PUBLIC SUBMISSION

Comment Submitted by SIFMA & BPI

Posted by the **Federal Trade Commission** on Feb 7, 2022

View More Comments 21 (/document/FTC-2021-0071-0001/comment)

View Related Comments 21 (/docket/FTC-2021-0071/comments)

Share

Comment

See attached file(s)

Attachments 1

Comment Letter on FTC Safeguards Rule SIFMA BPI Feb 7 2022

Download (https://downloads.regulations.gov/FTC-2021-0071-0015/attachment_1.pdf)

Comment ID

FTC-2021-0071-0015

Tracking Number

kzd-94tp-cdf5

Comment Details | Submitter Info

Received Date

Feb 7, 2022

Your Voice in Federal Decision Making

February 7, 2022

Submitted electronically via Regulations.gov
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Safeguards Rule, 16 C.F.R. part 314, Project No. P145407

Dear Secretary Tabor:

The Securities Industry and Financial Markets Association ("SIFMA")[1] and the Bank Policy Institute ("BPI")[2] (collectively, the "Associations") appreciate the opportunity to comment on the supplemental notice of proposed rulemaking issued by the Federal Trade Commission ("FTC" or "Commission") about further amending the Standards for Safeguarding Customer Information, 16 C.F.R. part 314 (the "Safeguards Rule").[3]

More than two decades ago, drafters of the Gramm-Leach-Bliley Act ("GLBA"), enacted in 1999, sought to establish new privacy and security standards for the protection of personal information processed by financial institutions. Rather than impose prescriptive technological controls, GLBA delegates to financial regulators the authority to create standards that evolve with technological changes. In 2002, the Commission first promulgated its version of the Safeguards Rule, and recently amended it to require specific security controls and accountability measures expressly modeled on the New York Department of Financial Services ("NYDFS") cybersecurity rule.

---

[1] 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 members, we advocate for 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).

[2] The Bank Policy Institute is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

[3] SIFMA and BPI would like to thank Edward McNicholas and Briana Fasone of Ropes & Gray for their counsel and assistance in drafting this letter.

In October 2021, the Commission proposed an additional amendment to the updated Safeguards Rule that would require institutions within its jurisdiction that experience a security event, in which the misuse of customer information has occurred or is reasonably likely, to provide notice of the event to the Commission no later than 30 days after discovery of the event if it affected or reasonably may have affected at least 1,000 consumers ("Proposed Amendment").[4] The Commission seeks such report to "ensure the Commission is aware of security events that could suggest a financial institution's security program does not comply with the Rule's requirements, thus facilitating Commission enforcement of the Rule."[5] The Commission would then "input the information it receives from affected financial institutions into a database that it will update periodically and make available to the public"[6] in order to "assist consumers by providing information as to the security of their personal information in the hands of various financial institutions."[7]

While we share the Commission's concerns about the unique threat that current cyber risks pose for financial institutions, we write today to offer what we intend to be constructive comments on the Proposed Amendment, which, as currently drafted, could create operational and compliance challenges for some of our members without necessarily achieving the stated intent of the Proposed Amendment in an effective manner. We value the opportunity to provide input on the reporting requirement and address the issues highlighted by the Commission in its Proposed Amendment.

1. The Associations Support Reporting Requirements that Level the Field[8]

The Commission requests comment as to whether the amended Safeguards Rule should include a notification requirement at all. It also seeks comment on whether a notice obligation should exist as a "stand-alone reporting requirement" or as a supplemental responsibility triggered only when institutions notify other governmental regulators of security intrusions. The Associations fully endorse a stand-alone reporting requirement that attaches only to those financial institutions subject to GLBA but not regulated by other financial agencies (such institutions, "Non-financially Regulated Institutions"). The membership of the Associations comprises entities which are already actively regulated through their primary prudential regulators (such institutions, "Financially Regulated Institutions"), and we believe that the Commission's intent was not to add redundant notification obligations to such entities.[9] We strongly support the Commission's effort to level the playing field so that all entities subject to GLBA face appropriate incident reporting

[4] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70062 (proposed Dec. 9, 2021) (to be codified at 16 C.F.R. 314).
[5] 86 Fed. Reg. at 70064.
[6] *Id.*
[7] *Id.* at 70066.
[8] The Comment is intended to address the Commission's questions 6 and 7, as well as its request for information as to potentially duplicative, overlapping, or conflicting federal rules under the Regulatory Flexibility Act ("RFA"). *See id.* at 70064, 70067.
[9] If the amended rule does extend to Financially Regulated Institutions, then we propose that the notification requirement exist only as a supplemental obligation for such institutions. For Financially Regulated Institutions , notice to the Commission should be required only when that an institution is required to provide notice of a security incident to a governmental entity under another state or federal statute, rule, or regulation. If an entity is primarily subject to oversight by another regulator, such as a state insurance commission or the SEC, and that regulatory regime does not require a data breach notification, it would be unusual to nonetheless require a notice to the Commission and could arguably be interpreted as possibly encroaching on the authority of the entity's principal regulator.

obligations to ensure consistently applied transparency to the occurrences of these events wherever the information resides. While we recognize that a properly tailored notification requirement can have benefits, reporting obligations should apply only to situations where such notice is not redundant to existing notification requirements and only to those institutions for which the Commission is the principal financial regulator.

a. Coordinate with other regulators to avoid duplicative reporting

While the Associations acknowledge that, in drafting the Proposed Amendment, the Commission commendably attempted to reduce burdens, an additional notification requirement for robustly regulated institutions adds an unnecessary layer to the already-complex existing threat detection and reporting process. Our concern about reporting for organizations already subject to the oversight of another primary regulator is not limited to extra filings. Most of the Financially Regulated Institutions are required to maintain comprehensive compliance programs to address information security, third-party and vendor risk management, business continuity, and are required to adequately disclose certain cybersecurity vulnerabilities to numerous federal regulators, including the Office of the Comptroller of Currency ("OCC"), the Federal Reserve System ("Federal Reserve"), the Federal Deposit Insurance Corporation ("FDIC"), and the Securities and Exchange Commission ("SEC"), in addition to state agencies.[10]

State and federal regulators of Financially Regulated Institutions are essential monitors of the soundness of the information security systems of such institutions, but we strongly believe imposing additional and redundant notice obligations on these institutions serves not only to distract them from focusing on protecting systems and securing consumer information but also creates a dynamic in which an entity may be looking to multiple regulators with different timelines and priorities for guidance in responding to such an incident. Adding the Commission to the long list of regulators already receiving notice of security incidents from Financially Regulated Institutions would not create any supplemental benefits for the consumer or entities that are already prudentially regulated. More significantly, adding the Commission could unnecessarily interfere with the discretion of the primary federal regulator and result in consumer confusion.

b. Avoid Redundant Regulation of Private Funds and Complex Financial Groups

The Associations are also concerned that the Commission's Proposed Amendment may, in practice, impermissibly exceed its jurisdictional power – and it may do so in areas where there are only a handful of consumers and areas where other federal prudential and state insurance regulators already exercise pervasive oversight.

Section 45(a) of the Commission's organic statute expressly excludes from the Commission's core authority "banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title" as well as several other entities that are subject to extensive federal regulation under other primary federal

[10] Although the SEC does not have an official reporting requirement, its Division of Examinations expects notification of significant events. Additionally, SEC Reg S-P requires broker-dealers, investment advisers, and investment companies to notify customers of their privacy policies and establish sufficient safeguards for their personal and financial information and is capable of rulemaking.

regulators.[11] The Associations recognize that the Commission does not purport to exercise its limited section 45(a) authority but instead cites its authority under 15 U.S.C. § 6801(b), § 6805(b)(2) for its Proposed Amendment.[12] The Commission's Proposed Amendment could well result in effective regulation of entities that fall under the primary jurisdiction of other regulators and could, accordingly, create potentially conflicting and redundant requirements. Many financial institutions, including several members of the Associations, operate as corporate groups technically subject to various regulators, but, in reality, are primarily regulated by one entity. Significant data security events may impact multiple parts of these corporate groups in complex ways that are difficult to differentiate in a timely manner.

