INVESTMENT COMPANY INSTITUTE

1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

May 23, 2023

Ms. Vanessa Countryman, Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC, 20549-1090

Re: Proposed Revisions to Regulation S-P;
File No. S7-05-23

Dear Ms. Countryman:

The Investment Company Institute[1] supports the U.S. Securities and Exchange Commission's proposal to supplement the requirements of Section 248.30 of Regulation S-P, which govern safeguarding of customer information, to require "covered institutions"[2] to have more detailed and rigorous programs providing for the protection of customer information and to provide breach notices in the event of unauthorized access of sensitive customer information.[3] We commend the Commission for both pursuing these amendments and for patterning these new requirements with those of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (the "Interagency Guidelines") adopted by the federal banking regulators.[4] The Interagency Guidelines implemented the provisions from Section 501(b) of the Gramm-Leach-Bliley Act (the "GLB Act") that require financial institutions to implement information security standards. Our current support for the Commission's amendments to Regulation S-P is consistent with our support for similar amendments proposed in 2008 by the Commission. As we noted in our 2008 letter, aligning the SEC's requirements with the Interagency Guidelines

[1] The Investment Company Institute (ICI) is the leading association representing regulated investment funds. ICI's mission is to strengthen the foundation of the asset management industry for the ultimate benefit of the long-term individual investor. Its 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 Europe, Asia, and other jurisdictions. Its members manage total assets of $29.1 trillion in the United States, serving more than 100 million investors.

[2] The term "covered institution" would include any broker, dealer, investment company, investment adviser, or transfer agent registered with the Commission.

[3] *See Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information,* SEC Release Nos. 34-97141, IA-6262, IC-34852 (March 22, 2023) (the "Release").

[4] *See* 66 FED. REG. 8816 (February 1, 2001).

"will facilitate compliance by our members that are also subject to such regulators' jurisdiction."[5] Further, such an approach promotes a more coherent framework and will better serve the goals of the government and its agencies.

Executive Summary

The Institute supports adoption of the proposed amendments but recommends that the Commission:

- Expand the scope of Regulation S-P to include any cybersecurity risk management programs the Commission requires of covered institutions;
- Revise the timing of the breach notices to accommodate law enforcement investigations;
- Delete the timing of a breach incident from the breach notice's contents;
- Revise the definition of "sensitive customer information" to clarify its meaning;
- Provide a 24-month compliance period;
- Provide registrants a notice when the SEC's systems are breached; and
- Avoid including statements in the adopting release that might result in regulation by enforcement when enforcing compliance with the rule's requirements.

1. Broadening the Scope of Regulation S-P to Include Cybersecurity Requirements

While the Institute supports the proposed amendments to Regulation S-P to enhance the protection of non-public personal information ("NPPI") maintained by covered institutions, we strongly recommend that the amendments include within the regulation's scope any regulatory requirements relating to cybersecurity that the SEC imposes on registrants. This expansion is appropriate due to the interconnectedness of data safeguards, cybersecurity, and breach notices, all of which are within the scope of Regulation S-P. Addressing these issues in a single regulation will avoid a disjointed and disparate approach where there are related provisions on the same topic adopted in different rules under the federal securities laws.[6] Consolidating these

[5] *See* Letter from the undersigned to Ms. Nancy Morris, Secretary, US Securities and Exchange Commission, dated May 2, 2008 commenting on *Regulation S-P: Privacy of Consumer Information and Safeguarding Personal Information,* SEC Release Nos. 34-57427 and IA-2712, 73 FED. REG. 13692 (March 2008)(the "Institute's 2008 Letter"). The Institute's 2008 Letter supported the amendments the Commission proposed to Reg. S-P. Following publication of this proposal, no further action was taken on it.

[6] William Birdthistle, Director of the Division of Investment Management, recently commented on the connection between electronic records and the need to notify individual's when those records are compromised:

requirements in Regulation S-P is a superior approach and will better serve the Commission's goals and the public.

1.1. Regulation S-P is the Appropriate Vehicle to Address Cybersecurity

Regulation S-P was originally adopted by the SEC in 2000 to implement Section 501 of 1999's GLB Act. Section 501 of the GLB Act provides as follows:

> SEC. 501. [15 U.S.C. 6801] **PROTECTION OF NONPUBLIC PERSONAL INFORMATION.**
> (a) PRIVACY OBLIGATION POLICY.—It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.
> (b) FINANCIAL INSTITUTIONS SAFEGUARDS.—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
>
> (1) to insure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Under the GLB Act, federal regulators of financial institutions, including the SEC,[7] were directed by Congress to work together, through joint rulemaking initiatives, to implement the Act to ensure the consistent protection of individuals' NPPI without regard to what type of institution

---

> For asset managers, . . advancement in digital communications, information storage tools, and other technologies have simplified the ability of firms to obtain, share, and maintain individuals' personal information. While this technological progress may offer certain benefits, this evolution also has changed – or perhaps even exacerbated – risks of unauthorized access to or use of personal information. The proposed amendments to Regulation S-P would respond to these threats by requiring registered investment advisers to adopt written policies and procedures for incident response programs that address unauthorized access to or use of customer information and would require timely notification to individuals affected by an information security incident.

