June 5, 2023

By Electronic Submission

Vanessa Countryman, Secretary
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 Secretary Countryman,

The Securities Industry and Financial Markets Association ("SIFMA"), SIFMA Asset Management Group ("SIFMA AMG"), Bank Policy Institute ("BPI"), Institute of International Bankers ("IIB"), and American Bankers Association ("ABA"), (collectively, the "associations") appreciate the opportunity to respond to the proposed amendments to Regulation S-P issued by the Securities and Exchange Commission (the "Commission" or "SEC") on March 15, 2023 (the "Regulation S-P Proposal" or the "Proposal").[1] The associations welcome amendments to Regulation S-P to provide further clarity and guidance to its existing rules. Moreover, we appreciate the importance of strong cybersecurity practices for companies and our country, including appropriate notification of cybersecurity incidents to individuals.[2]

The associations recommend that the Commission reconsider, based on the recommendations in this letter, 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. Additionally, the Regulation S-P

[1] Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information Securities, Release Nos. 34–97141; IA–6262; IC–34854, 88 Fed. Reg. 20616 (proposed Apr. 6, 2023). 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. *See* SIFMA Letter to the SEC (Mar. 31, 2023), *available at* https://www.sec.gov/comments/s7-05-23/s70523-20162960-332927.pdf. The Commission failed to extend the comment deadline or otherwise respond to SIFMA's letter. The SEC's rushed proliferation of cybersecurity rulemakings is detrimental to sound policymaking in this crucial area and is not fair to regulated entities and other interested parties.

[2] *See Cybersecurity Resources*, SIFMA, *available at* https://www.sifma.org/resources/cybersecurity-resources/; *SIFMA Statement on Completion of Quantum Dawn VI Cybersecurity Exercise*, SIFMA (Nov. 18, 2021), *available at* 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), *available at* https://www.sifma.org/wp-content/uploads/2022/04/SIFMA-and-AMG-Comment-Letter-on-SEC-Cybersecurity-Proposals.pdf; Letter from SIFMA to the SEC (May 9, 2022), *available at* https://www.sifma.org/wp-content/uploads/2022/05/SIFMA-Comment-S7-09-22-May-9-2022.pdf.

Proposal could be improved by taking into account the Commission's other proposals related to cybersecurity, a covered institution's need to comply with existing data breach notification laws, and the benefit of coordinating with law enforcement, cybersecurity, intelligence, and national security agencies during a security incident.

I. Executive Summary

The Commission should consider the Regulation S-P Proposal in light of several considerations:

- **Harmonize and deconflict the Regulation S-P Proposal with other proposals and requirements**. The SEC should provide guidance for the industry with specific clarity on how the Regulation S-P Proposal will interact with the Rule 10 Proposal and other similar cybersecurity proposals. While the Commission's narrative does discuss the overlap between the proposals, it does not provide a clear roadmap to navigate the varying terms and processes of the proposals—and other cybersecurity rules imposed on the securities industry by the SEC, as well as various cybersecurity requirements imposed by other agencies.

- **Clarify the scope of service providers and permit flexibility in, and additional time to execute, service provider contracts**. The Commission should reconsider its broad definition of service provider and not impose a one-size-fits-all approach for service provider contracts and notification. Additionally, covered entities should have more than 12 months following the finalization of the Regulation S-P Proposal to renegotiate all of their contracts, as the process of negotiation, and potentially finding new service providers, will be time consuming, disruptive, and costly.

- **Retain the proposed risk-of-substantial-harm provision**: The associations agree that notification is not required if a covered 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." This standard is largely consistent with the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("Interagency Guidance") and with many state data breach laws which are designed to avoid over-notification to customers. However, notification should only be required if the covered institution affirmatively finds substantial harm or inconvenience to further align with the Interagency Guidance. The Commission should also list the specific data elements that are sensitive enough to trigger the notification requirement, subject to the risk-of-substantial-harm standard.

- **Eliminate the arbitrary 30-day notification requirement**. The Commission should eliminate the 30-day notification requirement, which represents an arbitrary and entirely insufficient amount of time for covered institutions to perform investigation and risk

assessments, collect and analyze the information necessary to generate customer notices, and provide notices in complex cases.

