



March 31, 2023

By Electronic Submission

Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: **File No. S7-05-23; Release Nos. 34-97141; IA-6262; IC-34854; File No. S7-05-23; Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information**

File No. S7-06-23; Release No. 34-97142; 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 Transfer Agents

Dear Ms. Countryman:

The Securities Industry and Financial Markets Association (“SIFMA”) hereby requests that the Securities and Exchange Commission (the “Commission”) extend the comment period for the two above-referenced rule proposals (collectively, the “Proposals”): the proposed enhancements to Regulation S-P (“Regulation S-P Proposal”)¹ and the new Rule 10 proposal to address cybersecurity risks to the U.S. securities markets (“Exchange Act Cybersecurity Proposal”).² The Proposals were both introduced on March 15, 2023, along with the proposal to extend the reach of Regulation Systems Compliance and Integrity (“Regulation SCI Proposal”),³ and less than a week after the Commission reopened the comment period for the previously proposed rules for Cybersecurity Risk Management for Investment Advisors, Registered Investment Companies, and Business Development Companies.⁴

¹ Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, Release No. 34-97141, IA-6262, IC-34854 (proposed Mar. 15, 2023).

² 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 Transfer Agents, Release No. 34-97142 (proposed Mar. 15, 2023).

³ Regulation Systems Compliance and Integrity, Release No. 34-97143 (proposed Mar. 15, 2023).

⁴ Reopening of Comment Period for “Cybersecurity Risk Management for Investment Advisors, Registered Investment Companies, and Business Development Companies,” Release Nos. 33-11167, 34-97144, IA-6263, IC-34855 (proposed Mar. 15, 2023).

The comment period for the three new proposals is 60 days from the date of publication in the Federal Register. These proposals collectively represent fundamental and significant changes to the privacy and cybersecurity obligations of market participants. However, the Commission has not provided a sufficient explanation as to how the proposals relate to, or would operate with, each other and the anticipated collective effects if more than one Proposal is adopted, which leaves interested entities to conduct that work themselves. SIFMA therefore requests that the Commission extend the public comment period to at least 120 days after publication in the Federal Register.

The Commission’s proposed rulemaking on cybersecurity issues is extensive, voluminous, and overlapping with current and previous proposals. In the past month, the Commission has published nearly 1,200 pages for the broad suite of three overlapping proposals,⁵ reopened comments on hundreds more pages of overlapping investment advisor cyber proposals,⁶ and considered yet another recently proposed Commission cyber rulemaking for public companies.⁷ All of these proposals need to be addressed and responded to by the same personnel at the same interested parties.

In both Proposals, the Commission has acknowledged that market participants are subject to the overlapping proposals that will need to be reviewed, taken into account, and commented on—that is, “certain types of entities that would be subject to” the Regulation S-P Proposal would also be subject to the Exchange Act Cybersecurity Proposal, and vice versa, as well as being subject to the Regulation SCI Proposal.⁸ The Exchange Act Cybersecurity Proposal also notes that the Commission has several pending proposals to address cybersecurity and related risks.⁹

The Proposals provide some narrative comparison of their requirements,¹⁰ and recognize that financial institutions are also subject to existing requirements to maintain certain relevant policies and procedures.¹¹ After acknowledging the interrelatedness of the Proposals and other

⁵ See *supra* notes 1–3.

⁶ See *supra* note 4.

⁷ Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11038, 34-94382, IC-34529 (proposed Mar. 9, 2022).

⁸ Regulation S-P Proposal, *supra* note 1, at 108 (Section II.G, “Covered Institutions Subject to the Regulation SCI Proposal and the Exchange Act Cybersecurity Proposal”); Exchange Act Cybersecurity Proposal, *supra* note 2, at 220 (Section II.F, “Market Entities Subject to Regulation SCI, Regulation S-P, Regulation ATS, and Regulation S-ID”).

⁹ Exchange Act Cybersecurity Proposal, *supra* note 2, at 22–23 n.52.

¹⁰ Regulation S-P Proposal, *supra* note 1, at 108 (Section II.G, “Covered Institutions Subject to the Regulation SCI Proposal and the Exchange Act Cybersecurity Proposal”); Exchange Act Cybersecurity Proposal, *supra* note 2, at 220 (Section II.F, “Market Entities Subject to Regulation SCI, Regulation S-P, Regulation ATS, and Regulation S-ID”).