See Remarks at the ICI Investment Management Conference, William Birdthistle (March 20, 2023).

[7] These regulators included, among others, the Board of Governors of the Federal Reserve System (the "Federal Reserve"), the Office of the Comptroller of the Currency ("OCC"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of Thrift Supervision ("OTS"). *See* Section 505 of the GLB Act.

held such NPPI. In response to this directive, the SEC adopted Regulation S-P to require the safeguarding of NPPI.

Like Regulation S-P, when the Interagency Guidelines were adopted in 2001, their focus was on safeguarding NPPI.[8] Since then, these Guidelines have been amended to address other issues relating to data security, including cybersecurity and breach notices. In 2005, the Interagency Guidelines were revised to add Appendix A to require institutions to have cybersecurity response programs for unauthorized access to customer information. The cybersecurity risk management programs proposed by the Commission last year for investment companies and investment advisers and for broker-dealers and transfer agents this year were patterned after the Interagency Guidelines.

1.2 The Commission Should Address Data Security Issues Holistically

We believe the Interagency Guidelines' holistic approach to banking institutions' data safeguards, cybersecurity, and breach notices is superior to a multiple, separate rules approach to impose similar regulatory requirements. Under the SEC's construct, registrants will have an obligation to safeguard information under Regulation S-P and, if that information is breached, Regulation S-P would require the registrant to notify the individual of a compromise of the individual's NPPI. But, the rules governing how these registrants maintain and protect the NPPI from a cyber intrusion will not be in Regulation S-P. Instead, to find those requirements, one must first identify the type of entity maintaining the NPPI. If it is an investment company, the SEC has proposed to regulate that information under a new rule, Rule 38-2 under the Investment Company Act of 1940. If it is an investment adviser, proposed Rules 204-6 and 206(4)-9 would govern the adviser's cyber information. If it is a broker-dealer or a transfer agent, proposed Rule 242.10 under the Securities Exchange Act of 1934 would be the operative provision.[9]

The Commission's multiple rule approach to addressing these issues was commented on during the Commission's March 15, 2023 open meeting in which the Commission proposed (i) amendments to Regulation S-P, (ii) a cybersecurity risk management program for broker-dealers and transfer agents, and (iii) a re-publication of last year's cybersecurity risk management program for investment companies and investment advisers. Commissioner Peirce observed:

> . . . let me make one comment that applies to all the rules before us today. The proposed expansion of Regulation SP is one of three cybersecurity and systems-protection proposals we are considering today. Regulation SP overlaps and intersects with each of the others, as well as with other existing and proposed regulations – *e.g.*, the cybersecurity rule for investment advisers, investment companies, and business development companies, and

[8] *See* 66 FED. REG. 8816 (February 1, 2001).

[9] As discussed in more detail below, if an investment company or investment adviser violates the proposed cybersecurity rule, they would be engaging in fraudulent activity. Identical violations by a broker-dealer or transfer agent under Rule 242.10 would not be considered fraud.

> the recently proposed investment adviser outsourcing rule. The release does not try to hide these facts, and actually goes into considerable detail about the redundancies, but then it simply declares them appropriate given the different purposes, that they are 'largely consistent,' and probably not 'unreasonably costly.' Admittedly, rationalizing these overlapping requirements would be hard. To paraphrase John Kennedy when addressing another difficult challenge, the Commission should choose to harmonize and synthesize these rules not because it is easy, but because it is hard, because the goal will serve to organize and measure the best of our energies and skills, because the challenge is one that we are willing to accept, one we are unwilling to postpone.[10]

Commissioner Mark T. Uyeda identified concerns with conflicts and confusion resulting from multiple regulations addressing information security:

> In addition, today we are considering two other proposals that overlap with this proposal [*i.e.*, the proposed cybersecurity management program rule for broker-dealers and other market entities]: amendments to Regulation SCI and Regulation S-P. Regulation S-P would require policies and procedures to address certain types of cybersecurity risks. . . . [It] would similarly require notifications sent to customers and others about cybersecurity incidents.
>
> Make no mistake about it: cybersecurity is an incredibly important topic and the potential for harm to market participants and investors is significant, and to the markets and economy as a whole. It is crucial that there is a clear regulatory framework to address cybersecurity. The Commission's 'spaghetti on the wall' approach with these overlapping and potentially inconsistent regulatory regimes can create confusion and conflicts, and could even weaken cybersecurity protections. While the proposals acknowledge the possibility of potential overlap, they fail to address those concerns and simply ask commenters to specifically identify areas of duplication and costs. A preferable approach would have been to propose a set of coordinated rules and to consider those costs and benefits both individually and as a package.[11]

---

[10] *See Statement on Regulation SP: Privacy of Consumer Financial Information and Safeguarding Customer Information*, Commissioner Hester M. Peirce (March 15, 2022) available at https://www.sec.gov/news/statement/peirce-statement-regulation-sp-031523.