- **Broaden the national security exception to include a law enforcement and cybersecurity agency exception, including foreign counterparts**. The proposed national security notification exception should be expanded to include cooperation with 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 federal government resources early during a cyber-related incident and reflect the White House directive which identified CISA, the FBI, and the intelligence community as being responsible for investigating cyber incidents.[3] A covered entity should not be required to make a Reg S-P data breach disclosure when the FBI or a state law enforcement agency is requesting a delay, or where a court order requires delay in public disclosure.

- **Do not require that a covered institution or transfer agent provide notice to customers with whom it does not have a preexisting relationship**. A covered institution or transfer agent should 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 or transfer agent 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.

II. Incident Response Program

A. The Commission Should Clarify the Scope of Service Providers. (Requests for Comment 17, 19, 23)

"Service providers" is broadly defined in the proposed Regulation S-P to mean any person or entity that is a third party and receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution; and as drafted, would include affiliates of covered institutions if they are permitted access to this information through their provision of services. This definition is substantially similar to the definitions adopted by the banking agencies and the Federal Trade Commission ("FTC") in their respective safeguard rules, as well as the customer breach notification guidelines adopted by the banking agencies in 2005. However, the associations request that the Commission clarify the scope

[3] Executive Order on Improving the Nation's Cybersecurity (May 12, 2021), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

of service providers, including whether service providers would include financial counterparties such as brokers, clearing and settlement firms, and custodial banks. 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.

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 48 hours is an unreasonably specific standard to mandate given the wide variety of service providers. Instead, the Commission should require service providers to provide notification to a covered institution without unreasonable delay after a reasonable investigation has been performed by the service provider, which 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."[4]

B. The Commission Should Permit Flexibility in Service Provider Contractual Requirements. (Requests for Comment 21, 22, 24, 25, 26)

The associations agree with the Commission 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 to a covered institution in the event of certain types of breaches in security.

However, the regulation should not include explicit requirements prescribing specific appropriate measures. Different service providers will require different types of contractual protections—and service providers that access sensitive customer information may need more granular security requirements than those that only handle limited sensitive customer information or none. The Commission should consider alternatives to mandating contractual requirements, such as permitting a covered institution to rely on "reasonable assurances" from service providers such as email, customer relationship management, cloud, and other technology vendors that they have taken appropriate measures to protect customer information, including but not limited to notification to the covered institution as soon as possible in the event of any breach in security resulting in unauthorized access to a customer information system.

Under the current proposed Regulation S-P amendments, covered institutions would be limited in which service providers they can choose, as some service providers, particularly those that handle limited customer information, would be unwilling to provide such contractual commitments and may choose not to enter into unduly burdensome contracts with covered

[4] Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 FR 38182, 38184 (proposed July 19, 2021).

institutions. The associations would expect to see significant pushback from their service providers due to these proposed provisions. Accordingly, we recommend the Commission remove its 48-hour deadline for notification provision, and instead require notification to be given without unreasonable delay. That language would be consistent with the phrasing under Article 33 of the General Data Protection Regulation ("GDPR") which requires "processors" to notify of a breach "without undue delay," and which is increasingly used in contracts with large service providers.

Additionally, the Regulation S-P Proposal's definition of "customer information system" is broad, and its service provider obligations should focus on "customer information" as opposed to the systems on which customer information is stored. In the context of a multi-tenant software as a service provider, for instance, the provider would not want to provide notice when there is no reason to think that any data was exposed. Such a requirement could also lead to over-notification, which may overburden the information security teams of both the service provider and the covered institution. The associations suggest the Commission limit service provider obligations to incidents involving unauthorized access to or use of "customer information"; and, at a minimum, the associations request the Commission clarify the definition of "customer information system," and the scope of notification obligations involving such a system. The SEC is proposing to use a definition that is broader than the banking agencies.[5] As above, the associations respectfully request that the SEC explain why it believes it is more appropriate to take a more expansive and burdensome view than other regulators have.