For large and complex corporate families of financial institutions, it may be that the SEC or another agency is the primary regulator of the vast majority of the entities, but some entities may be outside of the Commission's authority. For instance, insurance companies are already subject to extensive state regulation, including the very cybersecurity regulation on which the Commission bases its Proposed Amendment. Some entities with an insurance group, however, may not technically be subject to such rules, while functionally being connected to other corporate entities that are subject to those rules. Adding the Commission's rules to such complex situations would only create confusion, not protect consumers.

A particularly significant example of this issue arises in the context of a private investment fund, the investment adviser for the fund is subject to pervasive SEC regulation, but the fund itself is often excluded from the definition of "investment company" under sections 3(c)(1) or 3(c)(7) of the Investment Company Act of 1940. In practice, this is of little practical significance because the fund normally has no employees, a very small number of natural person investors, and is administered by the investment adviser under SEC rules – and certainly only a handful of consumers, all of whom are sophisticated investors. The Commission's Proposed Amendment, unless revised, would insert the Commission into this area that is certainly much closer to the SEC's expertise and control. To that end, the Proposed Amendment should not apply to investment entities such as private-equity funds, which are functionally administered by investment advisers under SEC jurisdiction, even though the fund itself is under Commission jurisdiction. A cyber attack that affects the fund's underlying infrastructure would almost inevitably impact data relevant to both SEC and Commission-regulated entities. In that instance, under the Proposed Amendment, a breach that would otherwise be reported to a primary regulator, like the SEC, must then be reported to the Commission in a public format, significantly impacting the ability of the primary regulator to address the attack consistent with normal practices and discretion. The Proposed Amendment would accordingly interject the Commission into an already-complex arrangement even if only a small part of the corporate family fell under its jurisdiction. The Commission's interference in these scenarios would cause confusion and conflict with the authorities of other agencies and exceed the Commission's statutory powers with respect to unfair or deceptive acts or practices. While the Associations do endorse a reporting obligation for institutions under GLBA that are not subject to other primary federal financial regulators, a notification requirement should not extend to situations where it would be redundant, burdensome, and ultimately hinder other regulatory work.

[11] 15 U.S.C. § 45(a).
[12] 86 Fed. Reg. at 70067.

c. Intra-Governmental Information Sharing is Crucial

The Associations fully support the Commission's desire to remain informed about the full range of cybersecurity threats, which include exploitation of software vulnerabilities, ransomware, insider threats, nation-state attacks, trade secret theft, and other operational efforts, that undermine the confidentiality, integrity, or availability of their systems and the data that they process. Information sharing is unquestionably essential to preventing cyberattacks and assisting with broader incident response. To the extent an institution is subject to GLBA but not otherwise prudentially regulated, we agree that such an entity should provide the Commission with information regarding cyber intrusions. For entities already subject to federal prudential regulation, it may well be much more efficient and effective for the Commission to work with the other federal and state financial regulators to facilitate the sharing of information within the government, as opposed to requiring multiple differing reports about the same incident.

