



November 21, 2016

Donald S. Clark
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; and
Disposal Rule, 16 CFR part 682, Project No. 165410**

Dear Mr. Clark:

This letter is submitted on behalf of the Consumer Data Industry Association (“CDIA”). 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. The CDIA also provides companies with information and tools to manage risks and protect consumers.

On September 7, 2016, the Federal Trade Commission (“FTC”) issued a Federal Register Notice requesting public comment on possible amendments to its rule regarding Standards for Safeguarding Customer Information (“Safeguards Rule”).¹ On September 15, 2016, the FTC issued a Federal Register Notice requesting public comment on possible amendments to its rule regarding Disposal of Consumer Report Information and Records (“Disposal Rule”).² On November 4, 2016, the FTC extended the comment period on the Safeguards Rule notice from November 7, 2016, to November 21, 2016, to correspond with the close of the comment period for the Disposal Rule notice.³ This letter focuses on two potential changes to the existing Safeguards Rule and Disposal Rule that the CDIA believes would be costly and burdensome for industry, while providing little or no benefit to consumers. In addition, the CDIA asks the FTC to amend the scope of its Safeguards Rule to make it more consistent with the Federal banking agencies’ guidelines for safeguarding customer information.

¹ 81 Fed. Reg. 61,632 (Sept. 7, 2016).

² 81 Fed. Reg. 63,435 (Sept. 15, 2016).

³ 81 Fed. Reg. 80,011 (Nov. 15, 2016).

In other respects, the CDIA appreciates the existing flexibility provided by the Safeguards Rule and the Disposal Rule. Aside from the limited change in scope discussed below, the CDIA does not believe that any other changes to the Safeguards Rule or the Disposal Rule are necessary or warranted, absent a compelling demonstration of a specific harm, the identification of a proposed remedy that would address that harm, and a cost-benefit analysis that would justify adoption of the proposed remedy.

The Safeguards Rule Should Not Be Amended to Require a Response Plan in the Event of a Data Breach.

In its request for public comment regarding the Safeguards Rule, the FTC asks if “the elements of an information security program [should] include a response plan in the event of a breach that affects the security, integrity, or confidentiality of customer information.”⁴ The 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.

The 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.”⁵ 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.”⁶ Thus, the Safeguard Rule already references what is, in effect, a plan for responding to data breaches and similar events. Consequently, the CDIA sees little benefit in adopting a duplicative or more detailed and prescriptive requirement than what already exists in the current Safeguards Rule.

The 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.⁷ 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.⁸ The Interagency Guidelines provide that, in managing and controlling risk,

⁴ 81 Fed. Reg. at 61,634.

⁵ 16 C.F.R. § 314.4(b).

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

⁷ 70 Fed. Reg. 15,736 (Mar. 29, 2005).

⁸ 66 Fed. Reg. 8,616 (Feb. 1, 2001).

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.”⁹ 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.¹⁰

The 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. 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.

In addition, consumer reporting agencies are not subject to any requirement to file SARs under the rules of the Financial Crimes Enforcement Network (“FinCEN”), which is a key component of the response programs described in the Interagency Guidance.

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. 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. Consequently, the CDIA is concerned that the FTC may propose a blanket rule requiring notification of customers when a breach

⁹ See, e.g., 12 C.F.R. Part 208, Appendix D-2, at III.g.

¹⁰ 70 Fed. Reg. at 15,752.

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.

The CDIA also notes that consumer reporting agencies are subject to state breach notification laws in 47 states, the District of Columbia, and three U.S. territories.¹¹ 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.¹² 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. The CDIA also notes that all 50 states and the District of Columbia have enacted “security freeze” laws that allow consumers, including those notified of data breaches, to limit consumer reporting agencies from releasing consumer reports or information from consumer reports without the consumer’s authorization.

