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

August 2, 2019

April Tabor, Acting Secretary
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW.
Suite CC-5610 (Annex B)
Washington, D.C. 20024

**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. The CDIA is an international trade association with over 140 corporate members 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 April 4, 2019, the Federal Trade Commission ("FTC") published a notice of proposed rulemaking seeking comment on proposed amendments to the Safeguards Rule under the Gramm-Leach-Bliley Act ("GLBA"), which govern the security of customer information held by financial institutions.[1]

The current Safeguards Rule requires a financial institution to develop, implement, and maintain a comprehensive information security program. The FTC is now proposing changes to add more detailed requirements for what must be included in the information security program mandated by the Rule. The proposal generally would require financial institutions to:

(1) encrypt all customer data;

(2) implement access controls to prevent unauthorized users from accessing customer information; and

(3) use multifactor authentication to access customer data.

[1] 84 Fed. Reg. 13158 (April 4, 2019).

In addition, the proposal would require companies to submit periodic reports to their boards of directors and clarify the Rule's scope in the regulation itself.

CDIA is concerned that the proposed rule trades away the benefits of the current Rule's flexibility for a more rigid approach to compliance that is counterproductive. Today's Safeguards Rule allows a flexible approach appropriate to a company's size and complexity. This proposal would remove many benefits of that approach, even though it is unclear whether there would be any benefits in return for that trade-off. In addition, not all of the perceived shortcomings the FTC intends to address concern firms covered by the Safeguards Rule and may not represent a broad trend justifying a regulatory response. Indeed, in the 16 years in which the Safeguards Rule has been in effect, the FTC has brought at total of only 14 cases under the Rule, and only 3 cases within the past 5 years. To the extent that the Commission is basing these changes on some perceive need for regulation, CDIA submits that the data does not support this conclusion.

Moreover, CDIA believes that now may not be the best time for the proposed regulations. Many of the proposed changes are based on regulations promulgated only two years ago by the New York State Department of Financial Services, and there has not been sufficient time to gauge the impact of those regulations. Furthermore, the proposal overlaps with issues that Congress is currently debating as it contemplates potential privacy and data security legislation. These topics are part of a larger national policy debate that is most appropriately left to Congress to resolve.

**Proposed Amendments to Section 314.1: Purpose and Scope**

The proposed amendment would add language from section 313.1(b) of the Privacy Rule, relating to the scope of the Rule and the definition of financial institution, to section 314.1(b) of the Safeguards Rule. Section 314.1(b) states that the Safeguards Rule applies to the handling of customer information by all financial institutions over which the Commission has jurisdiction. The proposed amendment sets forth the general definition of "financial institution" and provides examples of financial institutions under the Commission's jurisdiction, such as finance companies and mortgage brokers.

The Federal banking agencies' Interagency Guidelines apply to "customer information maintained by or on behalf of" banks or other entities regulated by the particular regulator.[2] Similarly, the Interagency Guidelines define "customer information," to mean "any record containing nonpublic personal information, ... , about a customer, ... , that is maintained by or on behalf of the bank."[3] Thus, the Federal banking agencies limit the scope of the Interagency Guidelines and the "customer information" it covers to information about a customer of the bank or other regulated entity subject to the agency's jurisdiction.

By contrast, when the FTC adopted its Safeguards Rule in 2002, it decided to apply the rule not only to information about the financial institution's own customers, but also to information that a financial institution receives from another financial institution about the latter institution's customers. The scope section of the FTC's Safeguards Rule provides that "[t]his part applies to all customer information in your possession, regardless of whether such information pertains to individuals with

---

2 *See, e.g.,* 12 C.F.R. Part 208, Appendix D-2, at I.A.

