July 18, 2025

By Electronic Submission

The Hon. Paul Atkins
Chairman
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: File No. S7-05-23
Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information

Dear Chairman Atkins,

The Securities Industry and Financial Markets Association ("SIFMA"), SIFMA Asset Management Group ("SIFMA AMG"), American Bankers Association ("ABA"), Bank Policy Institute ("BPI"), Financial Services Institute ("FSI"), Institute of International Bankers ("IIB"), Investment Company Institute ("ICI"), Insured Retirement Institute ("IRI"), and the Committee of Annuity Insurers ("CAI") (collectively, the "associations") appreciate the opportunity to provide suggested changes to the recent amendments to Regulation S-P issued by the Securities and Exchange Commission (the "Commission" or "SEC") on May 16, 2024 (the "Regulation S-P Amendments").[1]

Regulation S-P should be further amended to provide further clarity and guidance to its existing rules. Our members appreciate the importance of strong cybersecurity practices for companies and our country, including appropriate notification of cybersecurity incidents to individuals.[2] The joint trades comment letter on the Regulation S-P Amendments ("Joint Trades

[1] Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information Securities, Release Nos. 34–100155; IA–6604; IC–35193, 89 Fed. Reg. 47688 (June 3, 2024). SIFMA notes that it requested an extension of the comment response deadline in order for it and other interested parties to have a full opportunity to comment effectively on this and many hundreds of pages of other SEC cybersecurity proposals that are simultaneously pending or were open or re-opened for comment at the same time as this Proposal.

[2] *See Cybersecurity Resources*, SIFMA, https://www.sifma.org/resources/cybersecurity-resources/; *SIFMA Statement on Completion of Quantum Dawn VI Cybersecurity Exercise*, SIFMA (Nov. 18, 2021), https://www.sifma.org/resources/news/sifma-statement-on-completion-of-quantum-dawn-vi-cybersecurity-exercise/; Letter from SIFMA to the SEC (Apr. 11, 2022), https://www.sifma.org/wp-content/uploads/2022/04/SIFMA-and-

Letter") as originally proposed urged the Commission to reconsider certain aspects of its Regulation S-P Proposal, which at times is too prescriptive and does not provide enough flexibility to covered institutions in responding to the unique circumstances that can arise during an incident.[3] Such prescriptive requirements may subject covered institutions to unnecessary and adverse enforcement actions if such requirements are not followed to the letter which may happen due to any number of circumstances surrounding a cyber event. As such, Appendix B includes detailed proposed revisions to improve the Regulation S-P Amendments, which takes into account a covered institution's need to comply with existing data breach notification laws and the benefit of coordinating with a range of law enforcement, cybersecurity, intelligence, and national security agencies during a security incident.

Further, the associations continue to urge the Commission to extend the compliance date for the Regulation S-P Amendments by an additional year. The associations believe that additional time is absolutely necessary to achieve our members' compliance with the prescriptive requirements in the Regulation S-P Amendments. Regardless of the Commission's decision on that extension request, we believe these additional changes are necessary to ensure that compliance can be achieved efficiently and without jeopardizing the security of customer information.

Summary of Proposed Changes

The associations' suggested revisions to the Regulation S-P Amendments in Appendix B reflect the following considerations, many of which were included in the Joint Trades Letter, which can be cross-referenced for additional details:[4]

- **Harmonize with the notification requirement for service providers with existing standards**. The Commission should eliminate the 72-hour notification requirement for service providers, which is an unreasonably specific standard that does not adequately align with the wide variety of service providers. The associations' proposed edits would harmonize service provider and covered institution requirements by requiring service providers to provide notification to a covered institution without unreasonable delay after a reasonable investigation has been performed. Importantly, this approach would be wholly consistent with, for example, the Final Interagency Guidance on Third-Party Relationships: Risk Management, which provides that banking organizations should adopt "sound risk management practices that are commensurate with the level of risk and complexity of their respective third-party relationships."