[11] *See Statement on the Proposed Cybersecurity Risk Management Rule for Market Entities*, Commissioner Mark T. Uyeda (March 15, 2023), available at https://www.sec.gov/news/statement/uyeda-statement-enhanced-cybersecurity-031523. Because the SEC has elected to propose separate rules to address these issues, in addition to filing this comment letter on the proposed amendments to Regulation S-P, the Institute will also be filing comment letters on the proposed cybersecurity rule for market entities and on the SEC's republication of the proposed cybersecurity rule for investment companies and investment advisers. As with this letter, in each of those letters, ICI will include commentary expressing concern with the Commission's proposed disjointed approach to address

We concur with the views of Commissioners Peirce and Uyeda and recommend that, consistent with the tested approach taken by the federal banking regulators in the well-established Interagency Guidelines, the Commission address these issues holistically in one regulation – Regulation S-P.

1.3 The Advantages of the Interagency Guidelines' Holistic Approach

We believe the holistic approach of the Interagency Guidelines is preferable to the SEC's proposed approach of adopting a variety of rules under the various securities laws to impose substantially similar requirements. Aside from the logic of combining related provisions in one regulation, another advantage of our recommended holistic approach is that the requirements will apply uniformly. As proposed by the Commission, while all covered institutions will be subject to the same regulatory requirements applicable to safeguarding customer information, providing breach notices, and disposing of NPPI, the SEC has proposed disparate rules for different SEC registrants as they implement new cybersecurity requirements. For example, as noted above, if a fund were to violate their proposed cybersecurity rule (Rule 38a-2), the fund would be deemed to be engaging in fraud. The same would not be true of a broker-dealer or transfer agent that violates their proposed cybersecurity program rule (Rule 242.10). This disparity in treatment is unnecessary, confusing, and serves no public purpose. It can be avoided by incorporating any provisions addressing registrants' cybersecurity risk management programs into Regulation S-P, where they could be applied to all registrants consistently with other regulatory provisions governing data security.

1.4 The Advantages of Addressing Data Security Holistically

We appreciate that the Commission is seeking to address complicated issues through the Regulation S-P and cybersecurity risk management program proposals and commend the Commission for its interest in addressing these issues. We strongly recommend, however, that the SEC rethink its disparate approach to protecting individuals' information and instead, like the Interagency Guidelines, protect such information holistically and more uniformly in Regulation S-P. Such an approach would ensure that:

(i) SEC registrants' responsibilities would not be dependent upon how the registrant is registered with the SEC;

(ii) All provisions relating to protection of customer information – whether in paper or electronic form – including its disposal and breach notices would be easily found in one regulation. This would obviate the need for registrants to review a variety of rules under the Investment Company Act, the Investment Advisers Act, and the Securities Exchange Act of 1934 to determine the applicable law; and

---

the safeguarding of individual's NPPI, the proper disposal of NPPI, breach notices, and cybersecurity risk management programs. Those letters, too, will recommend that the Commission harmonize those requirements into Regulation S-P.

(iii) A violation of the Regulation would be sanctioned the same for all registrants based on the facts and circumstances of the violation and not as fraudulent conduct if the violator is an investment company or investment adviser and as non-fraudulent conduct if the violator is a broker-dealer or transfer agent.

Also, a holistic approach should facilitate both registrants' compliance with these requirements and the Commission's efforts to consistently enforce them. Customers and investors also would be better served by a more coherent and less confusing regime.

Our recommendation is consistent with our April 2022 comments on the SEC's proposed cybersecurity risk management program rule. That letter recommended that the Commission address cybersecurity risks in Regulation S-P and noted that, among other advantages of this approach, it would subject broker-dealers and transfer agents to a uniform set of cybersecurity regulations.

2. The Institute Supports the Adoption of the Amendments Proposed to Regulation S-P

The Institute supports the amendments the SEC has proposed to Regulation S-P. We believe expanding the regulation's scope to include transfer agents and to require breach notices is long overdue. As noted above, our support today is consistent with our approach for revisions to Regulation S-P in 2008[12] and with recommendations we made last year when we commented on the SEC's proposed cybersecurity risk management program rule for investment companies and investment advisers.[13]

We are pleased that, in drafting the proposed amendments to Regulation S-P, the Commission strove to ensure that they were "consistent with the components of a response program" required by the Interagency Guidelines.[14] Consistency between the Commission's regulatory requirements and those of the federal banking regulators is appropriate for the totality of the financial services industry and their customers and clients. Indeed, it is not uncommon for entities subject to the Commission's requirements to have a parent, subsidiary, or affiliate that is regulated by federal banking regulators. In a global and interconnected financial services industry, greater consistency of regulatory requirements in this area for financial services firms facilitates their operations, provides for great efficiencies in their operations and better serves customers. It also provides greater efficiencies for regulators' enforcement of their regulations. The Commission did a great job of ensuring consistency between the proposed Regulation S-P

[12] *See* the Institute's 2008 Letter.

[13] *See* Letter from Susan M. Olson, General Counsel, ICI, to Ms. Vanessa Countryman, Secretary, SEC (April 11, 2022) (the "Institute's 2022 Letter"). The Institute's letter was filed in response to the SEC's request for comment on Release Nos. 33-1102j8, 34-94197, IA-5956, and IC-34497 relating to cybersecurity risk management programs for investment advisers and investment companies.