Finally, the Regulation S-P Proposal may overlap with the proposed Oversight Requirements for Certain Services Outsourced by Investment Advisers, and the associations request that the Commission review and harmonize these two standards.[6]

C. The Commission Should Provide Additional Time to Implement Contractual Requirements. (Requests for Comment 105, 106)

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. For instance, if a service provider indicates it will not revise its contract to provide notification within 48 hours of a security incident (which many service providers may be unwilling to do), a firm would have to take the time to engage another vendor and conduct standard vendor due diligence on such a service provider, which may not be feasible within 12 months. In practice, revising agreements and addendums can take well over 12 months due to the number of providers, conducting new or additional due diligence, delays in provider responses, and redlining/negotiations. Additionally, this obligation could cause a ripple effect if a service provider engages another service provider and has to ensure such contractual obligations are followed. These contractual obligations will also conflict with

[5] *See, e.g.*, 12 CFR Part 364, App. B, at para. I.C.2.f ("Customer information systems means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.")
[6] Proposed Outsourcing by Investment Advisers, 87 FR 68816 (proposed Oct. 26, 2022).

several other recently enacted laws which impose requirements for institutions to repaper contracts, such as the California Consumer Privacy Act and the New York Department of Financial Service's Cybersecurity Regulation. 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.

To the extent the SEC calls for contractual requirements for service providers, it should be guided by the banking agencies and the FTC, none of which mandate specific contract terms or a notification deadline. Twelve months to comply regarding service provider contracts is not consistent with the requirements imposed by banking agencies and the FTC; the banking agencies published their safeguards regulations in February 2001, with an overall effective date of July 2001 and existing contracts with service providers grandfathered until July 2003; and the FTC's original safeguards regulation was published in May 2002, with an overall effective date of May 2003, and existing contracts with nonaffiliated service providers grandfathered until May 2004. It would be helpful to obtain an explanation for why the SEC has departed from the banking agencies' and the FTC's requirements here. The SEC should consider either a longer time period for the implementation of its contractual requirements, or a phased implementation that takes into consideration the sensitivity and criticality of service providers.

III. Notice to Affected Individuals

A. The Standard for Providing Notice Should Include a Risk-of-Substantial-Harm Provision that Aligns with the Interagency Guidance (Requests for Comment 28, 29, 30, 31)

The associations agree that a risk-of-substantial-harm provision should be included in the standard for customer notification, although it recommends that the standard be harmonized further with the Interagency Guidance and with many state laws so as to require notification only if the covered institution affirmatively finds risk of harm. The Commission should avoid requiring covered institutions to prove a stringent negative, which could lead to excessive and unnecessary notifications to consumers where a low likelihood of harm is present. This, in turn, 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.

As discussed above, the Commission should consider stating specific data elements that could constitute sensitive customer information—i.e., those that could result in substantial harm or inconvenience, such as those that would lead to identity theft. The proposed risk-of-substantial-harm provision would not require notification if a covered 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." This type of risk-of-substantial-harm provision,

which limits unnecessary and burdensome notifications that could confuse consumers, is now routinely used by numerous other federal and state regulators. For example, the majority of data breach laws in the United States contain express risk-of-harm provisions that exempt an entity from notifying a customer or regulator of low-risk security incidents. In the European Union, under Article 34 of the GDPR, controllers need not notify individuals of a personal data breach where the incident is "unlikely to result in a *high risk* to the rights and freedoms" of the affected individuals.[7]

The associations would caution against attempting to define "substantial harm or inconvenience," much less to delve into concepts unrelated to identity theft, the means to access an account without authority, or other tangible harms. The trigger for the proposed required notice sensibly turns on preventing identity theft and safeguarding financial accounts from unauthorized access. Although an impacted customer may claim, for example, that the disclosure of his or her name and salary has damaged their reputation, those types of disclosures would not constitute substantial harm that triggers a notifiable breach under the Interagency Guidance or the laws of any state.

