenters discussed the alignment between the requirements of the final amendments and those of existing regulation affecting covered institutions. In particular, one commenter stated that a Federal notification requirement would complicate compliance efforts for covered institutions already complying with similar state laws.[877] On the other hand, another commenter stated that the proposed amendments' alignment with existing requirements would

---

872 Because some states require some of these elements to be included in the notification to affected individuals, we expect that many covered institutions already have procedures similar to those required by the final amendments. *See supra* section IV.C.2.a(2).

873 As discussed above, these costs will represent only a fraction of the policies and procedures costs discussed in section IV.D.1 above. *See supra* footnote 856 and accompanying text.

874 *See* IAA Comment Letter 1.

875 *See supra* section II.A.3.e.

876 *See* final rule 248.30(a)(4)(i). Under the final amendments, the notice can be sent electronically. *See supra* footnote 200 and accompanying text.

877 *See* CAI Comment Letter.

allow covered institutions to leverage existing programs.[878] We analyze here the expected benefits and costs of this provision of the final amendments vis-à-vis the baseline.[879]

We expect that the main benefit of this provision will be to help ensure that customers whose sensitive personal information has been breached receive the required information. We expect that the costs of this provision will be limited for most covered institutions since most states require similar methods of notification.[880] Hence, we expect that most covered institutions will not have to significantly modify their procedures and processes for notice issuance in order to satisfy this provision of the final amendments.

However, we do expect some benefits in some instances. First, 26 states allow a notice to be made over the telephone.[881] While 7 of these states require direct contact with the affected individuals when the notice is given using this method, 19 do not have such requirements.[882] We expect that for the 21 million potential customers residing in the 19 states allowing for telephonic notices but without such requirements,[883] receiving a written notice may result in clearer information and in a higher likelihood of taking appropriate mitigating actions.

Second, many states allow for electronic notifications. While most of these states require that this be done only under certain conditions that are similar to the final amendments' conditions, some states have conditions that are significantly looser. The final amendments provide that the notice can be provided through electronic means to customers who have agreed

---

878 *See* FSI Comment Letter.

879 *See supra* section IV.C.2.a(2).

880 *See id*.

881 *See id*.

882 *See supra* footnote 568 and accompanying text.

883 *See supra* footnote 767.

to receive information electronically.[884] In contrast, five states allow electronic notification without restriction, and two states require only that the institution has an email address for the affected individuals.[885] We expect that for the 11 million potential customers residing in these seven states[886]—that allow electronic notification even to customers who have not explicitly agreed to receiving electronic notification—the final amendments will help ensure that they receive a notice in a format that they are expecting.[887]

Third, all states allow for a substitute notice under certain conditions.[888] Substitute notification requirements vary across states but must generally include an email notification to affected individuals, a notice on the entity's website, and notification to major statewide media.[889] The final amendments do not provide for such substitute notice and instead have the same notice requirements in all cases. We expect that the final amendments will strengthen the benefits of notification by helping ensure that affected individuals are made aware of the relevant information regarding a breach of their sensitive information. Examples of customers who would benefit include customers who: interact infrequently with the covered institution, thereby not visiting the institution's website regularly; who do not consume local or state news sources; or who may be wary or skeptical of receiving such information by email if they have not given their prior informed consent (for example, customers who are used to receiving communications from

---

884 *See supra* footnote 200 and accompanying text.

885 *See supra* footnotes 565 and 566 and accompanying text.

886 *See supra* footnote 767.

887 We acknowledge that the final amendments may result in some customers receiving a notice in a format that they do not prefer. For example, customers could agree to an electronic notice but still receive a notice by mail, which they may be less likely to see or respond to.

888 These conditions often include a certain minimum number of affected individuals to notify and a minimum dollar cost to notify these individuals. *See supra* footnote 569 and accompanying text.

889 *See supra* section IV.C.2.a(2).

the covered institution by mail only or who interact with the covered institution very rarely). In other states, the requirements for substitute notice include fewer elements.[890] We expect that for the customers residing in these states, the final amendments will help ensure that they are made aware of the breach and provided an appropriate notice.

The final amendments require written notification, which may be provided electronically if certain conditions are met, such as if the customer has agreed to receive information electronically.[891] Not all state notification provisions include similar consent conditions for electronic communication.[892] Therefore, the final amendments may result in additional compliance costs in the instances where, prior to the final amendments, the covered institutions would have sent email notices or used substitute notification, but will instead have to obtain customer consent for electronic notification or else send individual notices by mail because their methods of electronic delivery are not consistent with existing Commission guidance on electronic delivery, for example if they have not obtained customer consent to receive electronic communications.[893] However, given the variety of state law conditions and requirements, we expect that most notices being sent already satisfy many of these provisions and we therefore expect that these provisions will result in limited additional costs.[894]

---

890 *See supra* footnote 571 and accompanying text.

891 *See supra* section II.A.3.e. and footnote 200.

892 *See supra* footnote 885 and accompanying text.

893 *Id*. Because some states have conditions for sending an electronic notice that are different from those under the final amendments, we expect that there might be some cases where a covered institution will be required to send a notice by mail when it could have sent an electronic notice under state law. *See supra* footnotes 884 through 888 and accompanying text.

894 An analysis of the notices sent to residents of California and Washington suggests that notices are frequently sent by postal mail. Both states allow for electronic notification if the notice is consistent with the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001). Nevertheless, we have found that in California, at least 90% of the notices appear to be sent by mail. The equivalent number is 89% for Washington. We identified the notices sent by mail (as opposed to those sent by email or satisfying other substitute notice requirements) as those including a redacted or mock recipient address, an address for

c. Service Provider Provisions

The final amendments require that a covered institution's incident response program include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers. Specifically, these written policies and procedures must be reasonably designed to ensure the service providers take appropriate measures to protect against unauthorized access to or use of customer information and provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred resulting in unauthorized access to a customer information system. Upon receipt of such notification, a covered institution must initiate its incident response program.[895] In the final amendments, "service provider" is defined as "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution."[896] Thus, the requirements might affect arrangements 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 service providers,[897] ensuring consistency in regulatory requirements increasingly requires consideration of the functions performed by service providers and how these functions interact with the regulatory regime.[898]

---

a return mail processing center, or an explicit mention such as "Via First-Class Mail." It is possible that notices containing none of these elements are sent by mail, and therefore we expect that the true percentages are likely to be higher than those reported here. *See supra* footnotes 777 and 782 and accompanying text for details on the notice data used for this analysis.

895 *See* final rule 248.30(a)(5)(i).

896 Final rule 248.30(d)(10).

897 *See supra* section IV.C.3.f

898 *See supra* section IV.C.2.a(3).

Ignoring such aspects could incentivize covered institutions to attempt to outsource functions to service providers to avoid the requirements that would apply if the functions were performed in-house. Thus, the service provider requirements will strengthen the benefits of the final amendments by helping ensure that they 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).

Commenters supported the proposal's objective to safeguard customer information in the case where this information rests with service providers.[899] One commenter stated that third-party service providers were specifically a favored attack vector, adding that the Commission's attention to this risk was well-directed.[900] Another commenter stated that it did not disagree that service providers should protect sensitive customer information and be required to provide timely notification of a breach to the covered institution.[901] Another commenter stated that service providers that have access to customer information should be contractually required to take appropriate risk-based measures and diligence designed to protect against unauthorized access to or use of customer information, including notification of a covered institution in the event of certain types of breaches in security.[902] Another commenter recognized and supported the importance of covered institutions having appropriate policies and procedures to manage the cybersecurity and privacy risks posed by service providers that process their customer information.[903]

---

899 *See, e.g.*, EPIC Comment Letter; SIFMA Comment Letter 2.

900 *See* EPIC Comment Letter.

901 *See* IAA Comment Letter 1.

902 *See* SIFMA Comment Letter 2.

903 *See* CAI Comment Letter.

Some commenters criticized the analysis of the proposed service provider provisions.[904] One commenter stated, referring to the proposed service provider written agreement obligation, that the Commission had failed to address the costs in any meaningful way and was thus dismissive of them.[905] Another commenter stated that the Proposing Release included no discussion or estimate of the costs that renegotiating contracts with service providers or hiring new service providers would impose on brokers.[906] In addition, some commenters disagreed with our analysis of specific parts of the requirements, stating that the analysis in the Proposing Release did not identify why a 48-hour reporting period was optimal,[907] or stating that the breadth of the definition of service providers was disproportionate to the benefits and risks presented.[908] In response to these commenters, we have modified this aspect of the amendments, as discussed in greater detail above.[909] These modifications mitigate, but may not eliminate entirely, commenters' concerns regarding the costs associated with the service provider provisions of the proposed amendments. We also have supplemented the economic analysis of the service provider provisions in response to comments as follows. First, we have supplemented the analysis of the potential costs to covered institutions. This includes an analysis of the indirect effects of the final amendments on covered institutions' service providers, and how these effects

---

904 *See, e.g.*, IAA Comment Letter 1; ASA Comment Letter.

905 *See* IAA Comment Letter 1.

906 *See* ASA Comment Letter. In the Proposing Release, we requested data that could help us quantify the costs and benefits that we were unable to quantify. We did not receive data or estimates from commenters that could help us quantify the costs of renegotiating contracts or hiring new service providers. *See* Proposing Release at section III.G, question 110.

907 *See* Microsoft Comment Letter.

908 *See* IAA Comment Letter 1 ("We believe the proposed definition of Service Provider is unrealistically and unnecessarily broad, reaching service providers where there are little or no marginal benefits to their inclusion and the costs (time, money, personnel, etc.) to advisers would be substantial.").

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

may affect covered institutions and their customers,[910] for example where costs to service providers are passed on to covered institutions, and ultimately to covered institutions' customers,[911] or have negative competitive effects that impact covered institutions.[912] Second, we are providing supplemental analysis specifically on the timeline requirement and the definition of service providers.[913]

The costs to covered institutions of implementing the final amendments will be influenced by the potential burdens on service providers that may result from the amendments. If implementing procedures that satisfy covered institutions' requirements were costless for them, service providers would be likely to agree to implement the requirements without much negotiation and the costs to covered institutions would be minimal. If, instead, such procedures were costly to implement for service providers, more negotiation would be required, which would be costlier for all parties involved. In addition, in this case, the service providers might increase the price of their services, further increasing the costs for covered institutions.[914] We discuss further below the expected indirect effects of the final amendments on service providers and how these effects may affect covered institutions.[915]

However, even if, as in the scenario described above, the cost per service provider turns out to be minimal for covered institutions, the total cost might still become significant for covered institutions that have a large number of service providers. Even in this case, covered

---

910 *See infra* footnotes 928-936 and accompanying text.

911 *See infra* text accompanying footnote 933.

912 *See infra* section IV.E.

913 Additional context for this analysis is provided in section IV.C.3.f.

914 Because we are not aware of any data, and no commenter suggested any data, that could be used to estimate how much service providers will pass through increased costs to covered institutions, we are unable to quantify the magnitude of the potential increased costs for covered institutions.

915 *See infra* text accompanying footnote 927.

institutions will need to devote time and resources to verify that they satisfy the final requirements with respect to each of their service providers. In addition, covered institutions will need to devote time and resources to oversee their service providers throughout their relationship with these service providers.[916] We are unable to quantify these costs, as the range would be too wide to be informative and commenters did not provide any data that would yield an estimation of such a range. The range of costs for covered institutions is likely to be wide given the varied nature of the uses of service providers by financial institutions. For instance, the cost for covered institutions that do not rely on service providers is likely to be minimal. However, for those covered institutions that have more complex arrangements with service providers, the cost would be significantly higher. The cost depends on a large number of factors that vary across covered institutions.[917] For example, the cost would depend on the number of service providers used, the extent to which service providers are used for multiple functions, each service provider's access to relevant customer information, as well as the staffing needs of the covered institutions.

The definition of service provider in the final amendments will affect the costs to covered institutions by determining the number of service providers for which covered institutions will

---

916 *See supra* section II.A.4. For PRA purposes, we have identified certain types of staff who we anticipate would be involved in implementing the rules. *See infra* section V.B. It is possible that those staff members may also be involved in oversight of service providers.

917 In a proposing release pertaining to service providers, the Commission anticipated a range of compliance costs associated with required oversight of service providers by registered investment advisers. For example, in the proposing release, the Commission estimated a range of $44,106.67 - $132,320 in ongoing annual costs per adviser associated with the proposed due diligence requirements (and further costs associated with proposed monitoring requirements and other aspects of the proposed rule). We do not believe those ranges of cost estimates are determinative in the context of the final amendments here. In particular, the scope of the final amendments differs substantially from the scope of that proposal. Those cost estimates pertained to a service provider's performance of outsourced functions that meet two elements: (1) those necessary for the adviser to provide its investment advisory services in compliance with the Federal securities laws; and (2) those that, if not performed or performed negligently, would be reasonably likely to cause a material negative impact on the adviser's ability to provide investment advisory services. By contrast, the final amendments here pertain to the protection of customer information in the case of all outsourced functions to all service providers. *See Outsourcing by Investment Advisers*, Release No. 6176 (Oct. 26, 2022) [87 FR 68816, 68821 (Nov. 16, 2022)].

have to perform these tasks. The final amendments adopt a definition of service provider to mean "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution."[918] Many commenters opposed the proposed definition of service provider.[919] These commenters suggested narrower definitions which would exclude a covered institution's affiliates.[920] In addition, one commenter stated that the proposed definition was unrealistically and unnecessarily broad, reaching service providers where there would be few or no marginal benefits to their inclusion and the costs (time, money, personnel, etc.) to covered institutions would be substantial.[921] This commenter suggested that the definition of service provider be limited to persons or entities with permitted access to sensitive customer information only.[922]

We acknowledge that fulfilling the requirements for each of their service providers will impose costs on the covered institutions. However, the potential benefits are also large given the increasing reliance of covered institutions on service providers.[923] Individual customers have no control over a covered institution's decisions to perform activities in-house or to outsource them.

---

918 Final rule 248.30(d)(10).

919 *See, e.g.*, IAA Comment Letter 1; Schulte Comment Letter. The definition of service provider in the final amendments is identical to the definition that was in the proposal. *See supra* section II.A.4.