AMG-Comment-Letter-on-SEC-Cybersecurity-Proposals.pdf; Letter from SIFMA to the SEC (May 9, 2022), https://www.sifma.org/wp-content/uploads/2022/05/SIFMA-Comment-S7-09-22-May-9-2022.pdf.

[3] *See* Letter from Joint Trades to the SEC (June 5, 2023), https://www.sifma.org/wp-content/uploads/2023/06/Regulation-S-P-Privacy-of-Consumer-Financial-Information-and-Safeguarding-Customer-Information-Joint-Trades.pdf.

[4] *See* Letter from Joint Trades to the SEC (June 5, 2023), https://www.sifma.org/wp-content/uploads/2023/06/Regulation-S-P-Privacy-of-Consumer-Financial-Information-and-Safeguarding-Customer-Information-Joint-Trades.pdf; see Letter from Joint Trades to the SEC Requesting Extension of Compliance Dates for Amendments to Regulation S-P (Apr. 25, 2025), https://www.sifma.org/wp-content/uploads/2025/04/Regulation-S-P-Time-Extension-Request-April-25-2025.pdf; *see* ICI Letter to the SEC (May 23, 2023), https://www.sec.gov/comments/s7-05-23/s70523-193259-384202.pdf; see IAA Letter to the SEC (June 17, 2023), https://www.sec.gov/comments/s7-05-23/s70523-206962-416982.pdf.

- **Allow for investigation and a reasonable notification period**. The Commission should allow a covered institution to provide notice only after it has conducted a reasonable investigation and concluded that misuse of customer information has occurred or is likely to occur. As such, covered institutions would not be subject to an arbitrary 30-day notification requirement, which is an entirely insufficient amount of time for covered institutions to perform reasonable investigations and risk assessments, collect and analyze the voluminous information necessary to generate customer notices, and provide notices, especially when dealing with in complex cases. It would also eliminate a maximum limit on notice delays, allowing for such delays for an unspecified period of time, subject to determination by law enforcement, intelligence, or cyber security authorities.

- **Do not require that a covered institution provide notice to customers with whom it does not have a preexisting relationship**. A covered institution should only be required to provide notice to its own customers or to the institution that provided the sensitive information that was, or is reasonably likely to have been, accessed or used without authorization (subject to the requisite triggering data elements and risk of harm threshold). It would be impractical for a covered institution to identify and contact customers of another institution and could cause customers to be confused and concerned about why they receive notification from an institution with which they do not have a relationship. Accordingly, we have created two sections regarding notification: one for affected individuals who are customers of the covered institution, and one for affected individuals who are customers of a third-party financial institution.

- **Allow covered institutions greater flexibility in notice content and format.** We agree that contact information sufficient for an individual to contact the covered institution should be included in customer notifications. However, covered institutions should have flexibility in determining the type of contact information to provide based on how they normally interact with their customers. As such, we propose revising the current requirement to require only one of the listed contact methods to better align with existing procedures.

- **Broaden the national security exception to include a law enforcement and cybersecurity agency exception, including foreign counterparts**. The national security notification exception should be expanded to include cooperation with appropriate law enforcement and cybersecurity agencies, as well as cooperation with international authorities with the flexibility to determine when such cooperation qualifies for the exception. Such a provision would incentivize the industry to include provisions in their incident response plans to seek help from international, federal, state, or local government resources early during a cyber-related incident. Given the priority of national security and public safety concerns, a covered entity should be allowed to temporarily pause any required Reg S-P data breach notification or disclosure when an appropriate law enforcement agency (such as, the FBI or a state law enforcement agency) is requesting a delay, or where a court order requires delay in public disclosure until such time as the delay is lifted.