However, the standard should be further harmonized with the Interagency Guidance, where the presumption should be that a covered institution does not need to notify customers absent an affirmative determination of harm.[8] As the Proposing Release recognizes, "[t]wenty-one states have a presumption *against* notifying customers of a breach, and only require notice if, after investigation, the covered institution finds risk of harm." The Interagency Guidance only requires notification if a financial institution affirmatively determines that misuse of information has occurred or is reasonably possible. The banking agencies specifically rejected a "proposed threshold [that would have] inappropriately required institutions to prove a negative proposition, namely, that misuse of the information accessed is unlikely to occur."[9] The Commission should do the same and require an affirmative determination that there is a risk of harm in order to notify individuals of a breach.

By providing a risk-of-substantial-harm provision in Regulation S-P, the Commission will provide covered institutions with additional flexibility in making appropriate judgments on whether to notify individuals of a breach. Covered institutions will already evaluate customer notification under applicable state and federal breach laws, and providing a risk-of-substantial-harm provision in Regulation S-P will give covered institutions additional time to respond and mitigate an incident as opposed to spending time deliberating over notification obligations. A risk-of-substantial-harm provision allows for a reasonable investigation to be conducted and

[7] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 (emphasis added).

[8] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736, 15743 (Mar. 29, 2005).

[9] *Id.*

notification to be provided when appropriate. Moreover, the Commission should follow the standard set by numerous state data breach laws and clarify that notification is not required if there is a good faith acquisition by an employee or agent of a covered institution or similarly situated personnel, so long as personal information is not otherwise misused or subject to further unauthorized disclosure. Specifically, the "good faith" exception should not require notice when customer information is acquired by an employee or agent of a covered institution, or by personnel of service providers with relevant confidentiality requirements, or another institution subject to the Gramm-Leach-Bliley Act ("GLBA"), so long as there is no unauthorized use or disclosure of the customer information.

Finally, covered institutions should be able to perform a reasonable investigation in order to assess risk of harm, with flexibility in how they conduct the investigation. This approach aligns with the approach applicable to banks under the Interagency Guidance which provides that "when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused."[10]

B. The Commission Should Define "Sensitive Customer Information" More Clearly and Consistent with Other Federal and State Breach Standards. (Requests for Comment 37, 42)

The Commission should list the specific data elements that are sensitive and could trigger notification (rather than leaving an open-ended standard while just offering potential examples of such data elements). This, again, would be consistent with the approach of the banking agencies in their Interagency Guidance. Specifically, sensitive customer information should consist of an individual's name in combination with another specified data element that the Commission agrees upon, such as a Social Security number, driver's license or state ID number, or financial account number with the required security code, access code, personal ID number, or password that can be used to access the customer's financial account. Most simply, the Commission could adopt the definition of "sensitive customer information" in the Interagency Guidance, which "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."[11]

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. This would incentivize organizations to leverage encryption to protect their customers' data, thereby reducing their breach risk. Additionally, information that is publicly

[10] *Id.* at 15752.
[11] *Id.*

available (independent of the incident) should also be exempted, as this does not pose a new risk of harm and is consistent with state data breach notification laws.

C. Covered Institutions Should Not Be Required to Provide Notice to Customers of Other Financial Institutions. (Request for Comment 51)

The proposed rule would require covered institutions to provide notice to each affected individual, including customers of other financial institutions where information has been provided to the covered institution. Doing so would be impractical, inappropriate, and likely to confuse customers. Even assuming that a covered institution would be able to identify and be able to contact customers of third-party financial institutions, such notification may cause confusion to customers, either causing unwarranted concern over why the covered institution has their data or causing customers to disregard the notification because they believe it was mistakenly sent to them. Instead, the covered institution should provide notice to the financial institution that provided the sensitive customer information. 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.[12]

D. Notification Should Be Required Within a Reasonable Timeframe. (Requests for Comment 52, 54, 55)

The associations recommend that the Commission eliminate the 30-day notification requirement, which represents an arbitrary and entirely insufficient amount of time for covered institutions to perform investigations and risk assessments, collect the information necessary to include in customer notices, and provide notices in complex cases. The Commission should conform its notice requirements for covered institutions to the requirements under the Interagency Guidance, which requires notice as soon as possible after the institution concludes, following investigation, that misuse of customer information has occurred or is reasonably possible. As the Regulation S-P Proposal recognizes, the majority of state data breach notification laws do not specify a number of days to report a breach, and instead include a variation of the Interagency Guidance regarding a reasonable timeframe.[13] Those states that do have a time frame, often have an exception allowing for compliance with the GLBA in lieu of adherence to their time frames. Such a flexible standard would permit appropriate enforcement in both simple cases—where notification in less than 30 days may be appropriate—and more complex cases—where it may take

