Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

Writer's direct dial: +1 (202) 408-7407

CDIAONLINE.ORG

February 7, 2022

April Tabor, Secretary
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW.
Suite CC-5610 (Annex J)
Washington, D.C. 20580

Re: Safeguards Rule, 16 CFR 314, Project No. P145407

Dear Ms. Tabor:

This letter is submitted on behalf of the Consumer Data Industry Association ("CDIA"). CDIA is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals, and to help businesses, governments and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity, helping ensure fair and safe transactions for consumers, facilitating competition and expanding consumers' access to financial and other products suited to their unique needs. CDIA is an international trade association of companies that educates policymakers, consumers, and others on the benefits of using consumer data responsibly. CDIA also provides companies with information and tools to manage risks and protect consumers.

On December 9, 2021, the Federal Trade Commission ("Commission") published a notice of proposed rulemaking seeking comment on proposed amendments to the Safeguards Rule under the Gramm-Leach-Bliley Act ("GLBA"), which governs the security of customer information held by financial institutions (the "Proposal").[1] The Proposal was issued concurrently with final regulations amending significant aspects of the Safeguards Rule, requiring those financial institutions subject to the Commission's jurisdiction to make substantial revisions to their existing information security programs. 86 Fed. Reg. 70,272 (Dec. 9, 2021) ("Amended Safeguards Rule"). In the Proposal, the Commission seeks to impose yet another new obligation, specifically to require financial institutions to report to the Commission any "security event" where the financial institutions have determined that

---

[1] See proposed section 314.4(j), 86 Fed. Reg. 70,062, 70,067 (Dec. 9, 2021).

"misuse of customer information has occurred or is reasonably likely" to occur and where at least 1,000 consumers have been affected or reasonably may be affected.[2]

CDIA believes the Proposal is unnecessary given existing state breach notification requirements. Adding an additional notification requirement would be burdensome, costly, and redundant while also providing no countervailing consumer benefit. Thus, CDIA urges the Commission to decline to issue the revisions to the Amended Safeguards Rule suggested in the Proposal. If the Commission elects to go forward with the Proposal, however, CDIA believes that the Commission should amend its Proposal by limiting the notification requirement to those security events that could result in substantial harm or inconvenience to at least 1,000 customers, consistent with the legislative purpose behind the Safeguards Rule. CDIA also suggests a number of additional modifications to better harmonize the Proposal with existing state laws.

I. The Proposal seeks to impose an unnecessary and additional requirement on financial institutions.

The Commission's Proposal to require notification to the Commission of certain security events is unnecessary, counterproductive, and potentially duplicative. The Safeguards Rule already requires Commission-regulated entities, including consumer reporting agencies, to "[e]stablish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information" in the entity's control.[3] These written incident response plans must address: "[e]xternal and internal communications and information sharing" and "[d]ocumentation and reporting regarding security events and related incident response activities."[4] Thus, the Safeguards Rule already requires financial institutions subject to Commission jurisdiction to consider appropriate notifications as part of their response plans. CDIA sees little benefit in adopting a duplicative or more detailed and prescriptive requirement for notification.

Further, as the Commission is aware, CDIA members are subject to state breach notification laws in all states, the District of Columbia, and three U.S. territories. In general, these laws require any person, business, or data collector that "owns or licenses" computerized data containing personal information or sensitive personal information about a state resident to provide breach notifications to state residents whose information was compromised under defined circumstances.[5] Consumer reporting agencies generally own, or

---

[2] *Id.* at 70,067

[3] 16 C.F.R. § 314.4(h).

[4] *Id.* at § 341.4(h)(4),(6).

[5] *See, e.g.,* Cal. Civil Code § 1798.82; 815 I.L.C.S. 530/10(a); N.Y. Gen. Bus. Art. 39-F, § 899-AA-2; Tex. Bus. and Comm. Code § 521.053.

in some cases, license, personal information which they maintain in computerized form. These state laws provide adequate protection to consumers in connection with any data breaches consumer reporting agencies may experience, and the industry has established procedures to comply with these state breach notification requirements.