3 *See, e.g.,* 12 C.F.R. Part 208, Appendix D-2, at I.C.1.c.

whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you."[4] To effectuate this broad scope, the FTC also defined "customer information" to mean "any record containing nonpublic personal information ... about a customer of a financial institution, … , that is handled or maintained by or on behalf of you or your affiliates."[5]

The FTC's approach subjects consumer reporting agencies to the requirements of the Safeguards Rule, even though the customers of consumer reporting agencies are companies that purchase consumer reports for credit, insurance, employment, and other permissible eligibility purposes, and not consumers whose information consumer reporting agencies assemble and maintain for the purpose of providing consumer reports to third parties.[6] Other types of entities also may be covered by the Safeguards Rule on the same basis, including debt collectors, independent check cashers, and automated teller machine operators.[7]

In response to commenters' concerns about the broad reach of the original Safeguards Rule, the FTC stated that "the flexible requirements of the Rule—which allow the safeguards to vary according to the size and complexity of a financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue—permit entities to develop safeguards appropriate to their operations and should minimize any burdens on recipient entities."[8] The changes now proposed by the FTC eliminate much of the flexibility of the original Safeguards Rule and impose significant costs on those covered by the Rule (even with the limited exemptions proposed by the Commission). Given the broad scope of the FTC's Safeguards Rule, we believe that the original flexibility of the Rule should be maintained. If the Commission adopts the revised Rule as proposed, however, CDIA believes that it is appropriate for the FTC to revisit the scope of the Rule or, alternatively, exclude those financial institutions that are covered by virtue of their receipt of information from another financial institution from the more costly requirements of the proposed amended Rule.

**Proposed Amendment to Section 314.2: Definitions**

The proposed amendments to section 314.2 add definitions to terms introduced in the proposed amended Rule. The proposed amendments do not alter or remove any definitions in the existing Rule.

Proposed paragraph (b) would define an "authorized user" of an information system as any employee, contractor, agent or other person that participates in the business operations of an entity and is authorized to access and use any of that financial institution's information systems and data. This term is used in proposed section 314.4(c)(10), which requires financial institutions to implement policies to monitor the activity of authorized users and detect unauthorized access to customer information.

Proposed paragraph (c) would define a "security event" as "an event resulting in unauthorized access to, or disruption or misuse of, an information system or information stored on such information

4 16 C.F.R. § 314.1(b).
5 16 C.F.R. § 314.2(b).
6 67 Fed. Reg. 36,484, 36,485-86 (May 23, 2002).
7 *See* 67 Fed. Reg. at 36,485 & note 21.
8 67 Fed. Reg. at 36486.

system." CDIA believes that "disruption" is too broad and would include a number of incidents that have nothing to do with the security of consumer information. For example, if an information system were to go off line, it would be a "disruption," but there may not necessarily be security risks associated with such disruption. Further, given the auditing and reporting requirements, a "security event" should be one that is material, meaning that it presents a security risk to a consumer. CDIA requests that the definition of a "security event" be limited to one that is (a) material, (b) involves a confirmed security incident, and (c) involves "customer information" as that term is defined by the Rule.[9]

Proposed paragraph (e) would define "encryption" as "the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key." This term is used in proposed section 314.4(c)(4), which generally requires financial institutions to encrypt customer information, with certain exceptions.

Proposed paragraph (h) would define "information system" as "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems." It is not clear that this definition is limited to systems involving *customer information*, which is the information that the Safeguards Rule seeks to protect. CDIA requests that the Commission clarify this definition.

Proposed paragraph (i) would define "multi-factor authentication" as "authentication through verification of at least two of the following types of authentication factors: 1. Knowledge factors, such as a password; 2. possession factors, such as a token; or 3. inherence factors, such as biometric characteristics." This term is used in proposed section 314.4(c)(6), which requires financial institutions to implement multi-factor authentication for individuals accessing "internal networks" that contain customer information. The term "internal network" is not defined, which creates ambiguity in the application of the multi-factor authentication requirement. Because of this ambiguity, this definition could be read to suggests that such authentication would be required for every program within an information system, which would be unworkable. CDIA recommends that this definition be modified to referred to "information system" (the term defined in proposed section 314.2(h)).