[12] This approach should also be taken to cover transfer agents. Although we understand that "customer information" in the context of transfer agent means information of the securityholder, the customer of the transfer agent with which it has contractual privity is the issuer of securities. Therefore, the transfer agent should only be required to notify the issuer of the relevant incident.

[13] Regulation S-P Proposal at 20656–57.

significantly longer to identify the appropriate notice population and prepare and deliver notification. The Commission should harmonize its approach to timing with these other agencies.

If the Commission were to keep the 30-day timeframe, the associations encourage the timing to run from the completion of a reasonable investigation and conclusion of the incident response process, rather than from when the covered institution becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred. The Commission should be aware that, in many incidents, victim entities require time after becoming aware of an incident to engage in system and data analysis to determine what data was impacted and what individuals were affected. For instance, in May 2023, the United States Department of the Interior notified federal agency employees, including Commission employees, of a security incident that it discovered in January 2023 that resulted in the unauthorized access of federal agency employees' personally identifiable information. It took approximately four months from the discovery of unauthorized access of information for Commission employees to receive notice of the incident. We assume that the SEC and the Department of the Interior, the SEC's service provider, took four months to notify SEC employees because that amount of time was necessary to respond to this incident, conduct the necessary data analytics, and execute the data breach notification. Had notification been required sooner, the notice could have provided incomplete information, and caused unnecessary concern. The Commission should follow this approach in the Regulation S-P Proposal, and only require notification after the completion of a reasonable investigation and conclusion of the incident response process.

E. Notification Should Be Subject to a Broader Law Enforcement/Government Agency Exception. (Requests for Comment 56)

The associations agree with the proposed inclusion of an exception to delay customer notification upon request by the Attorney General. However, this exception is far too narrow, and practically unfeasible, as it would permit the delay of customer notification only if a covered institution receives a "written request from the Attorney General of the United States that the notice required under this rule poses a substantial risk to national security." As the Commission has recognized, "a broader law enforcement exception could generally be expected to enhance law enforcement's efficacy in cybercrime investigations, which would potentially benefit affected customers through damage mitigation and benefit the general public through improved deterrence and increased recoveries, and by enhancing law enforcement's knowledge of attackers' methods."[14] Close cooperation and collaboration with law enforcement (and cybersecurity-focused agencies)—not only for national security purposes, but also for law enforcement more broadly—is key to successful incident response, and disclosure of information related to the incident while

[14] Regulation S-P Proposal at 20674.

an active investigation is ongoing could impede the investigation or other important governmental objectives.[15]

The associations encourage the Commission to expand its law enforcement exception to include active investigations and cooperation with law enforcement and cybersecurity agencies, as well as those responsible for national security, and compliance with court orders that may preclude public disclosure. The Attorney General cannot be expected to address every law enforcement issue that other agencies are working on, and the Attorney General's involvement—and a nexus with national security—should not be a pre-requisite for a delay in notification for purposes of cooperating and accommodating law enforcement and other appropriate agencies. The Commission should also permit exceptions where required for "responsible disclosure" that necessitates delay of public disclosure of vulnerabilities until remediation of those vulnerabilities is available.[16]

Moreover, the associations encourage the Commission to expand the range of law enforcement agencies that can provide a law enforcement exception and recommend that the Commission include at least the Cybersecurity and Infrastructure Security Agency ("CISA") and the Federal Bureau of Investigation ("FBI"), as well as applicable state and local law enforcement, as well as contemplating coordination with international counterparts in law enforcement, cybersecurity, and security. 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. However, in the limited cases where government agencies or courts do call for delay, the SEC should respect their expertise and authority. Other authorities on Team Cyber are directly charged with protecting national security and criminal investigations and assuring responsible disclosure that will protect potentially exposed companies, entities, and individuals from cyber damage until suitable remediation is available.