920 *See* IAA Comment Letter 1 (stating that "the IAA believes that it is neither appropriate nor necessary to treat affiliates that provide services to an affiliated firm through a shared services or similar model as Service Providers"); Schulte Comment Letter ("We believe that the proposed definition of 'service provider' should exclude a Covered Institution's affiliates."); SIFMA Comment Letter 2 ("The associations also recommend that the Commission exclude affiliates of covered institutions from the definition of service providers, as affiliates are part of the same enterprise information/cybersecurity oversight as the covered institutions."); CAI Comment Letter ("The Committee requests that proposed Rule 30(e)(10) be revised to specifically exclude affiliates and other entities under common control with the covered institution.").

921 *See* IAA Comment Letter 1.

922 *See* IAA Comment Letter 1. This commenter also requested, if the proposed written contract requirement were to be kept in the final amendments, that it apply only to those service providers that have physical or virtual access to a covered institution's customer information system.

923 *See supra* section IV.C.3.f.

As such, these customers have little control over who has access to their information. A broad definition of service providers will contribute to safeguard customers' information and will help ensure that customers are notified in the event their sensitive information is compromised, no matter where this information resides. Furthermore, the modifications in the final amendments to require covered institutions to establish, maintain, and enforce written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers, instead of requiring written contracts as was proposed,[924] will alleviate the commenters' concerns over the potential inclusion of affiliates. Since affiliates are likely to have policies and procedures similar to those of covered institutions,[925] we expect that both the benefits and the costs of implementing this provision of the requirements will be minimal.

The indirect effects of the final amendments on service providers might also affect the costs borne by covered institutions and, ultimately, their customers. In particular, these indirect effects may generate costs to service providers, which may be passed on (at least partly) to covered institutions and ultimately to covered institutions' customers,[926] or may result in negative competitive effects on service provider industries that then impact the services offered to covered institutions and their customers.[927] The potential indirect effects on service providers that will

---

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

925 *See* IAA Comment Letter 1 ("Many advisers are structured in a manner that makes it administratively beneficial for them to obtain services from affiliates. These services often are provided by affiliates in a manner established by the organization's policies without the need for formal contracts because the affiliates are typically subject to company-wide policies and standards relating to safeguarding PII. Moreover, the information security policies of affiliates are typically subject to oversight by an organizational component that monitors compliance.") and Schulte Comment Letter ("We note that affiliates are typically included within the scope of a Covered Institution's cybersecurity policies and procedures and would also be covered by an applicable incident response plan.").

926 *See infra* text accompanying footnote 933.

927 *See infra* section IV.E.

result from the final amendments can be divided into three parts.[928] First, entities that meet the definition of service providers will likely take appropriate measures to protect against unauthorized access to or use of customer information to facilitate covered institutions' compliance with the final amendments. We expect that many service providers already take such measures.[929] Hence, we expect that the number of service providers who will modify their business processes for this specific requirement is limited. Such modifications will benefit not only the customers whose information is being better protected and the covered institutions relying on the service providers, but also the service providers themselves, to the extent that the modifications decrease the likelihood of unauthorized access to their customer information systems which could affect their operations or reputation.

Second, covered institutions' policies and procedures will need to be reasonably designed to ensure that service providers take appropriate measures to provide notification of unauthorized access to a customer information system to the covered institutions as soon as possible, but no

---

928 We are unable to quantify the indirect costs associated with these indirect effects that would be incurred by service providers as a result of the final amendments, as the cost range would be too wide to be informative. The uncertainty around these costs is due to a number of factors, including variation in complexity of service provider functions provided to covered institutions, the degree of market concentration across service provider markets (and hence the number of covered institutions a service provider may need to work with to comply with the rule), and variation in current service provider practices. The costs to any single service provider of meeting the burden for any single function for any single covered institution may therefore have substantial variance. For example, in certain cases a few service providers may perform the same function for many covered institutions and hence benefit from economies of scale. By contrast, service providers in less concentrated industries would potentially face higher costs.

929 For example, many states impose some form of requirements regarding the safeguard and the disposal of customer information. *See supra* footnote 603. In addition, the FTC Safeguards Rule requires financial institutions to take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for customer information and to require those service providers by contract to implement and maintain such safeguards. *See supra* footnote 618 and accompanying text. Hence, we expect that the service providers of private funds subject to the FTC Safeguards Rule already have customer information safeguards in place. This could lower the costs of the service provider provisions of the final amendments for the private funds advisers that are registered with the Commission and that are therefore covered institutions. *See supra* footnote 614 and accompanying text. Furthermore, service providers that are subject to other regimes such as the GDPR or DORA may already have appropriate safeguards in place.

later than 72 hours after becoming aware that the breach has occurred. This provision might also result in a number of service providers adapting their businesses processes. However, considering that 24 states require entities that maintain but do not own or license customer information data to notify the entity that owns or licenses such data "immediately" in case of a breach of security, we expect that many service providers already have processes in place to ensure that such notification is made.[930] For the service providers who do not already have such processes in place, this approach will create benefits for the customers who will be informed in a timely manner in the event their sensitive information is compromised.

Third, because the final amendments require covered institutions to establish, maintain, and enforce written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers who have access to their customers' information, these service providers will face requests for information from covered institutions or otherwise participate in the covered institutions' oversight activities. This will impose costs on service providers, but it will also strengthen the benefits of the amendments by helping ensure that customer information is appropriately protected even when it is residing in service providers' systems.

For service providers that provide specialized services aimed at covered institutions, the final amendments may create market pressure to enhance service offerings that facilitate covered institutions' compliance with the requirements.[931] Such enhancement will entail costs for specialized service providers, including the actual cost of adapting business processes, as

---

[930] In addition, other existing regulations have 72-hour reporting or notification deadlines. *See supra* footnote 257 and accompanying text; *see also supra* footnote 245.

[931] A service provider involved in any business-critical function likely "receives, maintains, processes, or otherwise is permitted access to customer information." *See* final rule 248.30(d)(10).

discussed above, to accommodate the requirements.[932] That said, we do not expect that these costs will represent an undue burden as both the specialized service providers and the covered institutions are operating in a highly regulated industry and might be accustomed to adapting their business processes to meet regulatory requirements. Moreover, more specialized service providers may be likely to have particularly sensitive or valuable information about the customers of covered institutions, and therefore the investor protection benefits in those cases may be substantial. With respect to service providers providing services aimed at a broad range of institutions, such as those providing email or customer-relationship management services, covered institutions are likely to represent a small fraction of their customer base. These service providers may be unwilling to adapt their business processes to the regulatory requirements of a small subset of their customers if they do not already have such processes in place.

For the service providers that already have in place processes satisfying the covered institutions' requirements, we expect that the costs to both the service providers and the covered institutions will be minimal and will mostly result from covered institutions' oversight duties. If service providers modify their business processes to facilitate covered institutions' compliance with the final amendments' requirements, we anticipate they likely will pass costs on to covered institutions, and ultimately covered institutions may pass these costs on to customers.[933] We also expect that there might be a fraction of service providers who will be unwilling to take the steps necessary to facilitate covered institutions' compliance with the final amendments. In such cases, the covered institutions will need to either switch service providers and bear the associated

---

932 We have no data on the number of specialized service providers used by covered institutions and on the frequency with which these service providers already adapt their business processes to regulatory changes, and no commenter suggested such data.

933 *See supra* footnote 718.

switching costs or perform the functions in-house and establish the appropriate processes as a result.[934] We expect that these costs will be particularly acute for smaller covered institutions which lack bargaining power with large service providers, and that these costs might be passed on to customers.[935] However, the amendments will create benefits arising from enhanced efficacy of the regulation.[936]

The proposal included a requirement that a covered institution's response program must include written policies and procedures requiring the institution, pursuant to a written contract between the covered institution and its service providers, to require that service providers take appropriate measures that are designed to protect against unauthorized access to or use of customer information.[937] While one commenter supported this proposed requirement,[938] other commenters suggested that the final amendments not require written contracts with service providers,[939] stating that doing so would impose significant costs on covered institutions.[940] After

---

934 Such switching costs could include the time and other resources necessary to find an alternative service provider, conduct appropriate due diligence, and negotiate prices and services provided. Performing the functions in-house may also be more costly than outsourcing them for covered institutions. A recent report finds that 73% of surveyed asset managers cite cost considerations when deploying outsourcing solutions. *See* Cerulli Report. The competitive effects associated with the cases where service providers choose to stop providing services to covered institutions as a result of the final amendments are discussed below. *See infra* section IV.E.

935 We expect that smaller covered institutions may be less able to pass these costs to customers. *See supra* footnote 718.

936 From the perspective of current or potential customers, the implications of customer information safeguard failures are similar whether the failure occurs at a covered institution or at one of its service providers.

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

938 *See* ICI Comment Letter 1.

939 *See, e.g.*, SIFMA Comment Letter 2; IAA Comment Letter 1.

940 *See, e.g.*, SIFMA Comment Letter 2 ("Requiring each service provider to revise its contract with a covered institution within 12 months of the Proposal's finalization would add an unnecessary burden to both covered institutions and service providers, as well as a potential significant cost."); IAA Comment Letter 1 ("Even if Service Providers agreed to enter into written agreements with advisers as proposed, advisers and Service Providers would both likely incur significant negotiation and implementation costs, which we do not believe are justified, especially when an alternative and less burdensome approach is available."); STA Comment Letter 2 (stating that "transfer agents, because of their relatively small size, simply do not have the negotiating power to demand contractual terms requiring third party service providers to maintain

considering these comments, we are requiring that covered institutions establish, maintain, and enforce written policies and procedures to require oversight of service providers instead of requiring written contracts.[941] This change, while enhancing the policies and procedures obligations, will provide covered institutions with greater flexibility in achieving compliance with the requirements, which could reduce compliance costs without significantly reducing the benefits of the final amendments.[942] Providing this flexibility will also help address commenters' concerns that requiring a written contractual agreement could harm covered institutions, particularly those that are relatively small and may not have sufficient negotiating power or leverage to demand specific contractual provisions from a larger third-party service provider.[943] However, in a scenario where a covered institution has an existing contract with a service provider that is renegotiated as a result of the final amendments, the covered institution may incur additional costs.[944] In addition, in a scenario where a service provider would have agreed to a written contract under the proposed amendments but will not under the final amendments, a covered institution may have to exert greater efforts to oversee this service provider than would have been necessary had it signed a written contract with this service provider.[945]

---

certain policies and procedures, or to demand permission to perform due diligence on a service provider's systems, policies, and procedures.").

941 *See supra* section II.A.4 and final rule 248.30(a)(5).

942 See supra section II.A.4; *see also, e.g.*, AWS Comment Letter.

943 *See, e.g.*, IAA Comment Letter 1.

944 It is difficult for us to quantify these costs, as we have no data on the provisions of existing contracts between covered institutions and their service providers relating to customer information safeguards, and no commenter suggested such data. Such costs are likely to be contract specific, as they will depend on the degree to which each existing contract may be revised as a result of the final amendments. Many such contracts may not be revised at all, while others may undergo more revisions. Moreover, in many cases, even where a contract could be revised as a means of complying with the final requirements, the covered institution may pursue compliance by other means.

945 There are a variety of ways in which covered institutions will be able to satisfy the oversight requirement. *See supra* section II.A.4.

We also proposed that the measures taken by service providers include notification to the covered institution as soon as possible, but no later than 48 hours after becoming aware of a breach in security resulting in unauthorized access to a customer information system maintained by the service provider.[946] While one commenter supported this proposed requirement,[947] other commenters stated that a longer deadline would be preferable.[948] One commenter also suggested a change from "becoming aware" to "determining" that a breach has occurred in order to minimize pressure to report on service providers while an investigation is being conducted.[949]

After considering these comments, we have changed this provision. The final amendments require covered institutions to ensure that their service providers notify them of a breach as soon as possible, but no later than 72 hours after becoming aware that an applicable breach has occurred.[950] We expect that the change to 72 hours will reduce the cost to service providers not only because it will give them more time to assess an incident before notifying the covered institution, but also because it aligns with existing regulation.[951] Hence, we expect that this change will decrease compliance costs for covered institutions by making service providers more likely to agree to the requirements, which will decrease negotiation and switching costs for

---

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

947 *See* ICI Comment Letter 1 ("We concur with the Commission requiring service providers to notify a covered institution notice within 48 hours of a breach impacting the covered institution or its affected individuals.").

948 *See, e.g.*, Microsoft Comment Letter ("Specifically, where the SEC determines that a cybersecurity incident reporting requirement is appropriate, the applicable rule should provide that the entity with the notification responsibility shall provide the required notice to the recipient as soon as possible but no later than 72 hours. The reporting deadline should begin to run once the entity with notification responsibilities has a reasonable basis to conclude that a notifiable incident has occurred or is occurring."); ACLI Comment Letter ("In the early days of containment and remediation it is often difficult to determine exactly what data has been compromised, making the 48-hour timeframe overly short and burdensome.").

949 *See* Google Comment Letter.

950 *See* final rule 248.30(a)(5)(i).

951 *See supra* footnote 257 and accompanying text.

covered institutions.[952] We also expect that this will alleviate some of the commenters' concerns about having insufficient negotiating power to negotiate specific with service providers.[953] While this change may result in a longer period of time before customers receive notification of a breach, thereby decreasing the benefits of such notification,[954] it might also reduce the number of unnecessary notifications to covered institutions and, in turn, to customers.[955]

The final amendments provide, as proposed, that a covered institution may enter into a written agreement with a service provider to notify individuals affected by a breach on the covered institution's behalf.[956] Some commenters supported this proposed requirement.[957] We expect that this provision could reduce the compliance costs of the amendments, especially in the case where the breach happens at the service provider. In this case, the service provider may be in a better position to collect the relevant information and provide the required notice to customers.[958]

---

952 Alignment with existing regulation makes it more likely that service providers already have policies and procedures in place to comply with this requirement.

953 *See, e.g.*, STA Comment Letter 2.

954 *See supra* section IV.D.1.b(2) for a discussion of the benefits of a timely notice to customers.