**Proposed Amendments to Section 314.4: Elements**

The proposed amendments to section 314.4 would alter existing required elements of an information security program and adds several new elements. In addition to its general comments above that these changes are unnecessary, CDIA provides specific comments on a number of the elements below.

---

[9] *See, e.g.,* 12 C.F.R. Part 208, Appendix D-2, at I.C.1.c. With respect to materiality, the Department of Defense's Cyber Incident and Reportable Cyber Event Categorization standard provides guidance on categorizing "reportable" events from those that do not rise to that level. https://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651001.pdf?ver=2016-02-05-175710-897 at Appendix A to Enclosure B.

**Proposed Paragraph (a)**

Amended paragraph (a) would expand the current requirement of designating an "employee or employees to coordinate your information security program" by requiring the designation of a single qualified individual responsible for overseeing and implementing the financial institution's security program and enforcing its information security program. This individual is referenced in the Rule as a Chief Information Security Officer or "CISO." To the extent a financial institution meets this requirement by using a service provider or affiliate, however, the proposed amendment would require that the financial institution still: 1. Retain responsibility for compliance with the Rule; 2. designate a senior member of its personnel to be responsible for direction and oversight of the CISO; and 3. require the service provider or affiliate to maintain an information security program that protects the financial institution in accordance with the Rule. The FTC has explained that these proposed amendments are designed to ensure that, even when the financial institution outsources the CISO function, the financial institution retains responsibility for its own information security.

CDIA believes that this change greatly reduces the current flexibility of the Safeguards Rule and elevates form over substance. The current Safeguards Rule allows financial institutions to designate more than one employee to coordinate the information security program. For complex organizations, this type of flexibility may be needed to allow the organization to share responsibilities among different personnel with different strengths (such as personnel focused on physical security and personnel focused on the security of computer systems).

The FTC further states that it believes that the single CISO requirement would "lessen the possibility that there will be gaps in responsibility between individuals" and "increase accountability for the security of financial institutions' information systems." It is not clear how the single CISO requirement will achieve these goals. CDIA is not aware of any actions brought under the Safeguards Rule or similar laws that identify security failures that have resulted from the failure to have a single CISO. Further, although the FTC has requested any data to discuss the risks and benefits of this proposal, CDIA notes that the of Basis and Purpose for the proposed rule does not explain how a single CISO requirement will achieve the FTC's goals, nor does the proposed rule does not identify any evidence in support of this proposal.

**Proposed Paragraph (b)**

Proposed section 314.4(b)(1) would require that risk assessments be written, and that such risk assessments describe how the financial institution will mitigate or accept any identified risks and how the financial institution's information security program will address those risks. It is unclear from the FTC's proposal what level of specificity is required with respect to these written "risk assessments." CDIA is concerned that a requirement that risks and remediation plans be spelled out in detail could themselves become a roadmap for a security breach. If the FTC adopts this requirement, it should make clear that the financial institution need only include such detail as necessary to inform the overall structure of its information security program. Because a number of CDIA members receive information from financial institutions covered by the FFIEC guidelines, CDIA recommends that the Commission ensure that this requirement is no more onerous than that adopted by the prudential federal regulators. Alternatively, CDIA recommends that the FTC clarify the threshold for the risks to be identified in such

an assessment. Otherwise, a thorough assessment of all risks could produce hundreds of pages of risks identified as low/non-critical.

**Proposed Paragraph (c)**

Proposed paragraph (c) retains the existing Rule's requirement for financial institutions to design and implement safeguards to control the risks identified in the risk assessment. Notably, however, proposed paragraph (c) also adds more detailed requirements for what these safeguards must include. Although CDIA and its members appreciate the additional guidance that the FTC is seeking to provide through these detailed requirements, we are concerned that the proposed rule does not provide sufficient flexibility, as described on p. 2 above and more fully below.