- **Define "Sensitive Customer Information" more clearly and consistent with other federal and state breach standards.** The Commission should list the specific data elements that are sensitive and could trigger notification rather than leaving an open-ended standard that just offers potential examples of such data elements. This, again, would be consistent with the approach used in the Interagency Guidance. Accordingly, we proposed that the Commission adopt the definition of "sensitive customer information" in the Interagency Guidance, which means 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 a social security number, driver's license number, alien registration number, government passport number, or employer or taxpayer identification number; a biometric record; or a unique electronic identification number, address, or routing code that would permit access to the customer's account.

- **Clarify other select definitions to avoid over-notification.** First, the Commission should remove the "consumer information" definition and focus on customer information—that is, information that is actually related to an account with the covered institution or service provider. Additionally, service provider notification obligations should be limited to incidents of unauthorized access to or use of "customer information," rather than information existing on "customer information systems." The latter definition is overbroad and would be likely to overburden information security teams of both the service provider and the covered institution. Finally, we propose excluding affiliates of covered institutions from the definition of "service provider," since affiliates are part of the same enterprise information/cybersecurity oversight as the covered institutions.

- **Expressly exclude encrypted data**. Additionally, the associations recommend that the Commission exclude encrypted information where the decryption key has not been obtained, consistent with existing state data breach notification laws. Note that all U.S. state data breach notification laws provide an encryption safe harbor because it incentivizes encryption to protect customer data. To this end, we have proposed adding the word "nonencrypted" to the definition of customer information.

The associations appreciate the Commission's attention to cybersecurity and privacy and agree with the Commission regarding the importance of sound cybersecurity practices within the financial sector in order to decrease cybersecurity risk from threat actors. However, we encourage the Commission to consider our proposed changes as a means to avoid too many overly prescriptive, duplicative, and burdensome requirements on covered institutions. These changes would better promote harmonization between the various SEC-proposed rules—and with rules of other federal agencies—simplify requirements within the proposals, and design proposals that protect against cyberthreats without creating enforcement and litigation traps.

If you have any questions or would like to discuss these comments further, please reach out to Melissa Macgregor at mmacgregor@sifma.org.

Sincerely,

Securities Industry and Financial Markets Association
SIFMA Asset Management Group
American Bankers Association
Bank Policy Institute
Financial Services Institute
Institute of International Bankers
Investment Company Institute
Insured Retirement Institute
Committee of Annuity Insurers

Cc: The Hon. Hester M. Peirce, Commissioner
The Hon. Caroline A. Crenshaw, Commissioner
The Hon. Mark T. Uyeda, Commissioner
Vanessa Countryman, Secretary
Jamie Selway, Director, Division of Trading and Markets
Brian Daley, Director, Division of Investment Management

Attachments

Appendix A – Signatory Associations

The **Securities Industry and Financial Markets Association ("SIFMA")** is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association ("GFMA").

SIFMA Contact: Melissa MacGregor, Deputy General Counsel and Corporate Secretary

SIFMA's Asset Management Group ("SIFMA AMG") brings the asset management community together to provide views on U.S. and global policy and to create industry best practices. SIFMA AMG's members represent U.S. and global asset management firms whose combined assets under management exceed $45 trillion. The clients of SIFMA AMG member firms include, among others, tens of millions of individual investors, registered investment companies, endowments, public and private pension funds, UCITS and private funds such as hedge funds and private equity funds. For more information, visit http://www.sifma.org/amg.

SIFMA Contact: Kevin Ehrlich, Managing Director

The **American Bankers Association ("ABA")** is the voice of the nation's $24.5 trillion banking industry, which is composed of small, regional and large banks that together employ approximately 2.1 million people, safeguard $19.5 trillion in deposits and extend $12.8 trillion in loans.

ABA Contact: John Carlson, Senior Vice President, Cybersecurity Regulation and Resilience

The **Bank Policy Institute ("BPI")** is a nonpartisan group representing the nation's leading banks. BPI members include universal banks, regional banks, and the major foreign banks doing business in the United States. Collectively, BPI members hold $10.7 trillion in deposits in the United States; make 68% of all loans, including trillions of dollars in funding for small businesses and household mortgages, credit cards, and auto loans; employ nearly two million Americans and serve as a principal engine for the nation's financial innovation and economic growth.