955 *See* Microsoft Comment Letter ("Premature reporting according to a 48-hour or shorter deadline, in our experience, increases the likelihood of reporting inaccurate or incomplete information, which is of little-to-no value and tends to create confusion and uncertainty."). *See also supra* section IV.D.1.b(4) for a discussion of the effects of unnecessary notification. We expect that the change made to the notification timing requirements for service providers will mitigate these effects.

956 *See* final rule 248.30(a)(5)(ii).

957 *See* Schulte Comment Letter ("Covered Institutions should be permitted to reach commercial agreements that delegate notice obligations to service providers, as long as the notice actually provided to customers with potentially impacted data satisfies the Covered Institution's notice obligations."); ICI Comment Letter 1 ("We also concur with the Commission that covered institutions should be permitted to have their service providers send breach notices to affected individuals on behalf of the covered institution.").

958 One commenter stated that "if the service provider was the victim of a cyber attack that included unauthorized access to Covered Institution sensitive customer information, then the service provider would be better situated to notify the affected customers." *See* Schulte Comment Letter. Even when the service provider notifies customers directly, the obligation to ensure that the affected individuals are notified rests with the covered institution. *See supra* section II.A.4 and final rule 248.30(a)(5)(iii).

It is possible that a breach that will trigger a notification obligation might occur at a covered institution that will also be a service provider to another covered institution.[959] The final amendments provide that the obligation to ensure that affected individuals are notified rests with the covered institution where the breach occurred.[960] If this covered institution is also a service provider to another covered institution, it retains the obligation, as a service provider, to notify this other covered institution of the breach.[961] This will allow the other covered institution to initiate its own incident response program and to perform its oversight duties on its service providers, and contribute to enhance the protection of customer information. We modified the final amendments such that only one covered institution needs to notify the affected customers.[962] By requiring only one notice to be sent for a given incident, this modification will reduce compliance costs—since only one covered institution will have to devote resources to preparing and sending the notice—and reduce potential confusion for the affected customers.[963] We do not expect this modification to reduce the benefit for such customers, who will still receive a timely notice.

---

959 For additional discussions of the cases where multiple covered institutions are involved in the same incident, *see supra* section II.A.3.a and *infra* section IV.D.2.a.

960 The amendments allow the two covered institutions to coordinate with each other as to which institution will send the notice to the affected individuals. *See supra* section II.A.3.a.

961 Because this service provider is itself a covered institution, it will have appropriate policies and procedures in place. Hence, we do not expect that notifying the other covered institution will imply significant costs.

962 *See supra* section II.A.3.a. Some commenters stated that the proposed amendments could be interpreted to lead to duplicative notices. *See, e.g.*, CAI Comment Letter ("This dynamic could also create duplicative notification obligations where there is unauthorized access to sensitive customer information that is held or maintained by one financial institution on behalf of another, since proposed Rule 30 [sic – rule 248.30] notification obligations would appear to apply to both financial institutions simultaneously even though only one set of customer information was accessed."). The revisions specify that only one notification is required in that circumstance.

963 Duplicative notices may nevertheless happen as a result of different requirements from other existing regulations. *See supra* section IV.C.2.a(3).

2. Extending the Scope of the Safeguards Rule and the Disposal Rule

a. Definition of Customer Information

The final amendments more closely align the scope of the safeguards rule with the scope of the disposal rule. They also broaden the scope of information covered by the rules to all customer information, regardless of whether the customers are a covered institution's own, or those of another financial institution whose customer information has been provided to the covered institution.[964] The final amendments define customer information, for any covered institution other than a transfer agent, as "any record containing nonpublic personal information" about a customer of a financial institution, whether in paper, electronic or other form, that is in the possession of a covered institution or that is handled or maintained by the covered institution or on its behalf. Such information is customer information regardless of whether it pertains to (a) individuals with whom the covered institution has a customer relationship or (b) the customers of other financial institutions where such information has been provided to the covered institution.[965] For transfer agents, customer information is defined as 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."[966]

While some commenters supported the proposed scope of the rules regarding the definition of customer information,[967] one commenter stated that the rule should focus on sensitive customer information, and that the breadth of the proposed amendments was

---

964 *See supra* section II.A.3.a.

965 Final rule 248.30(d)(5)(i).

966 Final rule 248.30(d)(5)(ii).

967 *See, e.g.*, EPIC Comment Letter; Better Markets Comment Letter.

disproportionate to the risks of disclosure.[968] This commenter also stated that applying the service provider requirements to all service providers that have access to any customer information would be disproportionate to the benefits and risk presented and suggested that it apply only to service providers with access to sensitive customer information.[969]

We acknowledge that applying the policies and procedures requirements to all customer information will impose costs that would not be incurred if the amendments covered only sensitive customer information. However, this approach creates important benefits. For example, the disclosure of customer information could be used for phishing attacks or similar efforts to access sensitive customer information. Moreover, with respect to policies and procedures specifically, the costs of creating policies and procedures for all information should not be much larger than the cost of creating them for only sensitive customer information, because the cost is in the creation of the policies and procedures rather than in their application. We acknowledge, however, that in some organizations the sensitive customer information could be located in different systems or accessible to different employees, such that policies and procedures for non-sensitive information would be different. In addition, covered institutions' existing policies and procedures may be less likely to meet the new requirements as a result of the breadth of the definition and would thus require modifications.

Because the final amendments extend the scope of customer information subject to protection to information possessed by a covered institution regardless of whether the customers are a covered institution's own, or those of another financial institution whose customer information has been provided to the covered institution, the benefits of the final amendments

---

968 *See* IAA Comment Letter 1.

969 *See* IAA Comment Letter 1.

will extend 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.[970] We anticipate that, in many instances, the preventative measures taken by covered institutions to safeguard customer information in response to the final amendments will generally also protect these additional individuals.[971] Hence, while we expect that these measures could have potential significant benefits for these additional individuals, we do not expect them to result in significant additional costs for the covered institutions. 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. Regarding the measures taken by covered institutions to comply with the final amendments' incident response program requirements, following a data breach, we do not anticipate that extending the scope of information covered by the final amendments to include these additional individuals will have a significant effect. These costs will include additional reputational harm and litigation as well as increased notice delivery costs. However, 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 notification of data breaches to these additional individuals.

---

970 *See* final rule 248.30(d)(5).

971 For example, measures aimed at strengthening information safeguards such as improved user access control or staff training will likely protect a covered institution's customer information systems regardless of whether they house the information of the covered institution's own customers or those of another financial institution.

Some commenters agreed that covered institutions should safeguard the customer information they receive from other financial institutions.[972] Other commenters disagreed with the proposed requirement that a covered institution would have to notify individuals whose sensitive customer information was compromised even when these individuals were not the covered institution's customers.[973] Some commenters stated that it would be impractical for covered institutions to identify and contact such individuals, or that it could confuse these individuals.[974] However, such individuals will benefit from their information being included in the scope of the amendments' requirements. Another commenter stated that this provision of the requirement could lead to duplicative notification obligations if the two financial institutions involved—that is, the institution that received the information and the institution that provided the information—were both covered institutions.[975] After considering comments, we have modified the amendments to avoid requiring that multiple covered institutions notify the same affected individuals for a given incident.[976] The final amendments require that when an incident occurs at a covered institution or at one of its service providers that is not itself a covered institution, the covered institution has the obligation to ensure that a notice is provided to affected individuals, regardless of whether this covered institution has a customer relationship with the individuals. If this covered institution received the customer information from another covered institution, the two covered institutions can coordinate with each other to decide who

---

972 *See, e.g.*, ICI Comment Letter 1; Better Markets Comment Letter.

973 *See, e.g.*, SIFMA Comment Letter 2; CAI Comment Letter.

974 *See* ACLI Comment Letter; SIFMA Comment Letter 2; Federated Comment Letter.

975 *See* CAI Comment Letter.

976 *See* final rule 248.30(a)(4); *see also supra* sections II.A.3.a and IV.D.1.c.

will send the notice. As discussed above,[977] we expect that this modification will reduce compliance costs without reducing the benefits of the final amendments.

b. Extension to Cover All Transfer Agents

The final amendments extend both the safeguards rule and the disposal rule to apply to any transfer agent registered with the Commission or another appropriate regulatory agency. Before this adoption, the safeguards rule did not apply to any transfer agents, and the disposal rule only applied to transfer agents registered with the Commission.[978] In addition to requiring transfer agents to design an incident response program, the benefits and costs of which are discussed separately above,[979] the amendments 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.[980] Moreover, the final amendments create an obligation on transfer agents registered with a regulatory agency other than the Commission to develop, implement, and maintain written policies and procedures that address the proper disposal of customer information.[981]

As discussed in sections II.B.2 and IV.C.3.e, 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.

---

977 *See supra* section IV.D.1.c.

978 *See supra* section II.B.2.

979 *See supra* section IV.D.

980 *See* final rule 248.30(a).

981 *See* 17 CFR 248.30(a).

investing public.[982] Given the highly concentrated nature of the transfer agent market,[983] a general failure of customer information safeguards at a transfer agent could negatively impact large numbers of customers.[984]

One commenter stated that because transfer agents' customers are not the individuals whose information they hold but the issuers of securities, the proposed amendments were ill-fitting, which decreased their efficacy and increased their complications.[985] This commenter also stated that the proposed amendments were not well-suited for transfer agents, and that this highlighted the need for a more in-depth analysis of how the final amendments may impact transfer agents, their customers (the issuers of securities), and securityholders.[986] In response to this commenter, we have supplemented below the analysis of the benefits and costs of extending the scope of Regulation S-P to transfer agents.[987]

The final amendments extend the scope of the safeguards rule to cover any transfer agent registered with the Commission or another appropriate regulatory agency. As discussed above,[988] the safeguards rule requires covered institutions to develop written policies and procedures, including a response program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification

---

982 One commenter disagreed with this notion, stating that many transfer agents do not have the type or scope of personal information which could lead to further complications for shareholders. *See* STA Comment Letter 2. Transfer agents that do not possess customer information as defined in final rule 248.30(d)(5) will not be covered by the amendments and as such will not be subject to its associated costs.

983 *See supra* section IV.C.3.e.

984 More than 40% of registered transfer agents maintain records for more than 10,000 individual accounts. *See supra* Figure 8.

985 *See* STA Comment Letter 2.

986 *See* STA Comment Letter 2.

987 Additional context is provided in section IV.C.3.f. *See also supra* section II.B.2 for a discussion of why the amendments are appropriate for transfer agents.

988 *See supra* section IV.D.1.

procedures. The benefits and costs of the response program, as detailed above,[989] will also apply to transfer agents. Additionally, because transfer agents may be considered service providers under state law, or may maintain but not own or license customer information data, they are likely to be required by state law to notify the entity that owns or licenses the data (the issuer of the securities), which in turn could be required to notify the affected individuals (the holders of the securities).[990] Hence, it is possible that the final amendments will result in two notices being sent for the same incident—one by the issuer of the securities, as required by state law, and one by the issuer's transfer agent, as required by the final amendments.

Some commenters stated that a second notification would have negative consequences for customers without providing any benefits.[991] One commenter stated that the proposed requirements would not provide shareholders with helpful, new information but rather that two different notices, from two different entities, concerning the same breach would likely result in shareholder confusion.[992] Another commenter added that this second notice could potentially result in confusion, questions, and unnecessary costs to the transfer agent and the issuer.[993]

We disagree that no helpful, new information will be provided to the affected customers. In the situation where state law requires a notification from the issuer and the final amendments require a notification from the transfer agent as a covered institution, the final amendments will help ensure that the individuals whose information has been breached receive an informative and

---

989 *See supra* section IV.D.1.a; *see also infra* footnote 1003 and accompanying text for a discussion on additional costs for transfer agents.

990 *See supra* section IV.C.2.a(3).

991 *See, e.g.*, STA Comment Letter 2.

992 *See* STA Comment Letter 2.

993 *See* Computershare Comment Letter.

timely notice, with the benefits over the baseline described above.[994] Securityholders will benefit by potentially receiving additional and more timely information on a given breach.[995] In addition, in response to commenters' concerns, we have modified the final amendments such that, for the cases where multiple notifying entities are covered institutions, only one notice needs to be sent to satisfy the amendments' requirements.[996] Furthermore, some states allow for the entity that is the victim of a breach, but does not own or license the data, to notify individuals directly.[997] Hence, we expect that in some instances, the notice required by the final amendments will satisfy the state law requirements and only one notice will be sent. In these instances, additional costs related to the second notice will be avoided. For the instances where two notices will nevertheless be sent, we acknowledge that a second notification will impose costs on the transfer agent or its customer the issuer. As discussed below, we estimate that certain costs associated with the preparation and distribution of notices will be, on average, $5,178 per year per covered institution.[998] We understand it is possible that, in some cases, customers may be confused when receiving a notice from an entity they do not recognize and may read the notification as a phishing attempt or another nefarious scheme. However, we do not expect that a second notice will impose significant costs on the affected customers, and we expect that this confusion will be

---

994 *See supra* section IV.D.1.b.

995 *See supra* section IV.D.1.b. Commenters stated that issuers may already have adopted policies and procedures to adhere to the strictest standards thereby already notifying securityholders consistent with the proposed amendments. *See* Computershare Comment Letter; STA Comment Letter 2. We acknowledge that this may be the case.

996 *See supra* sections IV.D.1.c and IV.D.2.a for additional discussions of the case where two covered institutions are involved in the same incident.

997 *See, e.g.*, Wyo. Stat. § 40-12-502(g) ("The person who maintains the data on behalf of another business entity and the business entity on whose behalf the data is maintained may agree which person or entity will provide any required notice as provided in subsection (a) of this section, provided only a single notice for each breach of the security of the system shall be required."). *See also supra* section IV.C.2.a(3).