Proposed paragraph (c)(2) would require financial institutions to "[i]dentify and manage the data, personnel, devices, systems, and facilities that enable [the financial institution] to achieve business purposes in accordance with their relative importance to business objectives and [the financial institution's] risk strategy." CDIA requests that the FTC clarify this requirement, including how the "relative importance to business objectives and risk strategy" should be evaluated.

Proposed paragraph (c)(3) would require that financial institutions restrict access to physical locations containing customer information only to authorized individuals. In the proposed rule, the FTC explains that this requirement is designed to protect physical locations and may include controls ranging from restricting access to work areas where personnel are using hard copies of customer information or requiring physical locks on filing cabinets containing customer information. CDIA is concerned that the proposed rule as written appears to require that restricting access to work areas is required, which may not be feasible for smaller businesses. CDIA recommends that the FTC consider including this important clarification in the text of the Rule.

Proposed paragraph (c)(4) would generally require financial institutions to encrypt all customer information, both in transit and at rest. The proposed amendment does, however, permit financial institutions to use alternative means to protect customer information, subject to review and approval by the CISO. CDIA supports this approach, as it provides financial institutions with the discretion and flexibility needed to address the impact of encryption on the real-time delivery of services, for example, and to allow for compensating controls where encryption is infeasible.

Proposed paragraph (c)(5) would establish a requirement that financial institutions "[a]dopt secure development practices for in-house developed applications utilized" for "transmitting, accessing, or storing customer information." Although CDIA recognizes the FTC's concern that financial institutions address the security of software they develop to handle customer information, it is unclear why this specific requirement is necessary and why it distinguishes from applications developed in house as opposed to those obtained and acquired from third parties. Regardless of the genesis of the software, financial institutions would be subject to the overall requirement to safeguard customer information, and it is not clear that this requirement provides additional direction or clarity to financial institutions.

Amended paragraph (c)(6) would require financial institutions to "implement multi-factor authentication for any individual accessing customer information" or "internal networks that contain customer information." The Commission views multi-factor authentication as a minimum standard to

allowing access to customer information for most financial institutions. To the extent that a financial institution finds that a method other than multi-factor authentication offers reasonably equivalent or more secure access controls, the institution may adopt that method with the written permission of its CISO. As noted above on p. 4, this requirement uses the term "internal network," which is undefined. Because of this ambiguity, this definition could be read to suggests that such authentication would be required for every program within an information system, which would be unworkable. CDIA recommends that this definition be modified to referred to "information system," which is defined in the proposed rule. CDIA supports the FTC's proposal to provide for the flexibility to adopt other controls that are reasonably equivalent.

Amended paragraph (c)(7) would require information systems under the Rule to include audit trails designed to detect and respond to security events. At the outset, CDIA notes that audit trails themselves do not detect or respond, but are used to detect and respond to security events. CDIA believes that the phrase "for use in" should be added to this paragraph.

With respect to the specific requirement, the proposed rule does not provide the same flexibility for this requirement as it does with encryption or multi-factor authentication, namely the ability of the CISO to approve the use of alternative compensating controls. Depending upon the level of detail of activities captured in logs from system to system, such logs may become noise that hinders a company's ability to identify true risks to their organization. Further, not all systems have a logging capability, and there may be situations where this requirement is infeasible. CDIA requests that the FTC adopt an approach similar to the one taken with respect to other requirements and permit flexibility.

Amended paragraph (c)(8) would require financial institutions to develop procedures for the secure disposal of customer information in any format that is no longer necessary for their business operations or other "legitimate business purposes." CDIA understands that the FTC is concerned with the risks associated with the retention of records, and appreciates the flexibility in the language of this provision, specifically the fact that the Commission does not define "legitimate business purposes." As noted above, the FTC's Safeguards Rule covers a wide variety of financial institutions, many of which research and explore a variety of uses of data to improve decision making and risk management to the benefit of industry and consumers. For these reasons, CDIA opposes any requirement to affirmatively demonstrate "a current need" for customer information that is retained. Given the existing protections and restrictions on the use of data by financial institutions, including the Privacy Rule and the Fair Credit Reporting Act, we believe any such requirement would stifle innovation and development.