Accordingly, CDIA members are subject to a myriad of state law requirements to provide notice in the event of a breach, including notice to consumers and, for over a majority of states, notice to the state attorneys general or other state regulator. Each state sets forth different requirements with respect to the circumstances under which notice is required to the consumer and/or the state, as well as the timing and content of such notices. CDIA members have established procedures to comply with these state breach notification requirements.

The requirement to notify the Commission in addition to state regulators or law enforcement bodies would provide little consumer benefit beyond what state breach notification laws already provide. From CDIA's perspective, any federal breach notification requirement would only benefit consumers if it created a single national standard for when notice is required, reducing compliance costs, introducing additional certainty for businesses and consumers, and requiring notice only when doing so is appropriate based on potential harm to the subject consumers. By contrast, the Proposal would add an additional notification requirement without providing uniformity or certainty. Given the existing compliance burden on financial institutions under the Amended Safeguards Rule, the Commission should decline to impose an additional regulatory requirement, particularly one that provides no discernable benefit over that required by existing law. [6]

II. If the Commission choses to adopt the Proposal, the Commission should substantially revise the notification requirement to more closely align with the statutory purpose of the GLBA safeguards requirements and to harmonize with existing state laws.

If the Commission moves forward with its Proposal, the Commission should revise its proposal to better align its requirements with the purposes of the GLBA. Further, CDIA recommends a number of modifications to the Proposal to better align the requirements with existing state laws. Such revisions would reduce the regulatory burden, increase regulatory certainty, and reduce consumer confusion and notice fatigue.

[6] To the extent that the purpose of the notification requirement is to ensure that the FTC is aware of security events for potential data security investigations, CDIA notes that there are a number of resources that capture information about data breaches, including the Identity Theft Resource Center.

A. The Commission should revise the Proposal to require notification only when there has been harm to a customer or there is reasonably likely to be harm to a customer.

The current Proposal requires a financial institution to notify the Commission if it determines that "misuse of customer information has occurred or is reasonably likely and that at least 1,000 [customers][7] have been affected or reasonably may be affected."[8] The concept of "misuse" is undefined and overly broad and will sweep in incidents that involve no potential harm to consumers. Consistent with the purposes of the GLBA, the Commission should limit the requirement to provide notification only to those security events that involve a likelihood of some harm occurring to those customers.

Amending the Proposal to require harm is consistent with the statutory purpose of the Safeguards Rule, as set forth in Section 501(b)(3) of the GLBA, which requires the Commission to:

> establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards – … (3) to protect against the unauthorized access to or use of such records or information ***which could result in substantial harm or inconvenience to any customer***.[9]

CDIA urges the Commission to adhere to this Congressional directive and only require financial institutions subject to its jurisdiction to provide notice of a security event that could result in "substantial harm or inconvenience" to at least 1,000 customers.

Alternatively, CDIA encourages the Commission to align the trigger for its notification requirement with existing laws. One approach would be to limit the notification requirement to misuse resulting in a "reasonable likelihood of financial or economic harm," which standard would be consistent with a number of state laws.[10] At a minimum, the Commission should

---

[7] The Proposal uses the term "consumers." CDIA believes the appropriate term to be used is "customer" given that the misuse relates to "customer information" as is discussed in more detail section II.B below.

[8] 86 Fed. Reg. at 70,067.

[9] 15 U.S.C. § 6801(b) (emphasis added).

[10] *See, e.g.,* Ariz. Rev. Stat. 18-552(J) (establishing that a person is not required to make the notification "if the person, an independent third-party forensic auditor or a law enforcement agency determines after a reasonable investigation that a security system breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals."); Fla. Stat. Ann. § 501.171(c) (providing that "notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed."); and Iowa Code § 715C.2(6) (stating that "notification is not required, if after an appropriate

require notification only where there is at least a "reasonable likelihood" of any sort of harm, which would also be consistent with the data breach notification triggers in a number of states.[11]

B. The Commission should revise the Proposal to limit the notification obligation only when there has been a security event involving "sensitive customer information."

Under the Proposal, the misuse of "customer information" is sufficient to trigger the notification requirement. The Safeguards Rule broadly defines the term "customer information" to mean "any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form that is handled or maintained by or on behalf of [the financial institution] or [it's] affiliates."[12] CDIA encourages the Commission to require notification only when "sensitive customer information" is involved, as defined in the Federal Financial Institutions Examination Council Guidance (FFIEC Guidance).

Under the FFIEC Guidance, "sensitive customer information" is defined to mean

> a customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. It also includes any combination of components of customer information that would allow someone to log on to or access the customer's account, such as user name and password or password and account number.[13]

---

investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach.").

[11] *See, e.g.*, statutes cited in n. 9, *supra*; Ala. Code § 8-38-5(a) ("A covered entity that is not a third-party agent that determines under § 8-38-4 that, as a result of a breach of security, sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates, must give notice of the breach to each individual."); La. Rev. Stat. § 51:3-7074 ("Notification as provided in this Section shall not be required if after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to the residents of this state.").

[12] 16 C.F.R. § 314.2(d).

[13] The Federal Financial Institutions Examination Council, "Final Guidance on Repose Programs – Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," at 3, *available at* https://www.fdic.gov/news/financial-institution-letters/2005/fil2705.html (last visited February 2, 2022).

This modification would keep the notification requirement in line with the FFIEC Guidance and most state laws.[14]

C. The Commission should revise the Proposal to limit the notification obligation to security events involving unencrypted sensitive customer information.

One of the substantial changes in the new Amended Safeguards Rule is the requirement of encryption. *See* 16 C.F.R. § 314.4(c) (requiring that safeguards include protecting "by encryption [of] all customer information held or transmitted by [the financial institution] both in transit over external networks and at rest"). Consistent with this change in the Safeguards Rule, CDIA suggest that the Commission harmonize the notification requirement and limit the requirement to notify the Commission only when *unencrypted* sensitive customer information is at issue or, alternatively, to exclude from the notification requirement any security event that involves encrypted information. This revision also would align the Commission's requirements with those of several states.[15]

---

[14] Generally, state data breach laws are triggered only when the information includes the type of information that could be used to access accounts or commit identity theft. For example, in Florida, the breach law applies to information consisting of an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (a) Social Security Number; (b) a driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (c) a financial account number or credit or debit card number in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; (d) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (e) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. Fla. Stat § 501.171.

[15] For example, Georgia requires that "any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Ga. Code Ann. § 10-1-912(a). Nevada provides that "any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Nev. Rev. Stat. § 603A.220(1). California provides that an entity must disclose a breach in the security of data to any California resident "(1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable." Cal. Civ. Code § 1798.29(a). Indiana provides that a "breach of the security of data" does not occur where there is "unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key: (A) has not been compromised or disclosed; and (B) is not in the possession of or known to the person, without authorization, acquired or has access to the portable electronic device." Ind. Code Ann. § 24-4.9-2-2(b)(2).

D. Proposed timing requirement is practicable.

The Proposal would require financial institutions to notify the Commission "as soon as possible, and no later than 30 days after discovery of the event."[16] CDIA supports the inclusion of a definitive time within which notification must be made, if notification is ultimately required. Further, given the investigation that must be conducted internally regarding any potential security event to determine whether misuse has occurred, CDIA suggests that any timeframe shorter than 30 days is not practicable. [17]

E. Publication of reported information is unnecessary and fails to achieve policy goals.

The Commission proposes to "input the information it receives from affected financial institutions into a database that it will update periodically and make available to the public."[18] Publishing the information provided by affected financial institutions is unnecessary and fails to achieve the Commission's stated purposes. In the Proposal, the Commission stated that requiring notifications to the Commission would "ensure that the Commission is aware of security events that could suggest a financial institution's security program does not comply with the [Safeguards] Rule's requirements, thus facilitating Commission enforcement of the [Safeguards] Rule."[19] Publishing the information obtained from such notifications would do nothing to help the Commission achieve its stated aim of enforcement – the Commission would have already obtained the necessary information through receipt of the notification itself.