BPI Contact: Clara Kim, Senior Vice President

The **Financial Services Institute (FSI)** is the only organization advocating solely on behalf of independent financial advisors and independent financial services firms. Since 2004, through advocacy, education and public awareness, FSI has successfully promoted a more responsible regulatory environment for over 80 independent financial services firm members and their 130,000+ affiliated financial advisors – which comprise over 60% of all producing registered representatives. We effect change through involvement in FINRA governance as well as constructive engagement in the regulatory and legislative processes, working to create a healthier regulatory environment for our members so they can provide affordable, objective advice to hard-working Main Street Americans. For more information, please visit financialservices.org.

FSI Contact: Renee Barnett, Vice President, Federal Regulatory Affairs and Senior Counsel

The **Institute of International Bankers ("IIB")** represents internationally headquartered financial institutions from over thirty-five countries around the world doing business in the United States. The membership consists principally of international banks that operate branches, agencies, bank subsidiaries, and broker-dealer subsidiaries in the United States. The IIB works to ensure a level playing field for these institutions, which are an important source of credit for U.S. borrowers and comprise the majority of U.S. primary dealers. These institutions enhance the depth and liquidity of U.S. financial markets and contribute greatly to the U.S. economy through direct employment of U.S. citizens, as well as through other operating and capital expenditures.

IIB Contact: Michelle Meertens, Deputy General Counsel

The **Investment Company Institute ("ICI")** is the leading association representing the asset management industry in service of individual investors. ICI's members include mutual funds, exchange-traded funds (ETFs), closed-end funds, and unit investment trusts (UITs) in the United States, and UCITS and similar funds offered to investors in other jurisdictions. Its members manage $39.1 trillion invested in funds registered under the US Investment Company Act of 1940, serving more than 120 million investors. Members manage an additional $9.3 trillion in regulated fund assets managed outside the United States. ICI also represents its members in their capacity as investment advisers to collective investment trusts (CITs) and retail separately managed accounts (SMAs). ICI has offices in Washington DC, Brussels, and London.

ICI Contact: Mitra Surrell, Associate General Counsel

The **Insured Retirement Institute ("IRI")** is the leading association for the entire supply chain of insured retirement strategies, including life insurers, asset managers, broker dealers, banks, marketing organizations, law firms, and solution providers. IRI members account for 90 percent of annuity assets in the U.S., include the foremost distributors of protected lifetime income solutions, and are represented by financial professionals serving millions of Americans. IRI champions retirement security for all through leadership in advocacy, awareness, research, diversity, equity, and inclusion, and the advancement of digital solutions within a collaborative industry community.

IRI Contact: Emily Micale, Director, Federal Regulatory Affairs

The **Committee of Annuity Insurers ("CAI")** is a coalition of life insurance companies that issue annuities. It was formed in 1981 to address legislative and regulatory issues relevant to the annuity industry and to participate in the development of public policy with respect to securities, state regulatory and tax issues affecting annuities. The CAI's current 33 member companies represent approximately 80% of the annuity business in the United States. For over 40 years, the CAI has been actively involved in shaping and commenting upon many aspects of the Securities and Exchange Commission's regulatory framework as it affects the offering of annuity and other retirement savings and protection products.

CAI Contact: Alexander F.L. Sand, Partner, Eversheds Sutherland (US) LLP

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 Part 240

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.

17 CFR Parts 270 and 275

Reporting and recordkeeping requirements; Securities.

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 authorities for §§ 240.17a-14 and 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,

Formatted: Indent: Left: -0.01", First line: 0"

Formatted: Space After: 12.6 pt, Line spacing: Multiple 1.08 li

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 Pub. L. 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 reserved 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~~ law enforcement, intelligence, or cyber security authorities, such as the Cybersecurity and Infrastructure Security Agency ("CISA"), European Union Agency for Cybersecurity ("ENISA"), National Cyber Security Center ("NCSC"), and the Federal Bureau of Investigation ("FBI"), 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)~~(v) ~~The~~ 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;

Commented [S1]: For global incidents, orders from a non-U.S. regulatory or cybersecurity authority should also be included.