F. Covered Institutions Should Have Flexibility in Notice Content and Format. (Request for Comment 61)

The Regulation S-P Proposal would require customer notifications to include contact information sufficient for an individual to contact the covered institution, which the Commission states should include "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." While the associations agree that contact

[15] For example, the Interagency Guidance provides that: "Customer notice may be delayed 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." Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736, 15752.

[16] *See* Coordinated Vulnerability Disclosure Process, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, available at https://www.cisa.gov/coordinated-vulnerability-disclosure-process.

information should be included in customer notifications, covered institutions should have flexibility in determining the contact information to provide, based on how they normally interact with their customers. The associations encourage the Commission to revise its requirement to only require one of the above contact methods.

IV. Safeguards and Disposal Rules Definitions and Coverage

A. The Scope of Customer Information in the Safeguards Rule Is Appropriately Narrow. (Request for Comment 74)

The Safeguards Rule is calibrated appropriately and should not extend to consumer information that is not customer information, including information from a consumer report about an employee or prospective employee. Employee information should not be considered consumer information under Regulation S-P. Rather, consistent with the approach of the banking agencies and the FTC, consumer information should be limited to customer information—that is, information that actually related to an account with the covered institution.

B. The Safeguards and Disposal Rules Should Cover Transfer Agents that Are Registered with the Commission. (Requests for Comment 83, 84)

The associations agree that protections should be in place for transfer agents that are registered with the Commission. However, expanding the safeguards and disposal rules to apply to all transfer agents, regardless of whether they are registered with the Commission, extends beyond the scope of the Commission's authority and could result in regulatory confusion. Transfer agents registered with an appropriate regulatory agency that is not the Commission could be subject to conflicting data security requirements from those regulators.

V. The Commission Should Extend the Compliance Date. (Requests for Comment 105, 106)

The associations recommend that the Commission extend the compliance date for both larger and smaller covered institutions, as the time for compliance may not suffice for many of them. We request the Commission reconsider extending this time period to at least 24 months, given the considerable amount of work a firm would need to undertake to comply with these rules, which would include reviewing an incident response program, incorporating the customer notification requirements into existing policies and procedures, and overhauling each service provider contract, which could require finding new service providers that will comply with the Commission's requirements, conducting due diligence, and negotiating contracts. To the extent that the Proposal deviates from the Interagency Guidance and from state data breach laws, it will take covered institutions even more time to identify those differences and adapt to meet new SEC requirements.

***

The associations appreciate the Commission's attention to cybersecurity and absolutely 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 respectfully submit the Regulation S-P Proposal contains too many overly prescriptive, duplicative, and burdensome requirements on covered institutions. The Commission should focus on 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.

Accordingly, the associations respectfully submit that the Commission should reconsider the Regulation S-P Proposal in accordance with the considerations described above. 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
Bank Policy Institute
Institute of International Bankers
American Bankers Association

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
Dr. Haoxiang Zhu, Director, Division of Trading and Markets

Jen Easterly, Director, CISA
Eric Goldstein, Executive Assistant Director for Cybersecurity, CISA

Graham Steele, Assistant Secretary for Financial Institutions,
U.S. Department of the Treasury

Todd Conklin, Deputy Assistant Secretary – Cybersecurity and Critical
Infrastructure Protection, U.S. Department of the Treasury

Brian Peretti, Director, Domestic and International Cybersecurity Policy,
U.S. Department of the Treasury

Christopher Wray, Director, FBI
Bryan Vorndran, Assistant Director, Cyber Division, FBI

Richard Revesz, Administrator, Office of Information and Regulatory Affairs, US Office for Management and Budget

James J. Halpert, General Counsel, Office of the National Cyber Director

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

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 **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: Tabitha Edgens, Senior Vice President and Senior Associate General 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: Beth Zorc, Chief Executive Officer

The **American Bankers Association ("ABA")** is the voice of the nation's $23.7 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2.1 million people, safeguard $18.7 trillion in deposits, and extend $12.2 trillion in loans.

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