The Commission seeks comment on whether the Rule should define legitimate business purposes to exclude certain uses of customer information, but does not provide any suggestions or directions with respect to the type of uses that the FTC believes should not be considered a "legitimate use." For the reasons expressed above, CDIA does not believe that such a line drawing exercise is appropriate in the context of a rule. If, however, the FTC decides to consider any such limitations, it should put such exclusions out for further comment prior to adoption. CDIA similarly opposes the adoption of any requirement to develop procedures to limit the collection of customer information "that is not necessary for business operation or other legitimate business purposes."

Finally, in response to the Commission's request for comments on whether the Safeguards Rule should require the destruction of certain types of data after a fixed period, CDIA believes that any such

requirement is beyond the scope of the rule and the Commission's authority. The Gramm-Leach Bliley Act authorizes the FTC to "establish appropriate standards ... relating to administrative, technical, and physical safeguards – (1) to insure the security and confidentiality of customer records and information; (2) to protect against any unanticipated 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." 15 U.S.C. § 6801(b). Nothing in the law authorizes the FTC to require the destruction of records, only to establish standards to protect customer records and information. Further, CDIA is not aware of any federal or state law that requires the destruction of certain types of data after a fixed period.

**Proposed Paragraph (d)**

Proposed paragraph (d)(1) would retain the current Rule's requirement that financial institutions "[r]egularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems." The primary change in this section is to add proposed paragraph (d)(2), which states that the monitoring and testing "shall include" either "continuous monitoring" or "periodic penetration testing and vulnerability assessments." If a financial institution does not adopt effective continuous monitoring, under the proposed amendments it would be required to engage in periodic penetration testing and vulnerability assessment consisting of no less than annual penetration testing based on the financial institution's risk assessment and biannual vulnerability assessments designed to detect publicly known vulnerabilities.

CDIA is concerned that the options presented here – either "continuous monitoring" or annual penetration testing and biannual vulnerability assessments – are too inflexible for the variety of businesses covered by the Commission's Safeguards Rule. A company could choose other methods of testing the effectiveness of their systems that would be equally effective. The prescriptive nature of this requirement also discourages innovation in data protection.

**Proposed Paragraph (h)**

Proposed paragraph (h) would require financial institutions to establish incident response plans. The written response plans would be required to be "designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information" in the financial institution's possession. The amendment would require the incident response plans to address the following areas: 1. The goals of the incident response plan; 2. the internal processes for responding to a security event; 3. the definition of clear roles, responsibilities and levels of decision-making authority; 4. external and internal communications and information sharing; 5. identification of requirements for the remediation of any identified weaknesses in information systems and associated controls; 6. documentation and reporting regarding security events and related incident response activities; and 7. the evaluation and revision as necessary of the incident response plan following a security event.

CDIA believes it is unnecessary, counterproductive, and potentially duplicative to require an information security program to include a response plan in the event of a data breach. At the outset, CDIA interprets the FTC's existing Safeguards Rule as broad enough to encompass appropriate response

plans. Specifically, the FTC's Safeguards Rule requires FTC-regulated entities, including consumer reporting agencies, to "[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information ... , and assess the sufficiency of any safeguards in place to control these risks."[10] The Safeguards Rule explicitly provides that such a risk assessment should include, at a minimum, consideration of risks related to "[d]etecting, preventing and *responding* to attacks, intrusions, or other systems failures."[11] Thus, the Safeguard Rule already references what is, in effect, a plan for responding to data breaches and similar events. Consequently, CDIA sees little benefit in adopting a duplicative or more detailed and prescriptive requirement than what already exists in the current Safeguards Rule.