Many of our members already voluntarily engage in extensive information sharing, including within the confines of the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), a nonprofit entity created by and for financial institutions that was established in response to President Clinton's 1998 Presidential Decision Directive 63. The Department of Treasury's Financial Sector Cyber Intelligence Group ("CIG"), an FS-ISAC partner, collects information regarding cybersecurity threats available only through law enforcement channels and disseminates it to financial institutions at an unclassified level, and this sharing could surely be a more efficient source of information collection for the Commission than receiving its own separate reports. Additional breach notification obligations, beyond what exists in the current disclosure framework, should be directed toward agencies and consortia, like FS-ISAC, specifically dedicated to information sharing.[13] Information reciprocity—the key to combatting cyberthreats—should not, however, have to involve redundant reporting. If the Commission seeks information for purposes of enforcing its rules, it should join the existing reciprocity framework and leverage current resources, allowing agencies already dedicated to information sharing to be the source of federal government data about cyber attacks.

2. Reported Information Should be Confidential[14]

The Commission seeks comment on whether reported information should be made public or kept confidential. It also requests comment on the proposed content of the notice, which includes: (1) the name and contact information of the reporting financial institution; (2) a description of the types of information involved in the breach; (3) the date or date range of the breach, if that information is possible to determine; and (4) a general description of the breach.[15]

---

[13] The Commission could also obtain information from the Cybersecurity and Infrastructure Security Agency ("CISA"), which shares substantive information with both the private sector and with international, federal, state, local, tribal, and territorial actors.

[14] The Comment is intended to address the Commission's questions 5 and 1. *See* 86 Fed. Reg. at 70064.

[15] We do not object to any proposed element, although we note that this provision could preempt the Massachusetts requirement not to provide information about the incident under its amended Data Breach Notification Law. *See* Mass. Gen. Laws ch. 93(H), § 3 ("[Notice to residents] shall not include the nature of the breach of security or unauthorized acquisition or use, or the number of residents of the commonwealth affected by said breach of security or unauthorized access or use."). If so, the Commission should be clear that it intends its rule to preempt state data breach notification requirements.

a. Confidentiality Leads to Better Cybersecurity Reporting

The Associations observe that confidentiality in the reporting of information provided to the Commission is essential and would be consistent with general norms of financial institution information sharing in order to enhance cybersecurity. The Commission will incentivize more comprehensive reporting—and accordingly facilitate more robust information sharing—if institutions are confident that nonpublic material will not be disclosed. As noted above, robust cooperation between private and public sectors is essential for forward-looking cyber-defense that involves not just mitigating disruptive intrusions, but also preventing future attacks. Companies must be able to share valuable information with the government and their industry without fear of undue reputational harm and unnecessary loss of consumer trust and confidence in financial institutions.

Under the Proposed Amendment, the Commission intends to "input the information it receives from affected financial institutions that it will update periodically and make available to the public."[16] The Commission notes that since it does not believe that the publicized information will include "confidential or proprietary information," it accordingly does not intend to provide any "mechanism for financial institutions to request confidential treatment of the information."[17] We urge the Commission to reconsider this scheme. The Commission's proposal to publicize information it deems nonproprietary will ultimately limit the kind of productive information sharing that is essential to incident response. Some breaches have systemic effects on financial markets and require the affected company to work closely with their primary regulatory, law enforcement, and national security agencies in response. For many financial institutions, investor confidence is key, and including only general information about an incident, while naming the institution, is likely to lead to confusion and unnecessary concern for many smaller incidents. The need to both minimize further institutional damage and maintain confidence in financial markets will often counsel confidentiality or the delay in releasing certain information about data security incidents.

The unnecessary revelation of confidential information may lead to needless consumer confusion, especially in this era of social media, instantaneous news-sharing, and rapid misinformation-proliferation. Information about data breaches can often evolve in complex ways as companies learn more about attackers as forensics unfold. Data breaches understandably leave potential victims feeling overwhelmed. Most significantly, virtually all security breach notification regimes impose on the institution an affirmative obligation to notify the impacted consumer of the incident and provide details of it including the personal information that was subject to the incident. Consequently, if consumers discover that a particular financial institution has suffered a security incident, but do not know which individuals are actually impacted, all of the institution's customers become unnecessarily fearful while only a fraction may be justifiably concerned. Confidentiality mitigates this confusion and allows financial institutions to communicate effectively with impacted customers directly.