998 This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $3,862 per year per covered institution. *See infra* section V.

mitigated by the content of the notice. As discussed in section IV.D.1.b(5), the notice is required to include a description of the incident in general terms. We expect that this description will help explain the situation in the case where customers do not have a direct relationship with the transfer agent sending the notice and, therefore, that it will reduce potential customer confusion from duplicative notification, as discussed above.[999]

Before this adoption, transfer agents that are registered with the Commission were not required to notify customers directly in case of a breach under Federal law.[1000] As discussed above, we also expect that, under state law, transfer agents are likely to be considered service providers (or entities that use or maintain but do not own or license data) and as such are typically only required to notify the issuer of securities in case of breach.[1001] Hence, we expect that to satisfy the amendments' requirements, these transfer agents might need to design and implement a response program and notification procedures, which will require some resources.[1002] As discussed below, we estimate that certain costs associated with developing and implementing policies and procedures, which include the response program and notification procedures, to comply with the final amendments will be, on average, $17,950 per year per transfer agent.[1003] In addition, as for other types of covered institutions, if transfer agents respond

---

999 *See supra* section II.B.2.

1000 In 2023, there were 251 such transfer agents. *See supra* section IV.C.3.e.

1001 However, there are some states where transfer agents may be required by state law to notify the affected individuals directly. *See supra* footnote 574 and accompanying text.

1002 Transfer agents registered with the Commission may already have such procedures in place and may already be notifying customers. *See* ICI Comment Letter 1 ("We understand that this is a common practice today for investment companies wherein their transfer agents assume responsibility for sending affected customers breach notices."). However, we do not have data on how common such arrangements are and commenters did not provide such data.

1003 This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $5,425 per year per transfer agent. *See infra* section V. These estimated costs are higher than for other types of covered institutions because transfer agents were not, before this adoption, covered by the safeguards rule. In addition, transfer agents registered with a

to this requirement by improving their customer information safeguards beyond what is required by the final amendments, they will incur additional costs.[1004] We expect that the different costs resulting from the written policies and procedures requirement will be passed on to the transfer agents' customers (the issuers of securities) and ultimately to the holders of these securities.

Transfer agents that are registered with an appropriate regulatory agency other than the Commission may already be required to notify affected individuals in case of a breach under the Banking Agencies' Incident Response Guidance.[1005] As discussed above, although the notification requirement under the final amendments is largely aligned with the Banking Agencies' Incident Response Guidance, there are some differences.[1006] Hence, for these institutions, we expect that the costs of the requirements will primarily be to review and, if needed, update their notification procedures to ensure consistency with the amendments, though there may be some costs associated with updating procedures to achieve consistency with the final amendments.[1007] As discussed below, we estimate that certain costs associated with

---

regulatory agency other than the Commission were not, before this adoption, covered by the disposal rule. The final amendments extend both the safeguards rule and the disposal rule to apply to any transfer agent registered with the Commission or another appropriate regulatory agency. The additional costs that could be incurred by transfer agents as a result are discussed below. *See infra* text accompanying footnote 1021.

1004 We are unable to quantify expected costs resulting from such enhancements. *See supra* footnote 717 and accompanying text.

1005 In 2023, there were 64 such transfer agents; *see supra* section IV.C.3.e; *see also supra* section IV.C.2.b.

1006 For example, the Banking Agencies' Incident Response Guidance requires entities to notify customers "as soon as possible," but does not specify a precise deadline, whereas the final amendments require that the notice be sent as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of sensitive customer information has occurred or is reasonably likely to have occurred. In addition, the Banking Agencies' Incident Response Guidance has a different definition of "sensitive customer information" and has different requirements regarding an entity's service providers. *See supra* section IV.C.2.b for a description of the Banking Agencies' Incident Response Guidance's requirements.

1007 We expect these reviews and updates will result in the entities incurring costs generally smaller than the costs of adopting and implementing new policies and procedures, as discussed in Section V.

developing and implementing policies and procedures to comply with the final amendments will be, on average, $17,950 per year per transfer agent.[1008]

One commenter supported the proposed inclusion of transfer agents in the safeguards rule, stating that it would eliminate the asymmetry between the transfer agents registered with the Commission and those registered with another regulatory agency and that it would promote investor protection, regulatory parity, and fair competition among firms.[1009] We agree with this commenter. Another commenter stated that expanding the regulation's scope to include transfer agents was long overdue.[1010]

Other commenters opposed the proposed inclusion.[1011] One commenter stated that requiring transfer agents to notify customers directly would create undue costs for transfer agents, that the proposed amendments included a potential for conflicting regulations where there are overlapping state and federal regulations, and that this would lead to unnecessary expenses as transfer agents attempt to develop policies and procedures capable of addressing these potentially conflicting regulations.[1012] This commenter suggested that the Commission either preempt state law or prepare and produce a cost-benefit analysis identifying the specific ways in which the amendments would be an improvement over existing regulations.[1013] Another commenter—a transfer agent—stated that it already had policies and procedures to notify issuers

---

1008 This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $5,425 per year per transfer agent. *See infra* section V.

1009 *See* Better Markets Comment Letter.

1010 *See* ICI Comment Letter 1.

1011 *See* STA Comment Letter 2; Computershare Comment Letter.

1012 *See* STA Comment Letter 2. The commenter did not describe such conflicts.

1013 *See* STA Comment Letter 2.

of securities in accordance with state law and that notifying the securityholders directly could violate some of its existing contracts with issuers.[1014]

In response to commenters and as discussed above,[1015] we have modified the final amendments to minimize the likelihood of multiple notices being sent for the same incident, which will decrease compliance costs.[1016] The final amendments do not necessarily require covered institutions to notify affected customers directly in case of breach, but instead provide that a covered institution must ensure that the required notice is sent.[1017] Hence, if a transfer agent has a contract with an issuer that prevents it from notifying securityholders directly, the transfer agent will be able to, under the final amendments, enter into an agreement with the issuer so that the issuer sends the notice on its behalf.[1018] In consideration of the commenter's request for an analysis that considers the incremental effects of the rule over existing regulations, we have (i) conducted supplemental analyses of the baseline regarding state law requirements,[1019] and (ii) supplemented the analysis of the benefits and costs of the final amendments over this

---

1014 *See* Computershare Comment Letter ("However, as state breach notification laws have been in effect for nearly two decades, Computershare has long-standing policies and procedures for notification, and contractual obligations to clients that are designed to track state law requirements. Such contract provisions may specifically prohibit Computershare as the transfer agent from notifying securityholders as the issuers have the requirement to notify their securityholders under state law.").

1015 *See supra* section IV.D.

1016 *See also supra* section II.B.2 for a discussion of how the final amendments permit transfer agents and issuers to develop arrangements to address potentially conflicting regulations.

1017 *See* final rule 248.30(a)(4).

1018 Such contract renegotiation will involve some costs for the transfer agents. It is difficult for us to quantify these costs, as we have no data on the provisions of existing contracts between transfer agents and security issuers relating to customer notification of data breaches, and no commenter suggested such data. Such costs are likely to be contract specific, as they will depend on the degree to which each existing contract may be revised as a result of the final amendments. Many such contracts may not be revised at all, while others may undergo more revisions. Moreover, in many cases, even where a contract could be revised as a means of complying with the final requirements, the covered institution may pursue compliance by other means.

1019 *See supra* section IV.C.2.

baseline, highlighting the different areas where the final amendments will improve over existing regulations.[1020]

The final amendments to the safeguards rule also require transfer agents to develop, implement, and maintain written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information.[1021] In general, transfer agents with written policies and procedures to safeguard customer information would be at reduced risk of experiencing such safeguard failures.[1022] Because some state laws require written policies and procedures to protect customer information,[1023] and because transfer agents, by the nature of their business models, are likely to hold information about individuals residing in a large number of states, we expect that most transfer agents already have policies and procedures in place.[1024] In addition, transfer agents registered with a regulatory agency other than the Commission may also be subject to the Banking Agencies' Safeguards Guidance or other Federal regulation.[1025] Hence, we expect the costs of this requirement to be limited and to consist mostly of reviewing and updating existing policies and procedures to ensure consistency with the safeguards rule.[1026] As discussed below, we estimate that certain costs associated with developing and implementing

---

1020 *See supra* section IV.D.1.b.

1021 *See* final rule 248.30(a)(1).

1022 *See supra* section IV.D.1 for a discussion of the benefits of written policies and procedures generally.

1023 *See supra* section IV.C.2.b.

1024 In addition, some transfer agents may also be subject to other regulations, such as the GDPR, and already have customer information safeguards in place as a result. *See supra* section IV.C.2.b.

1025 *See supra* footnote 604 and accompanying text.

1026 We expect these reviews and updates will result in the entities incurring costs generally smaller than the costs of adopting and implementing new policies and procedures, as discussed in section V.

policies and procedures to comply with the final amendments will be, on average, $17,950 per year per transfer agent.[1027]

The final amendments extend the disposal rule to transfer agents registered with a regulatory agency other than the Commission.[1028] The amendments require these transfer agents to properly dispose of customer information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.[1029] Because these transfer agents are subject to regulatory requirements and to state laws which require proper disposal of customer information,[1030] we expect that they are likely to already have procedures in place for the disposal of customer information. Therefore, to the extent that transfer agents already have in place procedures that are consistent with these provisions of the final amendments, the benefits and costs relating to this requirement will be reduced for these institutions and for the customers whose information is covered by this requirement. Hence, we expect the costs of this requirement to be limited and to consist mostly of reviewing and updating existing policies and procedures to ensure consistency with the safeguards rule.[1031] As discussed below, we estimate that certain costs associated with developing and implementing policies and

---

1027 This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $5,425 per year per transfer agent. *See infra* section V. As discussed above, these estimates reflect all of the policies and procedures required by the final amendments, including those regarding the incident response program. *See supra* footnote 1003 and accompanying text.

1028 Transfer agents registered with the Commission were already subject to the disposal rule before this adoption. *See* 17 CFR 248.30(b).

1029 *See* 17 CFR 248.30(b).

1030 The Banking Agencies' Safeguards Guidance requires that a covered entity's information security program be designed to ensure the proper disposal of customer information and consumer information. *See supra* footnote 612 and accompanying text; *see also supra* section IV.C.2.b for a discussion of state law disposal requirements.

1031 We expect these reviews and updates will result in the entities incurring costs generally smaller than the costs of adopting and implementing new policies and procedures, as discussed in section V.

procedures to comply with the final amendments will be, on average, $17,950 per year per transfer agent.[1032]

3. Recordkeeping

The recordkeeping provisions of the final amendments require covered institutions (other than funding portals) to make and maintain written records documenting compliance with the requirements of the safeguards rule and of the disposal rule.[1033] Each covered institution (other than funding portals) is required to make and maintain written records documenting its compliance with, among other things: its written policies and procedures required under the final amendments, 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.[1034]

These recordkeeping requirements will help facilitate the Commission's inspection and enforcement capabilities. Covered institutions may react to this enhanced ability of the

---

[1032] This estimate is an annual average for the first three years. The corresponding ongoing annual costs beyond the first three years are estimated to be on average $5,425 per year per transfer agent. *See infra* section V. As discussed above, these estimates reflect all of the policies and procedures required by the final amendments, including those regarding the incident response program. *See supra* footnote 1003 and accompanying text.

[1033] *See* final rule 248.30(c). As discussed above, funding portals have recordkeeping requirements that are different from those of other covered institutions under the final amendments. *See supra* footnote 385.

[1034] *See* the various provisions of final rule 248.30(a) and 248.30(b)(2).

Commission staff to detect deficiencies and impose sanctions against non-compliance due to the recordkeeping requirements by taking more care to comply with the substance of the amendments, which may result in material improvement in the response capabilities of covered institutions and mitigate potential harm resulting from the lack of an adequate response program. As such, the amendments' recordkeeping requirements might benefit customers through channels described in section IV.D.1.

One commenter supported the proposed recordkeeping requirements.[1035] Another commenter requested a clarification of the proposed requirements, suggesting that the text in the final amendments include more detail.[1036] In response to this commenter, we have provided a more detailed description of the requirements in the rule text of the final amendments.[1037] We expect that this change will mitigate compliance costs for covered institutions.

We do not expect the final 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 that covered institutions will need to invest in new recordkeeping staff, systems, or procedures to satisfy the new recordkeeping requirements.[1038] The incremental administrative costs arising from maintaining additional records related to these provisions using existing systems are covered in

---

1035 *See* ICI Comment Letter 1.

1036 *See* IAA Comment Letter 1.

1037 *See supra* section II.C and final rule 240.30(d)(1).

1038 *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. *See*, *e.g.*, 17 CFR 275.204-2(e)(2).

the Paperwork Reduction Act analysis in section V and are estimated to be $420 per year per covered institution other than funding portals, and $630 per year per funding portal.[1039]

4. Exception from Annual Notice Delivery Requirement

The final amendments 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.[1040] An institution may rely on the exception to forgo notice 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.[1041] The effect of the exception is to eliminate the requirement to send the same privacy policy notice to customers on multiple occasions. As such notices would provide no new information, receiving multiple copies of such notices is unlikely to provide 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.[1042] At the same time, reliance on the exception will reduce costs for covered institutions. However, we expect these cost savings to be limited to the administrative burdens discussed in section V.[1043] We received one comment supporting the proposed exception.[1044] We

---

1039 *See infra* section V. As discussed above, funding portals have recordkeeping requirements that are different from those of other types of covered institutions. *See supra* footnote 385.

1040 *See supra* section II.D; *see also* 15 U.S.C. 6803(f). Additionally, under existing statutory exceptions notice is not required when the institution provides certain information to a third party to perform services for or functions on behalf of the institution, such as information sharing necessary to perform transactions on behalf of the customer, information sharing directed by the customer, or reporting to credit reporting agencies. *See* 15 U.S.C. 6802(e).

1041 *See* final rule 248.5(e)(1)(ii).

1042 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.

1043 *See infra* footnote 1119.

1044 *See* ICI Comment Letter 1.

did not receive any comments suggesting alternatives to the proposed exception or suggesting that we not proceed with it.

Because the exception became effective when the statute was enacted, the aforementioned benefits are likely to have already been realized. Consequently, we do not expect that its inclusion will have any economic effects relative to the current status quo.