[14] *See* Release at fn. 74.

revisions and the Interagency Guidelines. Indeed, with respect to the provisions in the Commission's proposal relating to safeguarding customer information and breach notices, there are only a couple of provisions that we recommend tweaks to in order to better conform them to the Interagency Guidelines. The Institute's comments on the amendments proposed to Regulation S-P are next discussed.

2.1 Section 248.30(a), Scope

The Commission has proposed to expand the scope of Regulation S-P to include all consumer information possessed for a business purpose. The Institute supports this expansion. We concur with the Commission that NPPI possessed for a business purpose should be protected without regard to whether the information relates to a customer or a consumer.

2.2 Section 248.30(b)(1) and (2), Required Policies and Procedures

We support this section of the Regulation, which requires every covered institution to develop, implement, and maintain written policies and procedures to address administrative, technical, and physical safeguards for the protection of customer information, consistent with current law.

2.3 Section 248.30(b)(3), Required Response Programs for Unauthorized Access

Subsection 248.30(b)(3) would be added to Regulation S-P to require a covered institution's policies and procedures to include a program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. In part, this response program would require the covered institution to notify each individual whose "sensitive customer information" was, or is reasonably likely to have been, accessed or used without authorization unless the entity determines, after a reasonable investigation of the facts and circumstances 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.

The Institute supports the Commission revising Regulation S-P as proposed. We are pleased that the Commission will begin requiring covered entities to provide affected individuals notice of any unauthorized access to their NPPI if such access is reasonably likely to be used in a manner that would result in substantial harm or inconvenience to the individual. We are particularly pleased that this provision in Regulation S-P is substantively identical to the similar requirement in the Interagency Guidelines.

Our support today is consistent with our support for the SEC to require breach notices in the amendments it proposed in 2008 to Regulation S-P.[15] A significant advantage of SEC registrants being required to issue a breach notice is that, in several states, it will relieve SEC registrants from having to issue state-specific breach notices under state law. Today, approximately 13 states provide an exemption or exclusion from the state's breach notice requirements if the entity

[15] *See* the Institute's 2008 Letter.

experiencing the breach has a duty under federal law to provide notice of the breach.[16] In discussing breach notices with our members, we understand it is not uncommon for their current breach response programs to include separate notification letters depending upon the state the individual resides in. Each of these individual state responses would be unnecessary in states that permit the use of a federal breach notice in lieu of any state-specific notice.[17] Under state laws that do not provide an exception from the state's breach notice requirement for notices provided under federal law, it is possible that individuals in those states will receive two notices regarding a singular breach – *i.e.*, the newly required SEC notice and the state-specific notice.

2.4 Section 248.30(b)(4), Notifying Affected Individuals of Unauthorized Access

We support the proposed provisions to Regulation S-P to require covered institutions to notify individuals in the event of a breach involving sensitive customer information. These provisions will govern who must be notified, when they must be notified, and the information to be included in the notice.

2.4.1 Section 248.30(b)(4)(i), Notification Obligation

Section 248.30(b)(4)(i) would require covered entities to provide a notice to individuals whose sensitive customer information is likely to have been accessed without authorization. We support this provision and note that it is substantively identical to similar provision in the Interagency Guidelines. Under the SEC's proposal and the Guidelines, the obligation to provide a notice to any individual of unauthorized access to their NPPI would arise only *after* the covered institution has conducted a "reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive information" and, from that investigation, determined that sensitive customer information is reasonably likely to have been accessed, or used without authorization. We concur with aligning the SEC's requirements to the Interagency Guidelines and providing covered entities time to conduct the reasonable investigation necessary to determine which individuals may need to receive a breach notice.

2.4.2 Section 248.30(b)(4)(ii), Affected Individuals

This provision is intended to ensure that, when issuance of a breach notice is required, it is provided to all affected persons whose sensitive customer information is likely to have been accessed without authorization. As proposed, it addresses two important issues. The first relates to who must be notified. As proposed, if a covered institution knows which systems have been

---

[16] These states currently are Alabama, Colorado, Delaware, Idaho, Iowa, Kansas, Missouri, Nebraska, Oklahoma, Pennsylvania, Utah, Virginia, and West Virginia.

[17] This would occur in those states where it is impossible to reconcile the two notices. The Commission should consider avoiding this result by enabling covered institutions to satisfy their breach notice requirements under Regulation S-P by providing individuals in those states a breach notice compliant with the state's law even if it differs from the content requirements of Regulation S-P's breach notice. *See, e.g.*, Section 3(b) of Chapter 93H, which governs the breach notice required by the Commonwealth of Massachusetts.

accessed but cannot identify which individuals' sensitive NPPI within those systems have been accessed, then the covered institution must provide notice to each individual whose sensitive NPPI resides in the system. We concur with this approach to notification. Secondly, if the individual whose sensitive NPPI likely has been accessed without authorization is not a customer of the covered institution, the institution must provide a notice to such individual. We support this provision but recommend that, in the adopting release, the Commission address an issue relating to non-customer information.

As noted in the Release, a covered institution may come into possession of sensitive NPPI on individuals who are not customers of the entity.[18] Such information may be provided to the covered institution from another financial institution, such as a bank or a broker-dealer, or it may be provided to the entity by the individual who anticipates becoming a customer of the entity but does not. Regardless of how the sensitive NPPI comes into the covered institution's possession, we concur with the SEC that this information should be subject to the protections of Section 248.30 of Regulation S-P, including the breach notice requirements.