[16] 86 Fed. Reg. at 70064.
[17] *Id.*

b. Confidentiality Aligns with Other Regulatory Reporting Standards

According to the SEC's Guidance on Public Company Cybersecurity Disclosure ("SEC Guidance"), institutions should consider the importance of any compromised information and the impact of the incident on the company's operations in determining disclosure obligations following security incidents.[18] The SEC Guidance also notes that the materiality of cybersecurity risks and incidents depends on the range of harm those incidents could cause, and such harm might include damage to a company's reputation, financial performance, and customer and vendor relationships. The Associations ask that the Commission considers, too, the recently-adopted Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers ("Banking Rule"), issued by the OCC, FDIC, and Board of Governors of the Federal Reserve ("Board") (collectively the "Agencies").[19] Under the Banking Rule, any information provided by an organization related to a cybersecurity incident is subject to the Agencies' cybersecurity rules, which provide protections for "confidential, proprietary, examination/supervisory, and sensitive personally identifiable information."[20] Moreover, in its promulgation of the final Banking Rule, the Agencies concluded that telephone communication, which could foster confidentiality, is a sufficient method of incident notice.[21] The Associations recommend the Commission harmonize its notification standard with that of other agencies and regulators.

The Associations emphasize the distinction between productive discretion and harmful concealment. Much of the critical decision-making in data breach response involves considerations such as whether or not the affected entity could tip off the threat actors or engage with them, especially if there has been a ransom demand. Institutions should not be compelled to publicly disclose information about their cybersecurity framework or potential system vulnerabilities as to alert perpetrators of attacks or even empower additional threat actors to gain unauthorized access to compromised networks.

3. The FTC Should Trigger the Reporting Obligation With the "Determination" of a "Security Incident" or "Notification Incident"[22]

The Proposed Amendment provides that institutions must notify the Commission of certain "security event[s]" no later than 30 days after the "discovery" of the event.[23] At first glance, the 30-day provision appears generous, especially against the backdrop of other regulatory notification deadlines, some of which are measured in hours, not days. The Proposed Amendment's 30-day reporting requirement appears substantially longer than, for instance, the 36-hour deadline under the Banking Rule,[24]but that evaluation is misleading.

---

[18] 83 Fed. Reg. 8166 (Feb. 26, 2018).
[19] 86 Fed. Reg. 66424 (to be codified at 12 C.F.R. 53; 12 C.F.R. 225, 12 C.F.R. 304) (effective date April 1, 2022).
[20] *Id*. at 66437.
[21] *Id*. at 66433. The Commission proposes that notice be provided both by telephone or electronically through a form located on the FTC website. To reduce the compliance burden for financial institutions, the Associations recommend that the Commission keep the notice contents to a minimum and ensure its website form is a streamlined and secure method of notification.
[22] The Comment is intended to address the Commission's question 3. *See* 86 Fed. Reg. at 70064.
[23] *Id*.
[24] 86 Fed. Reg. 66424 (to be codified at 12 C.F.R. 53; 12 C.F.R. 225, 12 C.F.R. 304) (effective date April 1, 2022).

Under the Banking Rule, organizations are required to notify their primary federal regulator of significant computer-security incidents, known as a notification incidents, no later than 36 hours after the organization determines such an incident has occurred.[25] As set forth in greater detail below, a computer-security incident under that rule is one that actually harms the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.[26] By comparison, the trigger for the Commission's proposed reporting requirement is less clear: the obligation attaches to the "discovery" of a "security event," which, as currently proposed, is not a workable framework and would undoubtedly capture remediable cyber activity that should not rise to the level of mandatory disclosure.

We do not object to the 30-day deadline from the date of a known incident, but do recommend that the Commission, for the sake of clarity and efficacy, attach the reporting obligation to the "determination" of a "security incident" or "notification incident." Only at that point, should the 30-day clock begin to run.