E. Effects on Efficiency, Competition, and Capital Formation

As discussed above, market imperfections might lead to underinvestment in customer information safeguards, and to information asymmetry about incidents resulting in unauthorized access to or use of customer information.[1045] This information asymmetry might prevent customers whose sensitive information was compromised from taking timely mitigating actions. The final amendments aim to mitigate the inefficiency resulting from these imperfections by imposing mandates for policies and procedures. Specifically, the amendments require covered institutions to include a response program for incidents involving unauthorized access to or use of customer information. This response program must address assessment and containment of such incidents, and might thereby reduce potential underinvestment in these areas, improving customer information safeguards as a result.[1046] In addition, by requiring notification to customers about certain safeguard failures, the amendments could reduce the aforementioned information asymmetry and help customers choose a covered institution that meets their needs or preferences. The notification requirement, by imposing reputational costs on institutions whose safeguards of customer information fail, might also provide covered institutions with greater

---

[1045] *See supra* section IV.B.

[1046] *See supra* section IV.D (discussing the benefits and costs of the response program requirements).

incentives to improve their safeguards, contributing to lowering the probability of a breach even further.

While the amendments have the potential to mitigate these inefficiencies, the scale of the overall effect is difficult to estimate. Due to the presence of existing regulations, including state notification laws, and existing security practices,[1047] these inefficiencies are likely to be of limited magnitude. However, to the extent that they remain, the amendments might contribute to reduce them.[1048] 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 impracticable to quantify due to data limitations discussed previously.[1049]

The final provisions will 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 final amendments are unlikely to lead to significant effects on capital formation.[1050]

Because the amendments are likely to impose proportionately larger direct and indirect costs on smaller and more geographically limited covered institutions, these institutions' competitiveness vis-à-vis their larger peers might be affected. Such covered institutions—which

---

1047 *See supra* sections IV.C.1 and IV.C.2.

1048 Section IV.D.1.b discusses in detail how the amendments' requirements differ from existing state notification laws.

1049 *See, e.g.*, *supra* sections IV.A. and IV.D.1.

1050 While we do not expect first-order effects on capital formation, we agree with one commenter who stated that the amendments would contribute to promote transparency and consistency on capital markets, which would benefit investors, issuers, and other market participants. *See* Nasdaq Comment Letter. In addition, as discussed below, there might be incremental effects on the capital formation associated with issuers relying on funding portals. *See infra* text accompanying footnote 1053.

may be less likely to have written policies and procedures for incident response programs already in place—will face disproportionately higher costs resulting from the proposed amendments.[1051] Thus, the amendments might have negative effects on competition, to the extent these higher costs represent a barrier to entry or limit smaller institutions' viability as a competitive alternative to larger institutions. 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 adoption will significantly alter these challenges and therefore expect the incremental effects of these amendments on competition to be limited.

On the other hand, the amendments may have positive competitive effects also. Because safeguarding customer information, including through cybersecurity, is disproportionately more expensive for smaller institutions,[1052] customers today may already suspect that smaller institutions have more severe under-investments in cybersecurity than larger institutions and may therefore avoid smaller institutions. If disproportionately large costs faced by smaller institutions cause existing and potential customers to suspect that these institutions are more likely to avoid such costs, the existing information asymmetry may be greater for these institutions. Smaller institutions may be unable to overcome these suspicions on their own absent regulatory policy, and so asymmetries of information may represent a barrier to entry for smaller institutions. In this case, if the amendments result in customers having better information on the covered institutions' efforts towards protecting customer information, there will be a positive effect on

---

1051 The development of policies and procedures entails a fixed cost component that imposes a proportionately larger burden on smaller firms. We expect smaller broker-dealers and investment advisers will be most affected. *See supra* sections IV.C.3.a and IV.C.3.c.

1052 *See, e.g.*, Anna Cartwright et al., *Cascading Information On Best Practice: Cyber Security Risk Management in UK Micro and Small Businesses and the Role of IT Companies*, COMPUTERS & SECURITY 131 (2023) for a list of articles discussing the cybersecurity challenges faced by small businesses.

competition. Hence, the overall effect on smaller and more geographically limited covered institutions' competitiveness remains difficult to predict.

With respect to funding portals, the situation could be different. As discussed above, the final amendments are likely to impose proportionately larger costs on smaller covered institutions,[1053] including smaller funding portals. At the margin, it is possible that the final amendments will result in a smaller number of funding portals, which could result in a smaller number of crowdfunding intermediaries available to potential issuers. Crowdfunding intermediaries facilitate capital raising by smaller issuers relying upon Regulation Crowdfunding to offer or sell securities. To the extent that the final amendments result in a decrease in the availability of funding portals or in an increase in the costs of utilizing crowdfunding intermediaries for issuers or investors, they may have incremental negative effects on capital formation associated with issuers relying on such intermediaries. However, we expect the incremental negative effect on competition that could result from this to be mitigated by the already significant degree of concentration among crowdfunding intermediaries observed today.[1054] We further expect these effects to be mitigated to the extent that issuers may be able to switch to using other intermediaries for their Regulation Crowdfunding offerings, such as larger funding portals. Lastly, the amendments may have a positive effect on capital formation in offerings under Regulation Crowdfunding to the extent that the additional procedural requirements in the final amendments increase protection of customer information and thereby attract additional potential investors. Hence, the overall effect remains difficult to predict.

1053 *See supra* footnote 1051.

1054 *See supra* section IV.C.3.b.

Two commenters raised concerns about barriers to entry disproportionately affecting smaller covered institutions. One commenter stated that smaller advisers had been significantly affected by "one-size-fits-all" regulations that effectively require substantial fixed investments in infrastructure, personnel, technology, and operations, adding that they were concerned that these stressors and barriers would negatively affect smaller advisers' ability to continue to serve their clients.[1055] Another commenter stated that we had done "little analysis" about the impact of recent proposals on small broker-dealers, competition within the brokerage industry, and whether the proposals could contribute to barriers for new entrants into the markets.[1056] We acknowledge these commenters' concerns about smaller covered institutions and, as discussed above, understand that smaller covered institutions might be disproportionately affected by the final amendments.[1057] In response to these concerns, we have changed the final amendments from the proposal. We expect that some of these changes may mitigate costs and may reduce, but not eliminate, the degree to which the final amendments act as a barrier to entry.[1058] We have also responded to commenters' concerns by adopting longer compliance periods for all covered institutions relative to the proposal and an even longer compliance period for smaller covered

---

1055 *See* IAA Comment Letter 1.

1056 *See* ASA Comment Letter. In the Proposing Release, we discussed that the compliance costs of the proposed amendments could be higher for smaller covered institutions such as small broker-dealers who do not have a national presence. *See* Proposing Release at section III.D.1.a. We also discussed the potential negative competitive effects of the proposed amendments on smaller covered institutions and requested comments on the way we characterized the effects on competition. *See* Proposing Release at sections III.F. and III.G. We received no comment letter discussing specifically how the proposed amendments would affect the level of competition in the different markets in which covered institutions operate.

1057 *See supra* footnote 1051 and accompanying text.

1058 These changes include (1) requiring that a service provider notify the affected covered institution of a breach in a period of 72 hours instead of 48 hours; and (2) requiring that covered institutions oversee, monitor, and conduct due diligence on their service providers to ensure that they take appropriate measures to protect customer information and notify the covered institution in case of breach instead of requiring written contracts. *See supra* section IV.D.1.c on the expected effects of these changes. Because smaller covered institutions are more likely to have limited bargaining power when negotiating with their service providers, we expect that these changes may particularly reduce the burdens on those entities and may reduce, but will not eliminate, the extent to which these requirements act as a barrier to entry.

institutions.[1059] The final amendments provide 24 months for smaller covered institutions to comply with the final amendments after the date of publication in the Federal Register, compared to 18 months for larger covered institutions.[1060] Since smaller covered institutions are those most likely to exit the market in response to high compliance costs, this longer compliance period will mitigate the negative effect of the final amendments on competition, for example by giving smaller covered institutions opportunities to learn about compliance with the final requirements from larger covered institutions' earlier compliance.[1061]

With respect to competition among transfer agents, the situation could be different. Because transfer agents registered with a regulatory agency other than the Commission may already have been required to notify customers in case of breach,[1062] whereas the transfer agents registered with the Commission may, before this adoption, have only been required, by state law, to notify the security issuer, the latter group may face disproportionately high compliance costs compared to the former group since they might have to design and implement new policies and procedures, including the required incident response program and notification procedures.[1063] This might affect their competitiveness vis-à-vis the transfer agents registered with a regulatory agency other than the Commission.[1064] Because transfer agents registered with the Commission

---

1059 The proposed compliance period was 12 months from effective date for all covered institutions. *See* Proposing Release at section II.I.

1060 *See supra* Table 3 for a description of small covered institutions for the purposes of the final amendments' tiered compliance period.

1061 *See* FSI Comment Letter ("We propose a longer implementation period for smaller broker-dealers and investments advisers to allow these firms to benefit from implementation for larger industry participants.").

1062 *See supra* section IV.C.2.b.

1063 In 2023, there were 251 transfer agents registered with the Commission and 64 transfer agents registered with another appropriate regulatory agency. *See supra* section IV.C.3.e.

1064 In addition, because designing and implementing new policies and procedures entails fixed costs, competition among transfer agents registered with the Commission may be affected. *See supra* discussion of potential competition effects on covered institutions of different sizes.

may already have procedures in place to notify individuals affected by a data breach,[1065] the magnitude of this effect is difficult to estimate.

One commenter supported the proposed extension of the scope of the safeguard and disposal rules to all transfer agents and stated that it would promote fair competition among these firms by reducing asymmetry in the requirements with which different types of transfer agents must comply.[1066] We agree with this commenter that including all transfer agents in the scope of both the safeguards rule and the disposal rule will contribute to enhanced competition in the market for transfer agents.[1067]

With respect to efficiency and competition among covered institutions' service providers, the overall effects of the final amendments are difficult to predict. The final amendments require covered institutions to ensure that their service providers protect against unauthorized access to or use of customer information and notify the covered institution in case of a breach. The final amendments also require covered institutions to oversee their service providers to ensure that these measures are enforced.[1068] As discussed above,[1069] we expect that most service providers will continue their relationships with covered institutions, but some service providers might not. We expect that four possible scenarios may happen:

1065 *See supra* footnote 1002. In addition, we expect that many transfer agents already have some processes in place to contact customers since communicating information from the issuer to its security-holders is one of the core functions of transfer agents.

1066 *See* Better Markets Comment Letter.

1067 In particular, applying the final amendments to all transfer agents may be beneficial for competition, to the extent that applying different regulations to different entities could exacerbate existing differences in the competitive landscape. *See supra* section IV.C.3.e (discussing that transfer agents registered with the Banking Agencies are on average smaller than transfer agents registered with the Commission).

1068 *See* final rule 248.30(a)(5).

1069 *See supra* section IV.D.1.c.

- Scenario 1: The service provider already has the processes and procedures in place to satisfy the covered institution's obligations under the final amendments and is willing to cooperate with the oversight activities of the covered institution.
- Scenario 2: The service provider does not have the necessary processes and procedures in place but is willing to adapt them to satisfy the covered institution's obligations under the final amendments and to cooperate with the oversight activities of the covered institution.
- Scenario 3: The service provider does not have the necessary processes and procedures in place and is not willing to adapt to satisfy the covered institution's obligation under the final amendments.[1070]
- Scenario 4: The service provider already has the processes and procedures in place to satisfy the covered institution's obligations under the final amendments but is not willing to cooperate with the oversight activities of the covered institution.

Under scenarios 1 and 2, the relationship between the covered institution and its service provider is maintained. Hence, we do not expect significant effects on efficiency and competition in these cases.[1071] On the other hand, scenarios 3 and 4 imply that the covered institution will have to either switch to a new service provider or perform the former service provider's functions in-house. If the covered institution is unable to find a new service provider that is equivalent in its ability to provide the services, this is likely to result in a second-best outcome

---

[1070] *See supra* section IV.C.3.f. Because taking the appropriate measures to satisfy the amendments' requirements entails fixed costs, we expect that smaller service providers are more likely to exit (or not enter) this market than larger service providers.

[1071] The other benefits and costs of these scenarios are discussed in section IV.D.1.c.

for the covered institution and therefore to result in a loss of efficiency.[1072] Scenario 4 could also lead to covered institutions being forced to switch away from large, established service providers and instead to rely on smaller, less established providers that may be less capable of addressing the vulnerabilities within its control. This situation could result in a reduced ability to protect customer information.

Commenters identified service providers exiting the market as a significant potential cost of the proposed requirements.[1073] We expect that the changes that we have made to the final amendments, including the change from a written contract requirement to a requirement to oversee service providers and the change to an extended notification deadline of 72 hours, will reduce the likelihood of scenario 4 by giving covered institutions more flexibility in how they choose to satisfy the service provider requirements of the final amendments.[1074] This will reduce the likelihood of this potential negative outcome. However, such an outcome is still possible and to the extent that it occurs, it will represent a cost of the final amendments.

1072 Under scenario 3, we expect this effect on efficiency to be limited since the service providers who are the most efficient at the outsourced function are likely to also be more effective at protecting customer information. We expect this effect to be more significant under scenario 4.

1073 *See* ACLI Comment Letter ("If service providers are unable or unwilling to change their practices, this requirement could cause regulated entities to end essential service provider arrangements with inadequate alternatives"); SIFMA Comment Letter 2 ("Indeed, some service providers may not agree to the contemplated new terms, which could limit the number of service providers that agree to such requirements, causing an undue reliance on a small group of service providers in the industry. Another possible result is that the least commercially savvy service providers would agree to these terms, which could increase unqualified providers working in the industry."); CAI Comment Letter ("In practice, this will often force covered institutions to choose between either using the best and most dependable service providers or complying with these regulatory requirements, since many leading service providers (such as cloud service providers) do not negotiate the standard terms of their services with customers and those standard terms generally would not meet the proposed contractual requirements.").

1074 *See supra* section II.A.4. In addition, some commenters mentioned costs associated specifically with written contracts. *See, e.g.*, ASA Comment Letter; IAA Comment Letter 1. These contracting costs could also apply to service providers and potentially result in these service providers terminating their relationship with covered institutions.

Because scenarios 3 and 4 result in service providers exiting the market, they also have effects on competition. While scenario 3 would result in an overall decrease in the number of service providers available to covered institutions, it would not necessarily reduce competition among service providers who are able and willing to satisfy covered institutions' requirements. In fact, the final amendments will prevent service providers that are not willing to satisfy the minimum requirements from operating in that market and from potentially undercutting service providers who do satisfy the requirements. This will improve the competitiveness of the service providers who are able and willing to satisfy the requirements. The situation is different for scenario 4, which would result in a decrease in the number of service providers with adequate customer information safeguards and notification procedures. This would result in a decrease in competition, and this is a potential cost of the regulation.