CDIA recognizes that the Federal banking agencies' Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("Interagency Guidance") specifically address response programs in greater detail than the FTC's Safeguards Rule.[12] The Interagency Guidance builds upon a high-level reference to response programs in the Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Interagency Guidelines"), the Federal banking agencies' version of the Safeguards Rule.[13] The Interagency Guidelines provide that, in managing and controlling risk, regulated entities must consider whether to adopt "[r]esponse programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies."[14] The Interagency Guidance goes further by focusing specifically on response programs and the key components of a bank's response program, including:

(1) assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;

(2) notifying the bank's primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;

(3) notifying appropriate law enforcement authorities and filing a timely Suspicious Activity Report ("SAR");

(4) taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts; and

(5) notifying customers when warranted.[15]

---

10 16 C.F.R. § 314.4(b).

11 16 C.F.R. § 314.4(b)(3) and (c) (emphasis added).

12 70 Fed. Reg. 15,736 (Mar. 29, 2005). CDIA notes that the FTC cites to the regulations promulgated by the New York State Department of Financial Services ("New York DFS") in support of this proposed requirement, but CDIA notes that such requirements apply to those entities that are subject to examination by the New York DFS, and are distinguishable in the same way that the Interagency Guidelines are.

13 66 Fed. Reg. 8,616 (Feb. 1, 2001).

14 *See, e.g.,* 12 C.F.R. Part 208, Appendix D-2, at III.g.

15 70 Fed. Reg. at 15,752.

CDIA believes that the response programs described in the Interagency Guidance would not translate well into the FTC's Safeguards Rule for the following reasons. First, the response programs described in the Interagency Guidance assume an ongoing supervisory relationship between a Federal banking regulator and a banking institution, including the kind of ongoing interaction that would provide a natural means for a bank to notify its primary regulator of an incident and to seek and obtain guidance with respect to the type of incidents that should be subject to notification. The FTC does not supervise the entities subject to its jurisdiction, and thus lacks the framework and structure for the same kind of regulatory notification provision and ongoing interaction with regulated entities that the Federal banking agencies have.

Under the Interagency Guidance, when a banking entity experiences a data breach, the bank notifies its primary Federal regulator and the bank and its regulator collectively assess the circumstances and decide if, to what extent, and when customer notification is warranted, subject to state law requirements. The FTC, as noted above, has no supervisory relationship with the entities it regulates and is not similarly equipped to negotiate, on a case-by-case basis, different notice outcomes with financial institutions based on what the circumstances warrant, particularly in view of the broad scope of the FTC's Rule. Consequently, CDIA is concerned that the FTC may propose a blanket rule requiring notification of customers when a breach occurs without regard to whether such a notice would be in the best interests of consumers, a result far different than the iterative model followed by the Federal banking agencies.

In the context of this requirement, the Commission seeks comment on whether the proposed amendment should require that financial institutions report security events to the Commission and, if so, what the elements of such a provision should be. Specifically, the Commission seeks comment on 1. the appropriate deadline for reporting security events after discovery; 2. whether all security events should require notification or whether notification should be required only under certain circumstances, such as a determination of a likelihood of harm to customers or that the event affects a certain number of customers; 3. whether such reports should be made public; 4. whether the events involving encrypted information should be included in the requirement; and 5. whether the requirement should allow law enforcement agencies to prevent or delay notification if notification would affect law-enforcement investigations.

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.[16] Consumer reporting agencies generally own, or 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. CDIA also notes that in 2018, Congress amended the FCRA to provide for the ability of all U.S. consumers, including those notified of data breaches, to limit consumer

[16] *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.

reporting agencies from releasing consumer reports or information from consumer reports without the consumer's authorization.

Each of the states sets forth its own trigger for when notice to consumers and/or notice to the state is required. The requirement to notify the FTC in addition to consumers 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.