While the Commission recently engaged in an analysis of the term "security event" during the notice-and-comment period for the recently-amended Safeguards Rule,[27] as the Commission notes, the Rule defines "security event" as "an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form."[28] This definition, if applied to the term "security event" with respect to the notification requirement in the proposed new paragraph, is too broad and would capture less-significant cyber disruptions that do not result in exposure of protected consumer information and would ultimately be unduly burdensome to report. Instead of re-defining the term "security event" for this amendment—to avoid introducing confusion into the finalized Rule—we propose the Commission use either "security incident" or "notification incident" to identify the notification activity. This change would align the Commission's notification obligation criteria with that of other agencies.

The Banking Rule requires reporting of a "computer-security incident" that rises to the level of a "notification incident"—terms that were defined after the Agencies adopted commentators' suggested revisions to the proposed regulation.[29] The definition of "computer-security incident" was narrowed to include only an "occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."[30] Meanwhile, a "notification incident," as defined by the rule, constitutes a "computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's: (i) ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) business line(s), including associated operations, services, functions, and support, that upon failure would result in a material

[25] *Id.*
[26] *Id.* at 66425 n.3.
[27] *See* Standards for Safeguarding Customer Information, 86 Fed. Reg. 70272, 70274-75 (to be codified at 16 C.F.R. 314 (effective date Jan. 10, 2022)) (discussing the process of including and defining the term "security event").
[28] *Id.* at 70272.
[29] 86 Fed. Reg. 66430. The Associations submitted a comment on the notice of proposed rulemaking issued by the Agencies and were pleased that some of its suggestions were incorporated into the final Banking Rule.
[30] *Id.* at 66442.

loss of revenue, profit, or franchise value; or (iii) operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States."[31]

We respectfully recommend that the Commission adopt a similarly-targeted *incident* standard for its notification requirement and propose the use of "security incident" or "notification incident" to describe the notice trigger.[32] Such a standard would ensure that institutions are not forced to report harmless cyber events at the expense of directing time and resources toward effective data breach response.

Institutions need time to investigate cyber intrusions before reporting them to regulatory agencies. To that end, we believe that the reporting requirement should be triggered only upon a "determination" of a security or notification incident. "Determination" connotes a higher standard of certainty than "discovery," and we believe such a standard is appropriate in this context given the complicated nature of incident response. Cyber incidents are resolved in a fog of war; information is frequently incomplete, inaccurate, or shown later to be incorrect. A determination of the incident transpires at some point after the initial detection of it, while it is unclear where "discovery" falls in this knowledge spectrum. A regulator's review of a financial institution's analysis of threats to its security system is better conducted after a determination has been made, rather than at a premature point in time.

4. The FTC Should Further Clarify the Threshold for Requiring Notice[33]

The Proposed Amendment includes a threshold for requiring notice—for those incidents for which "misuse of the information of 1,000 or more consumers has occurred or is reasonably likely to occur."[34] We appreciate the request to evaluate whether this standard is an appropriate one. The Associations do not object to the fact that the reporting requirement would apply to misuse of information of 1,000 or more customers, and we encourage the Commission to include a carve-out for incidents solely involving encrypted data. However, we recommend the Commission clarify that "misuse of information" means "misuse of customer information that results in harm to consumers." We also suggest that the notification requirement be limited to

[31] *Id.* The Associations appreciate the fact that Agencies took into consideration their suggestions. We don't believe it is necessary to have a separate definition for "security incident" and "notification incident" but rather feel that the Commission can incorporate relevant information under one term.

[32] Other federal agencies use a "incident" to characterize the notification catalyst and there is general consensus that it a more targeted term than "event." *See, e.g.*, 17 C.F.R. § 39.18 (the SEC defines security incident as a "cybersecurity or physical security event that actually jeopardizes or has a significant likelihood of jeopardizing automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data"); Coalition Letter on Cyber Reporting to the Members of the Senate Committees on Intelligence, Homeland Security and Governmental Affairs and the House Committee on Homeland Security (Oct. 6, 2021), https://www.uschamber.com/assets/documents/211006_coalition_cyberincidentreporting_senateintel_senatehomeland_househomeland.pdf ("Businesses need clarity in reporting requirements, which should be targeted to well-defined and confirmed cyber incidents.").