Commented [S2]: As the Commission recognized in its proposing release, but declined to implement, "a broader law enforcement exception could generally be expected to enhance law enforcement's efficacy in cybercrime investigations, which would potentially benefit affected customers through damage mitigation and benefit the general public through improved deterrence and increased recoveries, and by enhancing law enforcement's knowledge of attackers' method.

Commented [S3]: As § 248.30(a)(5) does not require contracts or agreements to be entered into, the requirement to maintain policies/procedures under § 248.30(a)(5)(i) seems sufficient.

* * * * *

§ 240.17Ad-7 [Redesignated as § 240.17ad-7]

3. Redesignate §240.17Ad-7 as §240.17ad-7.

4. Amend newly redesignated §240.17ad-7 by:

a. Revising the section heading;

b. Adding a reserved paragraph (j); and

c. Adding paragraph (k).

The revision and additions 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 appropriate ~~the United States Attorney General~~law enforcement, intelligence, or cyber security authorities, such as CISA, ENISA, NCSC, and the FBI, 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)~~(4) ~~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)~~(5) 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

5. 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).

* * * * *

6. 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 (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]

7. Amend § 248.17 in paragraph (b) by removing the words "Federal Trade Commission" and adding in their place "Consumer Financial Protection Bureau" and removing the words "Federal Trade Commission's" and adding in their place "Consumer Financial Protection Bureau's".

8. Revise § 248.30 to read as follows:

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

(a) *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~~may include procedures for the covered institution that are designed 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 customer of the covered institution or third-party financial institution whose sensitive customer information was~~, or is reasonably likely to have been,~~ accessed or used without authorization in accordance with the protocols set forth in paragraph (a)(4)(ii) or (a)(4)(iii) of this section, as applicable, 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~~ When a covered financial institution ~~has determined, after~~becomes aware of a potential or reasonably suspected incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation of the facts and circumstances of the incident ~~of~~to promptly determine the likelihood that the information has been or will be misused and resulted or reasonably would result in substantial harm or inconvenience. If the covered institution determines that the 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~~or 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, and resulted or reasonably would result in substantial harm or inconvenience to the affected individual. 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~~.~~ who are customers of the covered institution.* If an incident of unauthorized access to or use of sensitive customer information has occurred that has or reasonably would result in substantial harm or inconvenience to the affected individual, the covered institution must provide notice to all individuals whose sensitive customer information was accessed or used without authorization, and resulted or reasonably would result in substantial harm or substantial inconvenience to the affected individual, unless those customers belong to third-party financial institutions~~. If~~, in which case the covered institution should follow protocols under paragraph (4)(a)(iii).

~~(ii)~~(iii) *Affected individuals who are customers of a third-party financial institution*. To the extent that the covered institution reasonably determines that sensitive customer information provided by a third-party financial institution ~~, it should provide notice to that third-party financial institution. Then, the financial institution that has a relationship with a customer should have the responsibility and authority to make its own decision on whether the notification should come from the financial institution holding the customer relationship, or request that the covered institution which experienced the relevant incident provide the requisite notice. 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~~was accessed or used without authorization and that such access or use has or reasonably would result in substantial harm or inconvenience, the covered institution ~~is not required to~~should provide notice to ~~that individual under this paragraph~~the third-party financial institution.