In the adopting release, we recommend that the Commission address a covered institution's obligation to provide a notice when the institution has the NPPI but does not have the individual's contact information (*i.e.,* a mailing address or email address). In those instances, we recommend that the adopting release clarify that, when the covered institution does not have contact information for the individual and, therefore, is unable to provide the breach notice, the covered institution is only required to provide notice to the person that provided the NPPI *if the covered institution knows who that person is and is able to provide such person notice of the breach*. So, for example, if the covered institution knows the information was provided by a broker-dealer, the covered institution would provide the breach notice to the broker-dealer. However, if the covered institution's records do not include contact information for the source of the NPPI, no notice would be required.

2.4.3 Section 248.30(b)(4)(iii), Timing of the Breach Notice

Section 248.20(b)(4)(iii) would govern when the breach notice must be provided to affected individuals. As proposed, this section would require notice be provided "as soon as practicable, but not later than 30 days after becoming aware that unauthorized access or use of customer information has occurred or is reasonably likely to have occurred . . .." The only exception is if the United States Attorney General notifies the covered institution in writing that a breach notice would pose "a substantial risk to national security." In such instance, the breach notice could be delayed for up to 15 days. We recommend this provision be revised as it is neither consistent with the Interagency Guidelines, nor the Commission's 2008 proposed amendments to Regulation S-P. It is also not consistent with the states' breach notice laws.

The Interagency Guidelines provide that the required breach notice "may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal

[18] *See* discussion beginning on p. 78 of the Release.

investigation and provides the [financial] institution with a written request for the delay." Notwithstanding the delay, the institution must provide the breach notice to its customers "as soon as notification will no longer interfere with the investigation." In 2008, when the SEC first proposed to revise Regulation S-P to require breach notices, the regulation would have required such notices as soon as possible unless delayed at the request of a law enforcement agency.

The current release, however, would not enable such a delay unless it is at the request of the U.S. Attorney General. According to the Release:

> . . . we recognize that a delay in customer notification may facilitate law enforcement investigations aimed at apprehending the perpetrators of the incident and preventing future incidents. Many states have laws that either mandate or allow entities to delay providing customer notifications regarding an incident if law enforcement determines that notification may impede its investigation. The principal function of such a delay would be to allow a law enforcement or national security agency to keep a cybercriminal unaware of their detection.[19]

We do not understand the public purpose served by the Commission proposing such a narrow exception. It is unclear what process would be followed to obtain written direction from the US Attorney General. Delays in breach notices should be permitted if such delay is requested by any law enforcement agency. That approach would align with the Commission's prior position and well established requirements in the Interagency Guidelines and state laws. The judgment of any law enforcement agency investigating a breach should be an adequate and respected basis for delaying a regulatory notice regarding such breach. We do not believe any public purpose would be served by ignoring the request of a law enforcement agency to delay the breach notice. We think the Commission's regulation should defer to a law enforcement agency's determination. Accordingly, we recommend that the Commission revise Section 248.30(b)(4)(iii) in relevant part as follows:

> (iii) *Timing.* A covered institution must provide the notice as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred unless 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. The institution should notify affected persons as soon as notification will no longer interfere with the investigation. ~~the Attorney General of the United States informs the covered institution, in writing, that the notice required under this rule poses a substantial risk to national security, in which case the covered institution may delay such notice for a period of time specified by the Attorney General of the United States, but not for longer than 15 days.~~

[19] Release at p. 61

2.4.4 Section 248.30(b)(4)(iv), Breach Notice Contents

Section 248.30(b)(4)(iv) of Regulation S-P will govern the contents of breach notices provided to affected individuals. With one exception, the contents of the Commission's breach notice would be identical to those of the Interagency Guidelines. This one exception is in Subsection 248.30(b)(4)(iv)(C), which would require the notices to include "the date of the incident, the estimated date of the incident, or the date range within which the incident occurred."

We recommend that the Commission delete this item from the contents. In support of our recommendation, we note that, since 2005, when the Interagency Guidelines required institutions to provide breach notices, this information has not been required in the notices. If the Commission retains this requirement, it would mean that institutions subject to both Regulation S-P and the Interagency Guidelines would have to revise their long-standing breach notices to add the information. Obviously, the federal banking regulators do not believe information relating to the date of the incident is necessary. The proposal does not detail a basis for a different conclusion by the SEC. We recommend that the Commission conform the Commission's notice requirements to those of the Interagency Guidelines, as consistent notices will better serve SEC registrants as well as their customers.

2.5 Section 248.30(b)(5), Service Providers

Section 248.30(b)(5) would govern the covered institution's engagement with service providers under the regulation. It would require a covered institution,

> . . . pursuant to a written contract between the institution and its service providers to require the service providers to take appropriate measures that are designed to protect against unauthorized access to or use of customer information, including notification to the covered institution as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security resulting in unauthorized access to a customer information system maintained by the service provider to enable the institution to implement its response program.

It would also provide that, as part of its incident response program, a covered institution may enter into a written agreement with its service provider to notify affected individuals on its behalf.