One commenter stated that the proposed amendments could lead to service providers not agreeing with the new requirements, adding that it could result in covered institutions relying on a small group of service providers in the industry.[1075] This commenter also stated that some service providers may choose not to enter into agreements with covered institutions as a result of the proposed amendments.[1076] We acknowledge that this is a risk of the final amendments. However, we expect that the modifications that we have made to the service provider provisions of the final amendments will reduce the costs to service providers of satisfying covered institutions' requirements,[1077] and might therefore reduce the likelihood of this potential negative outcome.

1075 *See* SIFMA Comment Letter 2.

1076 *See id.*

1077 *See supra* section IV.D.1.c.

Because of the reasons described above,[1078] we are unable to estimate the likelihood of the different scenarios and, therefore, we are unable to quantify the efficiency and competition effects of the service provider provisions of the final amendments.

Some commenters requested that the Commission consider interactions between the effects of the proposed rule and other recent Commission rules, as well as practical realities such as implementation timelines.[1079] As discussed above, the Commission acknowledges that overlapping compliance periods may in some cases increase costs, particularly for smaller entities with more limited compliance resources.[1080] This effect can negatively impact competition because these entities may be less able to absorb or pass on these additional costs, making it difficult for them to remain in business or compete. We acknowledge that to the extent overlap occurs, there could be costs that could affect competition. However, we do not expect these costs to be significant, for two reasons. First, the final amendments mitigate overall costs relative to the proposal,[1081] including by adopting longer compliance periods for all covered institutions, and an even longer compliance period for smaller covered institutions because they may have more limited compliance resources. The final amendments also reduce costs for both larger and smaller entities, relative to the proposal, notably by removing the proposed requirement to have a written contract with service providers. Thus, any higher costs or potential negative effects on competition due to overlapping compliance periods raised in the context of the proposal may be mitigated under the final amendments. Second, as explained in section IV.D, many of the rules commenters named affect limited sets of covered institutions, and the

---

1078 *See id*.

1079 *See supra* section IV.C.

1080 *See supra* section IV.D.

1081 *See supra* section IV.B.

compliance dates are generally spread out over a more than three-year period, including several that precede the compliance dates of the final amendments. These factors will limit the incidence of covered institutions affected by overlapping compliance dates.

Additionally, we anticipate that neither the recordkeeping provisions nor the exception from annual privacy notice delivery requirements will have a notable impact on efficiency, competition, or capital formation due to their limited economic effects.[1082] As discussed elsewhere, we do not expect the recordkeeping requirements to impose material compliance costs, and we therefore expect the economic effects of the exception to be limited. And, as the economic effects of the recordkeeping provisions are limited, any overlapping compliance dates involving recordkeeping will likewise have limited effect on competition.

F. Reasonable Alternatives Considered

In formulating the final amendments, we have considered various reasonable alternatives. These alternatives are discussed below.

1. Reasonable Assurances from Service Providers

Rather than requiring the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers to ensure service providers take appropriate measures to protect against unauthorized access to or use of customer information and provide notification to the covered institution if a breach of security occurs,[1083] the Commission considered requiring covered institutions to obtain "reasonable assurances" from service

---

[1082] *See* final rule 248.30(c) and final rule 248.5; *see also supra* sections IV.D.3 and IV.D.4.

[1083] *See* final rule 248.30(a)(5)(i).

providers instead. One commenter supported this alternative for some service providers.[1084] This alternative requirement would be a lower threshold than the final provisions requiring the establishment, maintenance, and enforcement of written policies and procedures designed to require oversight, and as such would be less costly to reach but also less protective for customers.

Under this alternative we would have used the final amendments' definition of "service provider," which is "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution."[1085] Thus, similar to the final amendments, 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.[1086] 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.

For those service providers that provide specialized services aimed at covered institutions, this alternative would, like the final amendments, create market pressure to enhance service offerings so as to provide the requisite assurances and facilitate covered institutions'

1084 *See* SIFMA Comment letter 2. Other commenters also suggested alternative thresholds that would be lower than the final amendments' provisions. *See, e.g.*, IAA Comment Letter 1; AWS Comment Letter.

1085 Final rule 248.30(d)(10).

1086 *See, e.g.,* Cal. Civil Code § 1798.81.5(b) and 1798.82(b); N.Y. Gen. Bus. Law § 899-AA(3).

compliance with the requirements.[1087] These service providers might 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 final amendments 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 final amendments, we generally anticipate that such costs would largely be passed on to covered institutions and ultimately their customers. As compared to the final amendments' requirements, we expect that "reasonable assurances" would in many cases require fewer changes to business processes and, accordingly, lower costs.[1088] However, this alternative—without more—could also be less protective than the final amendments.

With respect to service providers providing services aimed at a broad range of institutions (e.g., email, or customer-relationship management), the situation could be different. For these providers, covered institutions are likely to represent a small fraction of their customer base. As under the final service provider provisions, these 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.[1089] Some may be unwilling to make the assurances needed, although we anticipate that they would be generally more willing to make assurances than to participate in the

---

1087 A service provider involved in any business-critical function likely "receives, maintains, processes, or otherwise is permitted access to customer information." *See* final rule 248.30(d)(10).

1088 *See supra* section II.A.4 for a discussion of sufficient safeguards for ensuring compliance with covered institution's obligations under the final amendments.

1089 *See supra* section IV.D.1.c (discussing the final requirement for covered institutions to require policies and procedures reasonably designed to oversee, monitor, and conduct due diligence on service providers).

covered institutions' oversight activities.[1090] 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 final 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 some service providers. And, as outlined above, this alternative would be less protective than the final amendments' requirements.

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 adopted 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. One commenter suggested that the final amendments require notification when the unauthorized access to or use of sensitive customer information was "reasonably possible" instead of "reasonably likely."[1091] 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 IV.D.1.b, they would also increase the number

---

1090 *See id.* Additionally, the service provider's standard terms and conditions might in some situations provide reasonable assurances adequate to meet the requirement.

1091 *See* NASAA Comment Letter. In addition, another commenter suggested requiring customer notification 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. *See* Better Markets Comment Letter.

of false alarms. 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.[1092] Of more economic significance to covered institutions would be the resulting reputational effects.[1093] However, the direction of these effects is difficult to predict. On the one hand, increased notices resulting from a lower threshold can be expected to lead to additional reputational costs for firms required to issue more of such notices. On the other hand, lower thresholds could result in customers receiving a large number of notices. In this case, notices could become no longer notable, likely leading to the negative reputation effects associated with such notices being reduced.

3. Encryption Safe Harbor

The Commission considered including a safe harbor to the notification requirement for breaches in which only encrypted information was compromised. Several commenters supported an encryption safe harbor.[1094] An encryption safe harbor would also align with many existing state laws.[1095] Assuming that such an alternative safe harbor would be sufficiently circumscribed to prevent its application to insecure encryption algorithms, or to secure algorithms used in a manner as to render them insecure, the economic effects of its inclusion would be largely indistinguishable from the final amendments. This is because under the final amendments, notification is triggered by the "reasonable likelihood" that sensitive customer information was

---

1092 The direct compliance costs of notices are discussed in section V.

1093 *See supra* section IV.B.

1094 *See, e.g.*, SIFMA Comment Letter 2; AWS Comment Letter 1. *See also supra* section II.A.3.b for a discussion of the comments received on this matter.

1095 *See supra* section IV.C.2.a(1).

accessed or used without authorization.[1096] Given the computational complexity involved in deciphering information encrypted using modern encryption algorithms and secure procedures, [1097] the compromise of such encrypted information would generally not give rise to "a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information."[1098] It would thus not constitute "sensitive customer information," meaning that the threshold for providing notice would not be met. In addition, when determining that the compromised 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, a covered institution may consider encryption as a factor.[1099] Hence, in some cases, an explicit encryption safe harbor would be superfluous. In certain other cases, however, an explicit encryption safe harbor may not be as protective as the final amendments' Federal minimum 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."[1100] It may also become outdated as technologies and security practices evolve. Thus, while an explicit (and appropriately

---

1096 *See* final rule 248.30(a)(3)(iii).

1097 Here, "secure procedures" refers to the secure implementation of encryption algorithms and encompasses proper key generation and management, timely patching, user access controls, etc.

1098 *See* final rule 248.30(d)(9); *see also supra* footnotes 139 and 141 and accompanying text.

1099 *See* final rule 248.30(a)(4); *see also supra* footnote 138 and accompanying text.

1100 *See* final rule 248.30(d)(9). The Aug. 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.

circumscribed) safe harbor could provide some procedural efficiencies from streamlined application, it could also be misapplied.

4. Longer Customer Notification Deadlines

The Commission considered incorporating longer customer notification deadlines, such as 60 or 90 days instead of the adopted 30 days, as well as providing no fixed customer notification deadline. Several commenters suggested longer customer notification deadlines.[1101] Although longer notification deadlines would provide more time for covered institutions to rebut the presumption of notification discussed in section II.A.3.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 expect 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.[1102] Arguably, longer notification deadlines may increase reputational costs borne by covered institutions that choose to take advantage of the longer deadlines. Overall, however, we

---

[1101] *See, e.g.*, FSI Comment Letter; IAA Comment Letter 1. *See also supra* footnote 796 and accompanying text and *supra* section II.A.3.d(1) for a discussion of the comments received on this matter.

[1102] *See supra* section IV.D.1.b(2).

do not expect that longer notification deadlines would lead to costs for covered institutions that differ significantly from the costs of the adopted 30-day outside timeframe.

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 IV.D.1.b(2), some breaches are discovered very quickly. For customers whose sensitive customer information is compromised in such breaches, a longer notification deadline could significantly reduce the timeliness—and value—of the notice.[1103] 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).[1104]

5. Broader National Security and Public Safety Delay in Customer Notification

The Commission considered providing for a broader delay to the 30-day notification outside timeframe by extending its applicability to cases where any appropriate law enforcement agency requests the delay.[1105] This alternative delay would more closely align with the delays adopted by other regulators, such as the Banking Agencies,[1106] and by many states.[1107] Several

---

1103 *See supra* footnote 784 and accompanying text.

1104 *See supra* footnote 803 and accompanying text.

1105 The final amendments differ from the proposal in that they allow for a longer national security and public safety delay under certain circumstances and allow for a delay if the notice poses a substantial risk to either public safety or national security (the proposal referred to national security risk only). However, the final amendments allow for such a delay only if the Attorney General informs the Commission, in writing, of such risk. *See supra* section II.A.3.d(2).

1106 *See* Banking Agencies' Incident Response Guidance.

1107 *See, e.g.*, RCW 19.255.010(8); Fla. Stat. § 501.171(4)(b).

commenters suggested broader delays.[1108] On the other hand, another commenter stated that the Commission should not allow for any law enforcement delay.[1109]

The principal function of a law enforcement delay is to allow a law enforcement or national security agency to prevent cybercriminals from becoming aware 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.[1110] Notifying affected customers has the potential to alert attackers that their intrusion has been detected, hindering these efforts.[1111] Thus, a broader delay 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. It would also potentially reduce compliance costs for covered institutions by aligning more closely with the existing regulations discussed above.[1112]

That said, use of the delay provisions would necessarily result in customers affected by a cyberattack being notified later, reducing the value to customers of such notices.[1113] 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

---

1108 *See, e.g.*, Nasdaq Comment Letter; ICI Comment Letter 1.

1109 *See* Better Markets Comment Letter.

1110 *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").

1111 *Id*.

1112 *See supra* section IV.C.2.

1113 *See supra* footnote 784 and accompanying text.

could prevent additional harm.[1114] 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.[1115] No commenter suggested such data. Thus, we are unable to quantify the costs and benefits of this alternative.[1116]

V. PAPERWORK REDUCTION ACT

A. Introduction

Certain provisions of the final amendments contain "collection of information" requirements within the meaning of the Paperwork Reduction Act of 1995 ("PRA").[1117] We are submitting the final collection of information to the Office of Management and Budget ("OMB") for review in accordance with the PRA.[1118] The safeguards rule and the disposal rule we are amending will 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."[1119] An agency may

---

1114 *See supra* section IV.D.1.b(2).

1115 We do, however, have evidence that requests by law enforcement to delay customer notification are relatively rare events. *See supra* footnote 806.

1116 We requested public comment on these topics in the Proposing Release but did not receive any.

1117 44 U.S.C. 3501 through 3521.

1118 44 U.S.C. 3507(d); 5 CFR 1320.11.

1119 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 final amendments will implement a statutory exception that has been in effect since late 2015. We do not believe that the amendment to implement the statutory exception makes any substantive modifications to

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 amended requirement to adopt policies and procedures constitutes a collection of information requirement under the PRA. The collection of information associated with the final amendments will be mandatory, and responses provided to the Commission in the context of its examination and oversight program concerning the final amendments will be kept confidential subject to the provisions of applicable law. A description of the final 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 final amendments can be found in section III above. The Commission published notice soliciting comments on the collection of information requirements in the Proposing Release and submitted the proposed collections of information to OMB for review in accordance with 44 U.S.C. 3507(d) and 5 CFR 1320.11.