~~(iii)~~(iv) *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~~ after the institution concludes, following its investigation, that misuse of customer information has occurred or is reasonably likely to have occurred ~~unless the United States Attorney General determines~~, unless an appropriate law enforcement, intelligence, or cyber security authority, such as CISA, ENISA, NCSC and the FBI, determine that the notice required under this rule would impede active investigations and cooperation with such authority, poses a substantial risk to national security or

Formatted: Indent: Hanging: 0.01"

public safety, ~~and notifies the Commission of~~or otherwise warrants delay. Upon such a 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.~~authority. The notice may be delayed ~~for an additional period of up to 30 days if the Attorney General determines that the notice continues to~~until the relevant law enforcement, intelligence, or cyber security authority determine that the notice would no longer impede active investigations and cooperation with such authorities, 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~~, or otherwise warrant delay ~~is necessary, the Commission will consider additional requests for delay and may grant such delay through Commission exemptive order or other action~~.

~~(iv)~~(v) *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~~suspected to ~~have been~~be 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 one of the following contact ~~information sufficient~~methods 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 electronic method or means, a postal address, ~~and~~or 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 that are designed 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~~a reasonable investigation has been performed by a service provider to determine 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

Commented [S4]: Requiring all service providers to notify covered institutions of a breach in security that results in unauthorized access to a customer information system maintained by the service provider within 72 hours is an unreasonably specific standard to mandate given the wide variety of service providers. This proposed edit would harmonize service provider and covered institution requirements. For instance, the Proposed Interagency Guidance on Third-Party Relationships: Risk Management provides that banking organizations should "adopt third-party risk management processes that are commensurate with the identified level of risk and complexity from the third-party relationships, and with the organizational structure of each banking organization."

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 appropriate ~~the United States Attorney General~~law enforcement, intelligence, or cyber security authorities, such as CISA, ENISA, NCSC, and the FBI, 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)~~(v) 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:~~

~~(i) 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:~~

~~(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) 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) *Customer.* (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) *Customer information.* (i) Customer information for any covered institution other than a transfer agent registered with the Commission or another ARA means any record containing nonpublic, nonencrypted 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, nonencrypted 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)~~(6) *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)~~(7) *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)~~(8) *Sensitive customer information.* (i) Sensitive customer information means ~~any component of customer~~ information ~~alone~~ identifying an individual or the individual's account, including the individual's account number, name or online user name, in ~~conjunction~~combination with ~~any other~~authenticating information~~, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.~~ such as:

~~(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~~

(i) 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;

(ii) A biometric record;

(iii) A unique electronic identification number, address, or routing code~~;~~ that would permit access to a customer's financial account;

(iv) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)); or

(v) ~~(B) Customer~~Similar 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~~, if it 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)~~(9) *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~~.~~, but does not include any (i) affiliates of covered institutions when they are part of the same enterprise information security/oversight, or (ii) financial counterparties to a covered institutions, such as brokers, clearing and settlement firms, and custodial banks.

~~(11)~~(10) *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)).

Formatted: List Paragraph, Indent: First line: 0"

Formatted: List Paragraph, Indent: First line: 0", Space After: 0 pt, Line spacing: single

Formatted: Indent: Left: 0.5", Space After: 0 pt, Line spacing: Double, Numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Indent at: 1"

Commented [S5]: We recommend 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.

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

9. 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.

10. Amend § 270.31a-1 by adding paragraph (b)(13) to read as follows: **§ 270.31a-1 Records to be maintained by registered investment companies, certain majority-owned subsidiaries thereof, and other persons having transactions with registered investment companies.**

* * * * *

(b) * * *

(13)(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~~ appropriate law enforcement, intelligence, or cyber security authorities, such as CISA, ENISA, NCSC, and the FBI, 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)~~(iv) ~~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).

* * * * *

11. 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).

The addition reads 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.

* * * * *

Formatted: Space After: 0.25 pt, Line spacing: Multiple 1.99 li

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

12. 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.

* * * * *

13. 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~~);~~);), including, if applicable, the basis for reliance on reasonable assurances from service providers;

(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~~ appropriate law enforcement, intelligence, or cyber security authorities, such as CISA, ENISA, NCSC, and the FBI, 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.