[33] The Comment is intended to address the Commission's question 2. *See* 86 Fed. Reg. at 70064.

[34] *Id.*

security incidents in which such misuse "has occurred" as opposed to the amorphous "reasonably likely" language currently proposed.[35]

A well-defined notification requirement requires a clear threshold for reporting. That threshold should relate to known harms involving concrete financial injury to consumers. This specification achieves the Commission's goal of ensuring timely notification of critical security incidents while avoiding needlessly capturing the kind of information misuse that does not ultimately result in injury to consumers. Without this clarifying language, the amendment as written would compel financial institutions to over-report less-significant occurrences that do not cause harm and leave them subject to a potentially unconstitutional standard.

5. Consumer Notification Would be Duplicative[36]

As briefly referenced above, every U.S. state, as well as Washington, D.C. and many territories, have enacted legislation requiring that institutions notify consumers of data security breaches involving personally identifiable information. As noted above, withholding certain information from certain actors is sometimes justifiable if consumer confusion can be avoided. To that end, consumers should not be notified under the Safeguards amendment, given the plethora of other existing consumer-notification requirements.

In short, any additional requirement would be duplicative, overlapping, and would potentially violate the Regulatory Flexibility Act ("RFA").[37] The Commission indeed concedes that it does not know how many small entities could be impacted by its Proposed Amendment,[38] but has nonetheless proceeded with the Proposed Amendment despite not having sampled, surveyed, or otherwise accounted for the impact on small entities. Several members of the Associations are smaller entities, some of which are owned by minorities who have suffered from the discriminatory impact of prior federal rules. We accordingly object to the Commission's effort to proceed with the Proposed Amendment before informing itself of the impact of this Proposed Amendment while remaining uninformed of its impact on such small, minority-owned enterprises.

6. Delay for Law Enforcement Should be Respected[39]

The Commission also seeks comment as to whether the Proposed Amendment should contain a provision that allows law enforcement agencies to prevent or delay notification if notification will affect law-enforcement investigations. We support the inclusion of a good-faith law enforcement delay under any circumstance, whether or not the notice at issue is publicized, but such a requirement should include compliance with guidance from CISA, law enforcement, or the U.S. intelligence community. Surely a company should not be compelled by federal law to

---

[35] The Commission has in the past reserved to itself the ability to make ex-post facto judgments about the determinations regarding security events, and these efforts have been adjudicated to violate Due Process rights. Penalizing a company for failing to comply with an imprecise standard would violate due process of law because it would not give the company fair notice of the prohibited conduct. *See* LabMD v. FTC, 894 F.3d 1221 (11th Cir. 2018).

[36] The Comment is intended to address the Commission's question 8. *See* 86 Fed. Reg. at 70064.

[37] 5 U.S.C. § 601 et seq.

[38] 86 Fed. Reg. at 70066.

[39] The Comment is intended to address the Commission's question 4. *See* 86 Fed. Reg. at 70064.

report to the Commission when such a disclosure could harm national security, law enforcement investigations, or a coordinated federal response to the incident.

* * * * * *

SIFMA and BPI appreciate the opportunity to comment on this Proposed Amendment. If you have further questions or would like to discuss these comments further, please reach out to Melissa MacGregor at mmacgregor@sifma.org or Brian Anderson at brian.anderson@bpi.com.

Sincerely,

Melissa MacGregor

Melissa MacGregor
Managing Director & Associate General Counsel
SIFMA

Brian R. Anderson

Brian R. Anderson
Senior Vice President, Technology Regulation
Bank Policy Institute