The Commission did not receive any comments that specifically addressed the estimated PRA analysis in the Proposing Release but did receive comments regarding the costs and burdens of the proposed rules generally. Those comments are discussed in more detail in section IV above. In particular, several commentators raised concerns regarding the costs associated with

---

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 final 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 final 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.

negotiating and renegotiating written contracts with service providers.[1120] One commenter did support the proposed written contract provision due to its very narrow scope.[1121] In response to commenters' concerns about the costs of negotiating contracts, we have replaced the proposed requirement for a covered institution to have a written contract with a service provider with a requirement to implement written policies and procedures to oversee, monitor, and conduct due diligence on the service provider. In a modification from the proposal, rather than requiring written policies and procedures requiring the covered institution to enter into a written contract with its service providers to take certain appropriate measures, the policies and procedures required by the final amendments must be reasonably designed to ensure service providers take appropriate measures to: (A) protect against unauthorized access to or use of customer information; and (B) provide notification to the covered institution regarding an incident affecting customer information in the timeframes and circumstances discussed above. The modifications to the proposal are designed to address many of commenters' concerns regarding the costs associated with the service provider provisions of the proposed amendments. We have not reduced the Proposing Release's PRA estimates, however, because the final amendments still require policies and procedures regarding service providers that we estimate will involve PRA burdens consistent with those we estimated for the proposed requirement. As discussed above, some commenters urged for more time to investigate incidents, suggesting that failing to do so

---

1120 *See* STA and ComputerShares Comment Letters (transfer agents don't have the leverage to negotiate contracts with service providers); ASA Comment Letter (no discussion or estimate of the costs the written contract requirement would impose on brokers); IAA Comment Letter (individual advisers, particularly smaller advisers, lack leverage to engage in contractual negotiations with many service providers); ACLI Comment Letter; Cambridge Comment Letter; CAI Comment Letter; AWS Comment Letter; Google Comment Letter. Other commenters raised this issue but suggested extending the implementation period as a remedy. *See* NASDAQ Comment Letter; FIF Comment Letter; SIFMA Comment Letter 2.

1121 *See* ICI Comment Letter.

would result in an increase in the amount of notices being provided.[1122] We are increasing the estimates associated with the final rule with regards to the preparation and distribution of notices because these comments seem to suggest a view that the proposed estimates related to these burdens were too low. We have also adjusted the proposal's estimated annual burden hours and total time costs to reflect updated wage rates.

B. Amendments to the Safeguards Rule and Disposal Rule

As discussed above, the final amendments to the safeguards rule will 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 final amendments).

The final amendments to the disposal rule will require covered institutions that maintain or otherwise possess customer information, or consumer information to adopt and implement written policies and procedures that address proper disposal of such information, which will include taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

[1122] *See, e.g.*, *supra* footnote 165 and accompanying text.

Finally, the final amendments will require covered institutions other than funding portals to make and maintain written records documenting compliance with the requirements of the safeguards rule and the disposal rule. Under the final amendments, the time periods for preserving records will vary by covered institution to be consistent with existing recordkeeping rules.[1123]

Based on FOCUS Filing, Form BD Filing, and Form BD-N data, as of the third quarter of 2023, there were 3,476 brokers or dealers, other than notice-registered brokers or dealers or funding portals. Based on Investment Adviser Registration Depository data, as of Oct. 5, 2023, there were 15,565 investment advisers registered with the Commission. As of Sept. 30, 2023, there were 13,766 investment companies.[1124] Based on Form TA-1, as of Sept. 30, 2023, there were 251 transfer agents registered with the Commission and 64 transfer agents registered with the Banking Agencies. Based on staff analysis and publicly available filings, as of Dec. 31, 2023, there were 92 funding portals.

Table 5 below summarizes our PRA initial and ongoing annual burden estimates associated with the final amendments to the safeguards rule and the disposal rule.

Table 5: 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

[1123] The final amendments will 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 covered institution or is handled or maintained on its behalf, 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.

[1124] Data on investment companies registered with the Commission comes from Form N-CEN filings; data on BDCs comes from LSEG BDC Collateral; and data on employees' securities companies comes from Form 40-APP. *See supra* Table 4.

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 senior programmer)	$381	$0
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
FINAL ESTIMATES					
Broker-dealers other than notice registered broker-dealers, investment advisers registered with the Commission and investment companies					
Adopting and implementing policies and procedures	60 hours	25 hours[3]	$501 (blended rate for compliance attorney and assistant general counsel)	$12,525 (equal to the internal annual burden X the wage rate)	$2,920[9]

Preparation and distribution of notices	12 hours	9 hours[5]	$329 (blended rate for senior compliance examiner and compliance manager)	$2,961 (equal to the internal annual burden X the wage rate)	$2,217[10]
Recordkeeping	1 hour	1 hour	$420 (blended rate for compliance attorney and senior programmer)	$420	$0
Total new annual burden per applicable covered institution		35 hours (equal to the sum of the above three boxes)		$15,906 (equal to the sum of the above three boxes)	$5,137 (equal to the sum of the above two boxes)
Number of applicable covered institutions		x 32,807 covered institutions[11]		x 32,807 covered institutions	16,404[8]
New annual applicable covered institutions aggregate burden		1,148,245 hours		$521,828,142	$84,267,348
Transfer Agents					
Adopting and implementing policies and procedures	75 hours	30 hours[12]	$501 (blended rate for compliance attorney and assistant general counsel)	$15,030 (equal to the internal annual burden X the wage rate)	$2,920[9]
Preparation and distribution of notices	12 hours	9 hours[5]	$329 (blended rate for senior compliance examiner and compliance manager)	$2,961 (equal to the internal annual burden X the wage rate)	$2,217[10]
Recordkeeping	1 hour	1 hour	$420 (blended rate for compliance attorney and senior programmer)	$420	$0

Total new annual burden per transfer agent		40 hours (equal to the sum of the above three boxes)		$18,411 (equal to the sum of the above three boxes)	$5,137 (equal to the sum of the above two boxes)
Number of transfer agents		x 315[13]		x 315	158[8]
New annual transfer agent aggregate burden		12,600		$5,799,465	$811,646
Funding Portals					
Adopting and implementing policies and procedures	60 hours	25 hours[3]	$501 (blended rate for compliance attorney and assistant general counsel)	$12,525 (equal to the internal annual burden X the wage rate)	$2,920[9]
Preparation and distribution of notices	12 hours	9 hours[5]	$329 (blended rate for senior compliance examiner and compliance manager)	$2,961 (equal to the internal annual burden X the wage rate)	$2,217[10]
Recordkeeping	1.5 hours[14]	1.5 hours	$420 (blended rate for compliance attorney and senior programmer)	$630	$0
Total new annual burden per funding portal		35.5 hours (equal to the sum of the above three boxes)		$16,116 (equal to the sum of the above three boxes)	$5,137 (equal to the sum of the above two boxes)
Number of funding portals		x 92		x 92	46[8]
New annual funding portal aggregate burden		3,266		$1,482,672	$236,302
Total Estimated Burdens of the Final Amendments					

Total new annual aggregate burden		1,164,111 hours		$529,110,279	$85,315,296
TOTAL ESTIMATED BURDENS INCLUDING AMENDMENTS					
Current aggregate annual burden estimates		+ 65,760 hours			+ $0
Revised aggregate annual burden estimates		1,229,871 hours		$529,110,279	$85,315,296

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 25 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 9 hours is based on the following calculation: ((12 initial hours / 3 years) + 5 hours of additional ongoing burden hours) = 9 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.
9. This estimated burden is based on the estimated wage rate of $584/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.
10. This estimated burden is based on the estimated wage rate of $584/hour, for 3 hours, for outside legal services and $93/hour, for 5 hours, for a senior general clerk.
11. Total number of applicable covered institutions is calculated as follows: 3,476 broker-dealers other than notice-

registered broker-dealers or funding portals + 15,565 investment advisers registered with the Commission + 13,766 investment companies = 32,807 covered institutions. The burdens for funding portals and transfer agents are calculated separately.

12. Includes initial burden estimates annualized over a three-year period, plus 5 hours of ongoing annual burden hours. The estimate of 30 hours is based on the following calculation: ((75 initial hours / 3) + 5 hours of additional ongoing burden hours) = 30 hours.
13. The number of transfer agents includes 251 transfer agents registered with the Commission + 64 transfer agents registered with the Banking Agencies = 315 transfer agents.
14. Funding portals are not subject to the recordkeeping obligations for brokers found under Rule 17a-4. Instead, they are obligated, pursuant to Rule 404 of Regulation Crowdfunding, to make and preserve all records required to demonstrate their compliance with, among other things, Regulation S-P. While the final amendments do not modify funding portals' recordkeeping requirements to include the same enumerated list of obligations as those applied to brokers under the amendments to Rule 17a-4, funding portals generally should look to make and preserve the same scope of records in connection with demonstrating their compliance with this portion of Regulation S-P. Further, Rule 404 requires funding portals to preserve these records for a longer period of time than brokers are required to preserve records under Rule 17a-4. Due to this longer required period for records preservation, the estimated burden for funding portals is higher than for brokers.

VI. FINAL REGULATORY FLEXIBILITY ACT ANALYSIS

The Regulatory Flexibility Act ("RFA") requires the Commission, in promulgating rules under Section 553 of the Administrative Procedure Act,[1125] to consider the impact of those rules on small entities. We have prepared this Final Regulatory Flexibility Analysis ("FRFA") in accordance with Section 604 of the RFA.[1126] An Initial Regulatory Flexibility Analysis ("IRFA") was prepared in accordance with the RFA and was included in the Proposing Release.[1127]

A. Need for, and Objectives of, the Final Amendments

The purpose of the final amendments is to limit potential harmful impacts to customers by enhancing and modernizing the protection of customer information. Among other things, the amendments update the rule's requirements to address the expanded use of technology and corresponding risks.

1125 5 U.S.C. 553.

1126 5 U.S.C. 604.6.

1127 Proposing Release at section V.

The need for, and objectives of, the final amendments are described in Sections I and II above. We discuss the economic impact and potential alternatives to the amendments in Section IV, and the estimated compliance costs and burdens of the amendments under the PRA in Section V.

B. Significant Issues Raised by Public Comments

In the Proposing Release, the Commission requested comment on any aspect of the IRFA, and particularly on the number of small entities that would be affected by the proposed amendments, the existence or nature of the potential impact of the proposed amendments on small entities discussed in the analysis, how the proposed amendments could further lower the burden on small entities, and how to quantify the impact of the proposed amendments.

One commenter urged the Commission to conduct a more holistic cost-benefit analysis, and in particular consider the disproportionate costs on smaller advisers.[1128] The commenter noted that smaller advisers have been significantly burdened by one-size-fits-all regulations – both in isolation and cumulatively – that effectively require substantial fixed investments in infrastructure, personnel, technology, and operations.[1129] Another commenter stated that the Commission did little analysis about the impact of these proposals on small broker-dealers, competition within the brokerage industry, and whether they could contribute to barriers for new entrants into the markets.[1130] We discuss the cost-benefit analysis and challenges small entities may face above.[1131]

1128 *See* IAA Comment Letter 2.

1129 *See* IAA Comment Letter 1.

1130 *See* ASA Comment Letter.

1131 *See supra* section IV.

Additionally, multiple commenters discussed the burden small entities would face. For instance, several commenters stated that an increased compliance cost for implementing new systems, training employees, and conducting audits, may disproportionately affect smaller firms, inhibiting their ability to compete and grow.[1132] Multiple commenters asserted small covered institutions, who may not have the negotiating power or leverage to demand specific contract provisions from large third-party service providers, would potentially be harmed by the written contract requirement for service providers.[1133] Another commenter noted the outsized impact small broker-dealers face.[1134] However, another commenter noted while small firms may be impacted by increased costs, this should not come at the expense of customer protection, and stated that driving competition towards better protections will ultimately benefit customers and promote a healthier market.[1135]

Commenters proposed multiple alternatives to lower the burden on small entities. One commenter urged the Commission to provide a longer time to transition for smaller advisers.[1136] Additionally, the commenter stated that it has frequently called on the Commission to take steps to tailor its rules to minimize impacts the proposed amendments would have on smaller advisers, for example through preserving a flexible, risk- and principles-based approach, excluding or exempting smaller advisers from specific requirements where the burdens on those advisers outweigh the benefits, and tiering and staggering compliance timetables.[1137] Likewise, another commenter

---

1132 *See* Grey Comment Letter, Robinson Comment Letter, and Scouten Comment Letter; *see also* ASA Comment Letter.

1133 *See* IAA Comment Letter 2; *see also* STA Comment Letter 2 and Computershare Comment Letter.

1134 *See* FSI Comment Letter.

1135 *See* Wohlfahrt Comment Letter.

1136 *See* IAA Comment Letter 1.

1137 *See* IAA Comment Letter 2; *see also* STA Comment Letter suggesting exempting transfer agents that do not maintain a threshold number of shareholder accounts. *See supra* section IV.E for further discussion of exemption based upon size.

proposed a longer implementation period for smaller broker-dealers and investments advisers to allow these firms to benefit from implementation for larger industry participants.[1138]

We expect the benefits and the costs of the final amendments to vary across covered institutions.[1139] For example, because smaller covered institutions are less likely to have an existing incident response program than larger covered institutions, some small entities may be more likely to face greater costs but also expect greater benefits complying with the final amendments, because they must adopt and implement new procedures. Creating new programs will likely cost more, but the new programs would result in improved efficacy in notifying customers and improve the manner incidents are handled. Smaller entities may have less negotiating power than larger entities, so requiring contracts with service providers could potentially be more detrimental to them than other entities. Additionally, smaller covered institutions are less likely to have a national presence, so small entities whose customers are concentrated in states with less informative customer notification laws are likely to face higher costs to comply with the final amendments. These costs and benefits may have an effect on competition for smaller entities.[1140]

We have revised the final amendments in several ways to mitigate potential compliance costs that small entities may face, as raised by commenters. As previously discussed, the changes made to the service provider provisions of the amendments requiring that the covered institution's policies and procedures are reasonably designed to oversee, monitor, and conduct due diligence on service providers instead of requiring written contracts between covered institutions and their service providers, and requiring that the covered institution's policies and

---

1138 *See* FSI Comment Letter.

1139 *See supra* section IV.

1140 *See supra* section IV.E.

procedures be reasonably designed to ensure service providers take appropriate measures to notify covered institutions of an applicable breach in security within 72 hours instead of 48 hours) may reduce some costs relative to the proposal and facilitate their implementation, especially for smaller covered institutions.[1141] For example, it could potentially reduce compliance costs by reducing the number of notices being sent (e.g., if the covered institution is able to determine that a notice is not needed or if it is able to determine with more precision which individuals must be notified).[1142] Additionally, we are now adopting a longer compliance period of 24 months for smaller covered institutions, who are less likely to already have policies and procedures broadly consistent with the final amendments.