The CDIA does not believe that the FTC should propose a response plan that incorporates federal data breach notification requirement. Such a requirement would provide little consumer benefit beyond what state breach notification laws already provide. The lack of state breach notification laws in three states is not a sufficient reason for adopting a federal requirement layered on top of 47 state laws. Moreover, a federal breach notification requirement would increase costs and burdens on consumer reporting agencies without providing a substantial consumer benefit. From the CDIA’s perspective, a federal breach notification requirement would only benefit consumers if it created a single national standard, 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.

The Scope of the FTC’s Safeguards Rule Should Be Consistent With the Scope of the Federal Banking Agencies’ Interagency Safeguards Guidelines.

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.¹³ Similarly, the Interagency Guidelines define “customer information,” to mean “any record containing nonpublic personal information, . . . , about a customer, . . . , that is maintained by or

¹¹ Alabama, New Mexico, and South Dakota are the three states with no security breach law.

¹² 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.

¹³ See, e.g., 12 C.F.R. Part 208, Appendix D-2, at I.A.

on behalf of the bank.”¹⁴ 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 whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.”¹⁵ 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.”¹⁶

The FTC’s approach subjected 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.¹⁷

In 2002, the CDIA strenuously opposed the FTC’s decision to apply its Safeguards Rule to financial institutions that receive from another financial institution customer information about the latter’s customers,¹⁸ and the CDIA reiterates those objections in response to the FTC’s request for public comment. The CDIA continues to believe that section 501(a) of the Gramm-Leach-Bliley Act is clear on its face and applies to a financial institution’s obligation to “its customers.”¹⁹ The CDIA further believes that the expansive scope of the FTC’s Safeguards Rule is unnecessary and burdensome for consumer reporting agencies, particularly in light of the substantial obligations already imposed on consumer reporting agencies under the Fair Credit Reporting Act, such as the requirement to maintain reasonable procedures to ensure that consumer report information is provided only for legitimate purposes and the requirements to

¹⁴ See, e.g., 12 C.F.R. Part 208, Appendix D-2, at I.C.1.c.

¹⁵ 16 C.F.R. § 314.1(b).

¹⁶ 16 C.F.R. § 314.2(b).

¹⁷ 67 Fed. Reg. 36,484, 36,485-86 (May 23, 2002). 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. See 67 Fed. Reg. at 36,485 & note 21.

¹⁸ See 67 Fed. Reg. at 36,485 & note 21.

¹⁹ 15 U.S.C. § 6801(a).

securely dispose of consumer report information and information derived from consumer reports.

The CDIA, therefore, respectfully requests that the FTC propose revisions to the Safeguard Rule's scope section and definition of "customer information" to align with the Federal banking agencies' Interagency Guidelines.²⁰ The CDIA believes that the FTC's Safeguards Rule should apply only to information about a financial institution's own customers, and should not apply to financial institutions that receive information about customers of other financial institutions from those institutions.

The Disposal Rule (and the Safeguards Rule) Should Not Be Amended to Cover or Apply to Aggregate Information, Blind Data, or Otherwise De-Identified Data.

In its request for comment on the Disposal Rule, the FTC notes that the defined term "consumer information" does not include "information that does not identify individuals, such as aggregate information or blind data."²¹ The FTC asks whether "the Rule should be modified to change the definition of "consumer information" to include "information that can be reasonably linked to an individual in light of changes in relevant technology or market practices," and, in particular, whether the Rule should be "modified to define 'aggregate information' or 'blind data.'"²²

The CDIA urges the FTC to retain without modification the existing definition of "consumer information" in the Disposal Rule. The current definition states simply and clearly that "consumer information" means "any record about an individual, . . . , that is a consumer report or is derived from a consumer report," as well as "a compilation of such records."²³ The definition specifically excludes "information that does not identify individuals, such as aggregate information or blind data."

The CDIA believes that the FTC should retain without modification the Disposal Rule's exception for aggregate information, blind data, or otherwise de-identified data. Regulators traditionally have given companies latitude to use aggregated, anonymized, or de-identified data without becoming subject to regulation,²⁴ and the FTC has followed this approach.²⁵

²⁰ See, e.g., 12 C.F.R. