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