Moreover, the final amendments still maintain that the incident response program must include policies and procedures containing certain general elements but will not prescribe specific steps a covered institution must undertake when carrying out incident response activities, thereby enabling covered institutions to create policies and procedures best suited to their particular circumstances, including size. This design balances the necessity of maintaining general elements to achieve the investor protection objectives the amendments are designed to achieve, while still providing covered institutions the ability to tailor policies to their individual needs. We will not exempt small entities from any specific requirements, because entities of all sizes are vulnerable to the types of data security breach incidents we are trying to address, and therefore, no entity should be exempted from requirements, regardless of size.[1143]

Additionally, one commenter argued that the Commission does not accurately analyze the impact of its regulations on small advisers as required under the RFA because according to the

---

1141 *See supra* section IV.

1142 *See supra* section IV.

1143 *See infra* section VI.E for further discussion of exemption based upon size.

commenter, virtually no SEC-registered advisers fall under the "asset-based" definition of small adviser adopted by the Commission.[1144] However, the commenter believes that the vast majority of advisers are small businesses.[1145] The commenter stated that the Commission adopted Rule 0-7 under the Advisers Act defining "small business" or "small organization" for purposes of treatment as a "small entity" under the RFA as including an investment adviser that has less than $25 million in assets under management, but with few exceptions, advisers are not permitted to register with the Commission unless they have at least $100 million in assets under management.[1146] The commenter argued that this makes any analysis the Commission does regarding the impact on smaller advisers virtually meaningless.[1147] As discussed below, we estimate that approximately 872 broker-dealers[1148], 132 transfer agents, 81 investment companies, and 579 registered investment advisers may be considered small entities under the Regulatory Flexibility Act.[1149] The Commission takes seriously the potential impact of any new rule on these advisers who meet this definition and on other smaller advisers that do not meet the definition of small entity under the Regulatory Flexibility Act, as considered and discussed throughout this release.

C. Small Entities Subject to Final Amendments

The final amendments to Regulation S-P will 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

---

1144 *See* IAA Comment Letter 2.

1145 *See* IAA Comment Letter 2.

1146 *See* IAA Comment Letter 2.

1147 *See* IAA Comment Letter 2.

1148 This 872 broker-dealers includes 89 funding portals.

1149 *See infra* section VI.C.

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.[1150] 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.[1151] 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.[1152] 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.[1153]

1150 17 CFR 240.0-10. Funding portals, who are considered "brokers" for purposes of this release unless otherwise noted, are also included in this definition. *See* 17 CFR 227.403(b); *See also supra* footnote 5.

1151 *Id.*

1152 17 CFR 270.0-10.

1153 17 CFR 275.0-7.

Based on Commission filings, we estimate that approximately 872 broker-dealers,[1154] 132 transfer agents,[1155] 81 investment companies,[1156] and 579 registered investment advisers[1157] may be considered small entities.

D. Projected Reporting, Recordkeeping, and Other Compliance Requirements

The final amendments to Regulation S-P will 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 final 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 final 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 will also need to require that covered institutions oversee, monitor, and conduct due diligence on service providers and ensure that service providers take appropriate measures to notify covered institutions of an applicable breach in security within 72 hours. Upon receipt of

---

1154 Estimate based on Q3 2023 FOCUS Report data, staff analysis and public filings. This 872 broker-dealers includes 89 funding portals.

1155 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 collected by the Commission as of September 30, 2023.

1156 Based on Commission staff approximation that approximately 41 open-end funds (including 10 exchange-traded funds), 23 closed-end funds, 3 UITs and 14 business development companies are small entities. This estimate is derived from an analysis of data obtained from Morningstar Direct and data reported to the Commission (*e.g.* N-PORT, N-CSR, 10-Q and 10-K) for the second quarter of 2023.

1157 Based on SEC-registered adviser responses to Items 5.F. and 12 of Form ADV as of October 5, 2023.

such notification, the covered institution must initiate its incident response program. 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. However, the covered institution's obligation to ensure that affected individuals are notified in accordance with paragraph (a)(4) of the final amendments rests with the covered institution.

In addition, covered institutions will be required to make and maintain specified written records designed to evidence compliance with these requirements.[1158] Such records will 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.

Some covered institutions, including covered institutions that are small entities, will 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 will 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, including customer notification procedures, in a manner that provides clarity for firm personnel. Further, in developing these policies and procedures, covered institutions will need to include policies and procedures requiring the covered institution to ensure its service providers take appropriate measures to protect against unauthorized access to or use of customer information, and notify the covered institution as soon as possible, but no later than 72 hours after becoming

---

[1158] With regard to funding portals, please see discussion as to their applicable recordkeeping obligations *supra* footnote 385 and accompanying discussion.

aware that a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider, and upon receipt of such notification, the covered institution must initiate its response program. However, as the Commission recognizes the number and varying characteristics (e.g., size, business, and sophistication) of covered institutions, these final 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 final amendments will 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. Such costs will 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 final amendments. Such costs will 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 final amendments 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 will need to respond appropriately to incidents that entail the unauthorized access to or use of customer information. This will 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 will need to provide a clear and conspicuous notice, or ensure that such notice is provided, to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. This notice must be provided as soon as reasonably practicable, but not later than 30 days, after the covered institution becomes aware that unauthorized access to or use of sensitive customer information has, or is reasonably likely to have, occurred, absent an applicable request from the Attorney General. This notice will 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 will need to satisfy

the specified content requirements of that notice,[1159] the preparation of which will incur some incremental additional costs on covered institutions.

Finally, covered institutions will 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 record maintenance provisions 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 will be associated with the final amendments to Regulation S-P.[1160] Some proportion of large or small institutions would be likely to experience some increase in costs to comply with the amendments.

More specifically, we estimate that many covered institutions will incur one-time costs related to reviewing and revising their current safeguarding policies and procedures to comply

---

[1159] *See* final rule 248.30(a)(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) 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; (iii) 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; (iv) 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; (v) 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; (vi) recommend that the individual periodically obtain credit reports from each nationwide credit reporting company and that the individual have information relating to fraudulent transactions deleted; (vii) explain how the individual may obtain a credit report free of charge; and (viii) include information about the availability of online guidance from the FTC and usa.gov regarding steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the FTC, and include the FTC's website address where individuals may obtain government information about identity theft and report suspected incidents of identity theft.

[1160] 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.

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 have such policies and procedures. We also estimate that the ongoing, long-term costs associated with the final amendments could include costs of responding appropriately to incidents that entail the unauthorized access to or use of customer information.

E. Agency Action to Minimize Effect on Small Entities

The RFA directs us to consider alternatives that would accomplish our stated objectives, while minimizing any significant adverse impact on small entities. Accordingly, we considered the following alternatives:

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, the final amendments to Regulation S-P that will 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. However, it is necessary 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 will include customer notification

procedures.[1161] The 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 amendments. However, we are providing smaller covered institutions a longer compliance period to establish and implement processes to comply with the final amendments.

With regard to the second alternative, the final amendments will, 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 amendments will 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 and procedures to its individual facts and circumstances. The 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 amendments already will be simplified for small entities. In addition, the requirements of the amendments could not be further simplified, or clarified or consolidated, without compromising the investor protection objectives the amendments are designed to achieve.

With regard to the third alternative, the final amendments are design based. Rather than specifying the types of policies and procedures that an institution would be required to include in

---

[1161] *See* final rule 248.30(a)(3).

its response program, the amendments will 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, 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, 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 the final amendments 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 amendments or any part of the amendments could compromise the effectiveness of the 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.

STATUTORY AUTHORITY

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

FCRA [15 U.S.C. 1681w(a)], and sections 501, 504, 505, and 525 of the GLBA [15 U.S.C. 6801, 6804, 6805, and 6825].

List of Subjects

17 CFR Parts 240, 270, and 275

Reporting and recordkeeping requirements; Securities.

17 CFR Part 248

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

TEXT OF RULE AMENDMENTS

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

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

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

Authority: 15 U.S.C. 77c, 77d, 77g, 77j, 77s, 77z-2, 77z-3, 77eee, 77ggg, 77nnn, 77sss, 77ttt, 78c, 78c-3, 78c-5, 78d, 78e, 78f, 78g, 78i, 78j, 78j-1, 78j-4, 78k, 78k-1, 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, 1681w(a)(1), 6801-6809, 6825, 7201 *et seq.,* and 8302; 7 U.S.C. 2(c)(2)(E); 12 U.S.C. 5221(e)(3); 18 U.S.C. 1350; Pub. L. 111-203, 939A, 124 Stat. 1376 (2010); and Pub. L. 112-106, sec. 503 and 602, 126 Stat. 326 (2012), unless otherwise noted.

* * * * *

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

* * * * *

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

* * * * *

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

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

* * * * *

(e) * * *

(13) [Reserved]

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

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

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

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

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

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

* * * * *

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

a. Revising the section heading;

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

c. Adding paragraph (k).

The revisions read as follows:

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

* * * * *

(j) [Reserved]

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

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

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

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

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

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

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

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

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

Authority: 15 U.S.C. 78q, 78q–1, 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 §248.5 by revising paragraph (a)(1), and adding paragraph (e) to read as follows:

§ 248.5 Annual privacy notice to customers required.

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

* * * * *

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

(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.

§ 248.17 [Amended]

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

7. Revise § 248.30 to read as follows:

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

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

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

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

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

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

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

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

(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 (a)(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 occurred at the covered institution or one of its service providers that is not itself a covered institution, that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience, the covered institution must provide a clear and conspicuous notice, or ensure that such notice is provided, to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. The notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing.

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

(iii) *Timing*. A covered institution must provide the notice as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred unless the United States Attorney General determines that the notice required under this rule poses a substantial risk to national security or public safety, and notifies the Commission of such determination in writing, in which case the covered institution may delay providing such notice for a time period specified by the Attorney General, up to 30 days following the date when such notice was otherwise required to be provided. The notice may be delayed for an additional period of up to 30 days if the Attorney General determines that the notice continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. In extraordinary circumstances, notice required under this section may be delayed for a final additional period of up to 60 days if the Attorney General determines that such notice continues to pose a substantial risk to national security and notifies the Commission of such determination

in writing. Beyond the final 60-day delay under this paragraph (a)(4)(iii), if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such delay through Commission exemptive order or other action.

(iv) *Notice contents*. The notice must:

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

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

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

(D) If the individual has an account with the covered institution, recommend that the customer review account statements and immediately report any suspicious activity to the covered institution;

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

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

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

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

(5) *Service providers*. (i) A covered institution's response program prepared in accordance with paragraph (a)(3) of this section must include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers, including to ensure that the covered institution notifies affected individuals as set forth in paragraph (a)(4) of this section. The policies and procedures must be reasonably designed to ensure service providers take appropriate measures to:

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

(B) Provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider. Upon receipt of such notification, the covered institution must initiate its incident response program adopted pursuant to paragraph (a)(3) of this section.

(ii) As part of its incident response program, a covered institution may enter into a written agreement with its service provider to notify affected individuals on the covered institution's behalf in accordance with paragraph (a)(4) of this section.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) *Consumer information* means any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report, or a

compilation of such records, that a covered institution maintains or otherwise possesses for a business purpose regardless of whether such information pertains to (i) individuals with whom the covered institution has a customer relationship, or (ii) to the customers of other financial institutions where such information has been provided to the covered institution. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.

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

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

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

(ii) With respect to a transfer agent registered with the Commission or another ARA, for purposes of this section, *customer* means any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent.

(5)(i) *Customer information* for any covered institution other than a transfer agent registered with the Commission or another ARA means any record containing nonpublic personal information as defined in § 248.3(t) about a customer of a financial institution, whether in paper, electronic or other form, that is in the possession of a covered institution or that is handled or maintained by the covered institution or on its behalf regardless of whether such information pertains to (a) individuals with whom the covered institution has a customer

relationship, or (b) to the customers of other financial institutions where such information has been provided to the covered institution.

(ii) With respect to a transfer agent registered with the Commission or another ARA, *customer information* means any record containing nonpublic personal information as defined in § 248.3(t) identified with any natural person, who is a securityholder of an issuer for which the transfer agent acts or has acted as transfer agent, that is in the possession of a transfer agent or that is handled or maintained by the transfer agent or on its behalf, regardless of whether such information pertains to individuals with whom the transfer agent has a customer relationship, or pertains to the customers of other financial institutions and has been provided to the transfer agent.

(6) *Customer information systems* means the information resources owned or used by a covered institution, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of customer information to maintain or support the covered institution's operations.

(7) *Disposal* means:

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

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

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

(9)(i) *Sensitive customer information* means any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.

(ii) Examples of sensitive customer information include:

(A) Customer information uniquely identified with an individual that has a reasonably likely use as a means of authenticating the individual's identity, including

(*1*) A Social Security number, official State- or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(*2*) A biometric record;

(*3*) A unique electronic identification number, address, or routing code;

(*4*) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)); or

(B) Customer information identifying an individual or the individual's account, including the individual's account number, name or online user name, in combination with authenticating information such as information described in paragraph (d)(9)(ii)(A) of this section, or in combination with similar information that could be used to gain access to the customer's account such as an access code, a credit card expiration date, a partial Social Security number, a security code, a security question and answer identified with the individual or the individual's account, or the individual's date of birth, place of birth, or mother's maiden name.

(10) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution.

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

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

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

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

* * * * *

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

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

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

* * * * *

(b) * * *

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

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

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

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

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

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

* * * * *

10. Amend § 270.31a-2 by:

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

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

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

(a) * * *

(8) Preserve for a period not less than six years, the first two years in an easily accessible place, the records required by § 270.31a-1(b)(13) apart from any policies and procedures thereunder and, in the case of policies and procedures required under § 270.31a-1(b)(13),

preserve a copy of such policies and procedures in effect, or that at any time within the past six years were in effect, in an easily accessible place.

* * * * *

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

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

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

* * * * *

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

* * * * *

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

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

(a) * * *

(25)

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

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

(iii) The written documentation of any investigation and determination made regarding whether notification is required pursuant to § 248.30(a)(4) of this chapter, including the basis for any determination made, any written documentation from the United States Attorney General

related to a delay in notice, as well as a copy of any notice transmitted following such determination;

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

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

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

* * * * *

By the Commission.

Dated: May 16, 2024.

Vanessa A. Countryman,

Secretary.