We concur with the Commission requiring service providers to notify a covered institution notice within 48 hours of a breach impacting the covered institution or its affected individuals. We understand that this is not an uncommon arrangement today between covered institutions, such as investment companies, and the service providers

maintaining their NPPI (*e.g.*, their transfer agents).[20] We also concur with the Commission that covered institutions should be permitted to have their service providers send breach notices to affected individuals on behalf of the covered institution. We understand that this is a common practice today for investment companies wherein their transfer agents assume responsibility for sending affected customers breach notices.

The proposal's service provider provisions are substantively identical to the provisions in the Interagency Guidelines relating to service providers. Because of this uniformity we support their adoption. While, in connection with other SEC rulemakings, the Institute has opposed regulatory requirements requiring registrants to include specified provisions in their contracts with service providers,[21] we are not opposing this contractual requirement in Section 248.30(b)(5) because of its very narrow scope. As drafted, it would only apply to any service provider that receives, maintains, processes, or otherwise is permitted access to customer information through the service provider's provision of services directly to the covered institution. Importantly, too, the information covered by Section 248.30(b)(5) is already subject to a contractual agreement between the covered institution and the service provider.

Since Regulation S-P was adopted in June 2000, it has provided an exception to the regulation's privacy notice opt-out requirements for any registrant that shares NPPI with a nonaffiliated third party so the third party can perform services on the registrant's behalf or to function on its behalf. This exception, however, has always been predicated on the registrant entering "into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which [the registrant] disclosed the information."[22] In other words, since 2000, Regulation S-P has required that any NPPI that a covered institution shares with a service provider so the service provider can provide services to the covered institution be subject to a contract between the service provider and the covered institution. Such contract must require the service provider to protect the confidentiality and security of the NPPI. The proposed revisions to Regulation S-P would expand these existing contractual requirements to require the service provider to protect the NPPI from unauthorized access or use and to notify the covered entity notice within 48 hours of determining that such NPPI has been breached. Due to the contractual requirements that currently exist in Regulation S-P, we do not oppose the amendments to Regulation S-P expanding those requirements.

---

[20] While it is not uncommon for covered institutions to require their service providers, by contract or agreement, to notify the covered institution in the event of a breach, the timing of this notice may differ from what the SEC is proposing (*i.e.*, 48 hours).

[21] *See, e.g.*, the Institute's 2022 Letter.

[22] *See* Section 248.13(a)(1)(ii) of Regulation S-P.

2.6 Section 248.30(c), Disposal of Consumer and Customer Information

Section 248.30(c) would govern the disposal of consumer and customer information. Today, this provision is very narrow in its application as it only applies to "consumer report information." We support expanding its scope to include consumer and customer information as such terms are defined in the proposal.

2.7 Section 248.30(d), Recordkeeping

Section 248.30(d) would be added to Regulation S-P to require covered institutions to maintain records documenting their compliance with the regulation. The Institute supports the proposed recordkeeping requirements.

2.8 Section 248.30(e), Definitions

Section 248.30(e) would add the following definitions to Regulation S-P: consumer information; covered institution; customer; customer information; customer information systems; disposal; sensitive customer information; service provider; substantial harm or inconvenience; and transfer agent. As proposed, the definition of "covered institution" would expand the scope of Regulation S-P to include transfer agents.

We support this expansion and note that our support for it today is consistent with our recommendation in our 2022 comment letter on the proposed cybersecurity rule for registered investment companies and investment advisers.[23] With respect to the remaining definitions, as next discussed, we recommend a minor revision to the definition of "sensitive customer information" to clarify its meaning and better align it with the Interagency Guidelines' definition.

2.8.1 Section 248.30(e)(9), Sensitive Customer Information

The Commission has proposed to define "sensitive customer information" as "any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified in the information." This definition would seem to imply that a singular piece of customer information could be considered "sensitive customer information" that would trigger obligations under the revised regulation. In our view, this would unnecessarily broaden the notice obligations.

By contrast, the Interagency Guidelines define the term to mean, in relevant part, "a customer's name, address, or telephone number *in conjunction with* the customer's SSN, drivers' 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."

---

[23] *See* the Institute's 2022 Letter.

[Emphasis added.] We believe that, by focusing on information "that would permit access to the customer's account," the definition in the Interagency Guidelines is appropriately and better tailored to capture information that should trigger a breach notice. If unauthorized access of this information would enable a bad actor to access the individual's account, it could likely be exploited to harm other financial or personal interests of the individual. Accordingly, we recommend that the Commission revise the proposed definition of "sensitive customer information" to better align with the definition of this term in the Interagency Guidelines.

3.0 Section 248.50, Annual Privacy Notice to Customers

The Commission's amendments to Regulation S-P would also revise provisions in the regulation that govern the duty of covered institutions to provide annual privacy notices to their customers. As noted in the Release,[24] in 2015, the GLB Act requirement that financial institutions provide customers an annual privacy notice was revised by the Fixing America's Surface Transportation Act ("FAST Act"). As revised, those institutions that only share NPPI in accordance with the GLB Act and have not made changes to their sharing practices since the last annual notice they provided to customers are not required to provide an annual privacy notice. Instead, for qualifying institutions, they would only need to again begin providing annual privacy notices when their sharing practices change (or are no longer in accordance with the GLB Act).