Further, there is no added consumer benefit to making the information publicly available. As stated above, all fifty states as well the District of Columbia, and three U.S. territories impose data breach notification requirements on financial institutions. Consumers are thus already directly notified when a potential data breach has occurred. As further discussed in the next Section, publication of this information by the Commission could lead to further consumer confusion and angst about whether the consumer's information has been compromised.

---

[16] 86 Fed. Reg. at 70,067.

[17] However, if the Commission is inclined to make information regarding notifications public, which CDIA opposes (see section II.E below), the Proposal should be amended to allow law enforcement agencies to prevent or delay notification to the Commission in the event notification would affect law-enforcement investigations.

[18] 86 Fed. Reg. at 70,064.

[19] *Id.* at 70,066.

F. Requiring customer notification is unnecessarily duplicative and potentially harmful.

The Commission also requested comment regarding whether notification to customers, as well as the Commission, should be required. Amending the Safeguards Rule to require customer notification is unnecessarily duplicative of existing state law requirements and has the potential to result in consumer harm.

As outlined in greater detail above, the states, the District of Columbia, and three U.S. territories already impose consumer breach notification requirements. Adding an additional notification requirement would be burdensome, costly,[20] and redundant. Further, imposing an additional notification requirement could be harmful to consumers. Because state law already requires companies to notify consumers in the event of a security incident, imposing a separate notification requirement under the Safeguards Rule could result in a consumer receiving multiple notices regarding the same security incident. This in turn could cause a consumer to believe that they have been the victim of multiple data breaches, when in fact, only one data breach has occurred.

Additionally, if multiple notices are provided to consumers about a single data breach, consumers could start to suffer from notice fatigue. CDIA and its members agree that consumers should be notified if there is a reasonable likelihood of harm to the consumer; however, multiple notifications regarding the same incident may only serve to inundate and overwhelm consumers. At some point it is reasonable for consumers to start to ignore the notices if they get them often enough. This would be counterproductive to the notice requirement in the first instance and be detrimental to consumers in the long run.

G. If the Commission determines notification to customers is necessary, the Commission should only require notification under certain conditions.

The Commission also requested comment regarding the conditions that should be in place if notification to customers is required.

Most importantly, to help reduce the risk of consumer confusion and notice fatigue as discussed above, CDIA feels it is of the utmost importance that security event notifications under the Proposal not be required if the customer has already received, or will otherwise receive, a notice about the security event because of a state law requirement or any other reason.

---

[20] According to a 2021 study conducted by IBM, the average notification costs incurred as part of a data breach totaled $27,000. Duplicating the notification requirement would greatly increase these average costs. *See* IBM Security, "Cost of Data Breach Report 2021," *available at* https://www.ibm.com/downloads/cas/OJDVQGRY (last visited January 25, 2022).

Additionally, consistent with CDIA's earlier comments with respect to notification to the Commission, notification to customers should only be required under certain limited circumstances. Specifically, notification to customers should only be required when there has been a security event involving unencrypted sensitive customer information that could result in "substantial harm or inconvenience" to a customer.

CDIA's previous observations regarding the timing[21] of any required notices applies to notices to customers as well. In addition, the Proposal should be amended to allow law enforcement agencies to prevent or delay notification in the event notification would affect law-enforcement investigations. Most state data breach notification statutes provide for a law enforcement delay. For example, California, Florida, and New York permit notification to consumers be delayed if the law enforcement agency determines that notification will impede a criminal investigation.[22] Adding a similar exception to any security event notification requirement under the Proposal would help harmonize required state notifications and allow federal or state law enforcement agencies to effectively conduct criminal investigations related to the security event.

* * *

We appreciate the opportunity to comment on the Commission's proposed amendments to the Safeguards Rule, and hope the Commission will find these comments useful.

Sincerely,

Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs

[21] As discussed above, a period of less than 30 days after the discovery of a security event is impracticable.

[22] Cal. Civ. Code § 1798.29(c); Fla. Stat. Ann. § 501.171(4)(b); N.Y. Gen. Bus. Law § 899-aa(4).