¹¹ *E.g.*, Regulation S-P Proposal, *supra* note 1, at 37 n.95 (“Regulation S-ID, among other things, requires financial

regulatory requirements, the Commission encourages commenters to review the suite of cybersecurity-related proposals and how each will affect comments on another proposal.¹² Although the Commission has offered a limited comparative analysis, it has not offered a chart or matrix demonstrating the interrelationship of the Proposals and other related regulations and requirements. This will require interested parties to produce such comparisons themselves to assess duplication, redundancy, and conflicts—an exercise that should be conducted, in the first instance, by the Commission as part of its obligation to focus on harmonization, rationalization, and reconciliation. In other words, the Commission has shifted its planning obligations to the regulated community to undertake on its own. Sixty days after publication is simply too short for SIFMA and others to conduct this exercise and to provide meaningful input.

As Congress has recognized, the issue of managing cybersecurity risks is far too important for a rushed or siloed rulemaking process. The two-year rulemaking timeframe prescribed by Congress for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRCI”) ¹³ provides extensive opportunities for public comment, in the form of a 60-day response period for the Request for Information issued in September 2022, ¹⁴ to be followed by another comment period after publication of the Notice of Proposed Rulemaking.¹⁵ This dual-phased approach is much more likely to yield useful comments than the short timeline the Commission has imposed for the Proposals here.

Additionally, it will be imperative for the Commission to coordinate with CISA and other federal agencies to assure harmonization and deconfliction across cybersecurity-related regulations, rather than require the subjects of the proposed regulations to undertake that process themselves. CIRCI mandates that CISA consult with various entities throughout the rulemaking process, including Sector Risk Management Agencies, the Department of Justice, other appropriate Federal agencies, and establishes a Cyber Incident Reporting Council to “coordinate, deconflict, and harmonize federal incident reporting requirements.”¹⁶ Further, as the recently released National Cybersecurity Strategy emphasizes, regulatory frameworks must

institutions subject to the Commission’s jurisdiction with covered accounts to develop and implement a written identity theft prevention program.”).

¹² Regulation S-P Proposal, *supra* note 1, at 16 (“We encourage commenters to review those other cybersecurity-related rulemaking proposals to determine whether those proposals might affect comments on this proposing release.”); Exchange Act Cybersecurity Proposal, *supra* note 2, at 23 n.52 (“The Commission encourages commenters to review the proposals with respect to Regulation SCI and Regulation S-P to determine whether they might affect their comments on this proposing release . . . The Commission encourages commenters to review the Investment Management Cybersecurity Release and the comments on that proposal to determine whether they might affect their comments on this proposing release.”).

¹³ Pub. L. No. 117-103, 136 Stat. 49 (2022) (codified at 6 U.S.C. §§ 681-681g).

¹⁴ Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, 87 Fed. Reg. 55833 (Sept. 12, 2022),

¹⁵ 6 U.S.C. § 681b(b)(1).

¹⁶ Pub. L. No. 117-103, 136 Stat. 49 (2022) (codified at 6 U.S.C. § 681f).

be “harmonized to reduce duplication.”¹⁷ Thoughtful coordination, deconfliction, and harmonization take time, and cybersecurity proposals should not be pushed through without it. This is particularly true where, as here, the Commission’s prescriptive approach differs significantly from the federal bank regulatory agencies rule that acknowledges the importance of providing flexibility and confidentiality in reporting incidents to the agencies, and minimizing the burden on firms to do so.¹⁸

SIFMA and other commenters need additional time to evaluate the costs, benefits, and effects of these lengthy and overlapping Proposals and the critical interplay among them. Accordingly, SIFMA respectfully requests that the comment period for each Proposal be extended to at least 120 days following the Commission’s publication of the Proposal in the Federal Register.

Sincerely,



Melissa MacGregor
Deputy General Counsel and Corporate Secretary
SIFMA

Cc: The Hon. Gary Gensler, Chair
The Hon. Hester M. Peirce, Commissioner
The Hon. Caroline A. Crenshaw, Commissioner
The Hon. Mark T. Uyeda, Commissioner
The Hon. Jamie Lizárraga, Commissioner

Kenneth E. Bentsen, Jr., SIFMA

Alan Charles Raul, Sidley Austin LLP
Andrew P. Blake, Sidley Austin LLP

¹⁷ White House, National Cybersecurity Strategy 8 (Mar. 2023).

¹⁸ See Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (Nov. 23, 2021) (codified at 12 C.F.R. pts. 53, 225, 304).