The Institute supports the Commission updating Regulation S-P to conform it to the FAST Act, and we commend the Commission for including these amendments in its current proposal.

4.0 Proposed Compliance Date

According to the Release, the Commission proposes

> . . . to provide a compliance date twelve months after the effective date of any adoption of the proposed amendments in order to give covered institutions sufficient time to develop and adopt appropriate procedures to comply with any of the proposed changes and associated disclosure and reporting requirements, if adopted.[25]

The Institute recommends a compliance date no earlier than twenty-four (24) months after the effective date of the amendments adopted to Regulation S-P.

When the Commission amended Regulation S-P to add provisions relating to the disposal or destruction of consumer report information, it provided registrants eighteen (18)

---

[24] Release at pp. 99.

[25] Release at p. 131.

months to implement those amendments. Those amendments, in part, required registrants to revise their contracts with service providers. While the 2004 amendments, which were adopted in December 2004, had an effective date of January 11, 2005 and a compliance date of July 1, 2005, registrants were provided until July 1, 2006, to revise their existing contracts with service providers. We urge a longer compliance period for the current amendments to Regulation S-P because (1) they are far more extensive than the 2004 amendments; (2) they will necessitate revising contracts with service providers to align the breach notification provisions in those contracts to the rule's requirements; and (3) in light of all the other new regulatory requirements covered institutions must comply with, we are concerned with the availability of, and ability to devote, the necessary resources to implement these new requirements (and test their operation).

A longer period will provide registrants fair and sufficient time to most responsibly implement new breach and data security requirements, including time to revise their existing contracts with service providers, including the provisions in existing contracts relating to breach notices. As previously mentioned, while it is not uncommon for service providers to agree to provide the covered institution notice of a breach, the timing of these notices may not be consistent with the SEC's proposed 48-hour period. Also, what constitutes a "breach" under these agreements may not be consistent with how the rule would define a breach. We understand from our members that the notice period and the definition of "breach" in these agreements are highly contentious provisions in agreement negotiations.

In advocating for a 24-month compliance period, we note that, in the interim, individuals' NPPI will continue to be protected by Regulation S-P's safeguarding requirements and breach notices that are required by state law will continue to alert them to unauthorized access to their NPPI. Forcing a fast implementation will serve neither the interests of investors nor the goals of the Commission.

5.0 Notifying SEC Registrants of Breach of the Commission's Systems

In 2008, when the Commission proposed amendments to Regulation S-P to require breach notices, it also requested comment on whether the Commission should be required to provide notice whenever it is breached. In our 2008 comment letter, we supported the Commission's request for comment on this issue and "strongly recommended that the Commission" subject itself to breach notice requirements substantially similar to those imposed on registrants by Regulation S-P.

The Commission's current Release does not seek comment on this issue. Nevertheless, we reiterate our 2008 comment and recommend that the Commission give serious consideration to revising its rules of practice to ensure that, when any NPPI or confidential information the Commission possesses is subject to unauthorized disclosure, the Commission be required to notify the source of that information about the breach with the same level of detail that the Commission proposes for covered institutions. The Institute strongly believes breach notifications by regulators are important to protect registrants as well as investors, clients, and

customers of the financial services industry. Most recently, we strongly advocated for breach notifications related to the national market system plan to implement the consolidated audit trail ("CAT").[26] Members of Congress in the appropriations process, too, have recognized the importance of the SEC strengthening their information security and urged the SEC to ensure the CAT has adequate breach notification policies in place so affected participants are promptly notified of critical security events.[27]

Providing breach notifications is critical to helping registrants and others take steps to protect their interests and the interests of investors and clients. The SEC has a responsibility to act in the public interest and providing notifications of a breach will meaningfully support that mission.[28]

5.1 The Breach of the SEC's EDGAR System

In September 2017, SEC Chairman Clayton issued a public statement on cybersecurity.[29] This statement was the first public disclosure of a 2016 breach of the SEC's EDGAR system. As disclosed in the statement:

> In August 2017, the Commission learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading. Specifically, a software vulnerability in the test filing component of the Commission's EDGAR system, which was patched promptly after discovery, was exploited and resulted in access to nonpublic information. It is believed the intrusion did not result in unauthorized access to personally identifiable information, jeopardize the operations of the Commission, or result in systemic risk. An internal investigation was commenced immediately at the direction of the Chairman.

Reading the pleadings filed against the hackers in January 2019,[30] the public learned that the hackers had been able to penetrate the SEC's EDGAR computer network in May

---

[26] Comment Letter from ICI to Brent Fields, Secretary, July 18, 2016, available at https://www.sec.gov/comments/4-698/4698-8.pdf. We continued to engage with the Commission, including Chairman Clayton, and FINRA on CAT security and breach notification.

[27] See e.g., H. Rept. 117-393 - FINANCIAL SERVICES AND GENERAL GOVERNMENT APPROPRIATIONS BILL, 2023, at 102, available at https://www.congress.gov/congressional-report/117th-congress/house-report/393/1?q=%7B%22search%22%3A%5B%22H.Rept.+117-393%22%5D%7D&s=2&r=2.