**Proposed Paragraph (i)**

Proposed paragraph (i) sets forth a reporting requirement, requiring that the CISO "report in writing, at least annually, to [the financial institution's] board of directors or equivalent governing body" regarding the following information: 1. The overall status of the information security program and financial institution's compliance with the Safeguards Rule; and 2. material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program. For financial institutions that do not have a board of directors or equivalent, the CISO must make the report to a senior officer responsible for the financial institution's information security program.

CDIA agrees with the Commission that regular reporting is an important component of good compliance management, but is concerned that this requirement seems unnecessary. First, if a company is employing appropriate safeguards, it is already engaged in regular reporting as a part of its information security plan. Further, the CISO or equivalent already is charged with appropriate overseeing the information security plan, which oversight includes reporting to management as necessary. CDIA is concerned that the requirement of an annual written report is driven primarily by the desire of the FTC to have such information available in the event of an investigation. In addition, this specific requirement seems unnecessary in light of the proposed requirement for periodic written risk assessments and regular updating of the written information security plan.

The Commission also has requested comment on whether the proposed rule should also require the Board or equivalent governing body "to certify compliance with the Rule." Such a proposal would require the Board to gain a level of expertise with information security that may not be achievable and appears at odds with the separate requirement for a financial institution to employ a CISO or equivalent. If a financial institution employs a CISO, it should be able to rely on that CISO's expertise with respect to compliance with the Safeguards Rule. Further, this requirement appears to elevate form over substance, and encourages a "checkbox" approach to security that provides little value.

**Proposed Amendments to Section 314.5: Effective Date**

The proposed rule only provides to six (6) months to comply with the myriad of new requirements under the amended Safeguards Rule, specifically (a) the requirements to appoint a CISO

(314.4(a)), (b) the requirement to conduct a written risk assessment (314.4(b)(1)), (c) the incorporation of the new elements into the information security program (314.4(c)(1)-(10)), (d) the requirement to establish either continuous monitoring or annual penetration testing and biannual vulnerability assessments (314.4(d)(2)), (e) the training requirements (314.4(e)), (f) periodic assessment of service providers (314.4(f)(3)), (g) the development of a written incident response plan (314.4(h)), and (h) annual reports from the CISO (314.4(i)). Given the breadth and scope of the new requirements, and the far reach of the Commission's Rule, six months is insufficient time to incorporate these requirements. For example, many of the new requirements should be executed at the request or direction of a CISO or equivalent, and for those financial institutions that do not currently employ a CISO, that search alone can take 9-12 months, depending on the size of the financial institution and its complexity.[17] CDIA notes that when the original Safeguards Rule was adopted, which rule provides for more flexibility, the Commission provided one year for compliance.[18] CDIA suggests that, at a minimum, the FTC should provide for at least that length of time here.

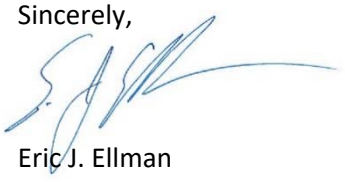
**Proposed Section 314.6: Exceptions**

Proposed section 314.6 is a new section that would exempt financial institutions that maintain concerning fewer than 5000 consumers from certain requirements of the amended Safeguards Rule. Such financial institutions would not be required to comply with the following subsections: 314.4(b)(1), requiring a written risk assessment; 314.4(d)(2), requiring continuous monitoring or annual penetration testing and biannual vulnerability assessment; 314.4(h), requiring a written incident response plan; and 314.4(i), requiring an annual written report by the CISO. As explained above at pp. 2-3, given the broad scope of the FTC's Safeguards Rule, CDIA requests that, if the Commission adopts the revised Rule as proposed, the Rule also should exclude those financial institutions that are covered by virtue of their receipt of information from another financial institution from these provisions of the amended Rule

* * *

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

Sincerely,



Eric J. Ellman

[17] CDIA also notes that the CISO responsibility provisions of the proposed rule will have a negative impact on the talent pool willing to take on this role for financial institutions, so these searches may take longer.

[18] 67 Fed. Reg. 36484 (May 23, 2003).