[28] At the time of our 2008 Letter, we were not aware of any breaches of the Commission. We were, however, aware of a report from the Government Accountability Office documenting deficiencies with the Commission's information security controls and the Commission's Office of Inspector General identified concerns with laptop controls. *See* the Institute's 2008 Letter.

[29] The Chairman's statement is available at: https://www.sec.gov/news/press-release/2017-170.

[30] *See U.S. Securities and Exchange Commission v. Oleksandr Ieremenko, et al.,* District of New Jersey, Civil Action No. 19-cv-505, (January 15, 2019).

2016 and their unauthorized access continued until at least October 2016. In addition, while the Commission did not alert the public to this hack until September 2017 – almost 18 months after it occurred – FORTUNE magazine reported as early as March 2017 that EDGAR users had been receiving SEC emails the scammers were spoofing.[31] These emails were indicative of the fact that the EDGAR system had been breached.

5.2 Notifications Would Enable Registrants to Take Protective Measures For the Benefit of Registrants and Customers, Clients, and Investors

We raise this history to emphasize the importance of registrants being notified, as soon as possible, of any breaches the Commission experiences if such a breach impacts non-public information. There is little doubt that notifications are valuable to mitigating harm to those affected by a breach – hence the SEC requiring covered institutions to provide breach notices. Such notifications from the Commission would enable registrants to protect themselves and their investors.

With each passing year, the Commission receives more and more confidential and sensitive information – including for example, in addition to any issuer filings, Form N-MFP and N-PORT information as well as information obtained by the Commission's Divisions of EXAMS and Enforcement, which often is extensive and includes individuals' NPPI. The ever-increasing amount of information the Commission obtains, receives, and maintains heightens concerns with the scope and range of harm that may result from a breach of the Commission's systems. And yet, the Commission has no duty to provide any notice of unauthorized access to such confidential and sensitive information to help those affected take mitigating and protective actions. We strongly recommend that the Commission, in the public interest, impose upon itself a duty to provide breach notices whenever non-public information it possesses has been accessed without authorization.

6. Regulation by Enforcement Concerns

In recent dissents filed in connection with enforcement actions brought by the Commission, Commissioners Peirce and Uyeda have expressed concern with the Commission engaging in "regulation by enforcement" – *i.e.*, imposing new regulatory

[31] The Fortune article noted, in part, that the cyber scammers were "sending spoofed emails, purporting to be from the SEC, and aiming them at lawyers, compliance managers, and other company officials who file documents with the SEC. . . . Those who clicked on instructions in the Word document granted the attackers access to internal corporate networks . . .." According to the article, the security firm FireEye discovered these spoofed emails in February 2016 when it intercepted suspicious emails targeted at companies in sectors ranging from transportation to banking to retail. At the time, FireEye believed the scammers were likely an Eastern European criminal syndicate that was looking to make money by trading on inside information. *See "Fake SEC Emails Target Execs for Inside Information,"* Fortune (March 7, 2017), which is available at: http://fortune.com/2017/03/07/sec-phishing/.

requirements on registrants when settling administrative actions.[32] The Release appears to suggest such an approach in connection with the proposed requirements. For example, in discussing the duty a covered institution would have to assess the nature and scope of any incident involving unauthorized access to NPPI maintained by the institution, the Release states: "Covered institutions generally should evaluate and adjust their assessment procedures periodically *regardless of any specific regulatory requirements* . . .."[33] [Emphasis added.] Similarly, in discussing a covered institution's duty to contain and control a security incident, the Release states: "Covered institutions generally should evaluate and revise their containment and control procedures periodically, *regardless of any specific regulatory requirement* . . .."[34] [Emphasis added.]

We are very concerned with the Commission signaling in its releases that it is expecting registrants to take specific actions not required by the regulation. All regulatory requirements the Commission intends to impose on registrants should be expressly stated in the rule itself. We recommend that the adopting release refrain from suggesting actions a registrants might take in the absence of the regulation requiring such action.

7. Conclusion

The Institute and its members appreciate the opportunity to comment on the amendments the Commission has proposed to Regulation S-P. If you have any questions or require further information regarding our comments, please do not hesitate to contact the undersigned (tamara@ici.org) or the Institute's General Counsel, Susan Olson (solson@ici.org).

Sincerely,

/s/
Tamara K. Salmon
Senior Associate Counsel

Cc: Gary Gensler, Chair, Securities and Exchange Commission
Hester M. Peirce, Commissioner, Securities and Exchange Commission
Caroline A. Crenshaw, Commissioner, Securities and Exchange Commission
Mark T. Uyeda, Commissioner, Securities and Exchange Commission
Jaime Lizárraga, Commissioner, Securities and Exchange Commission

---

[32] *See, e.g., Statement Regarding Huntleigh Advisors, Inc. and Datatex Investment Services, Inc.*, Commissioners Hester M. Peirce and Mark T. Uyeda (February 27, 2023), which is available at: https://www.sec.gov/news/statement/peirce-uyeda-statement-huntleigh-datatex-022723.

[33] Release at p. 27.

[34] Release at p. 29.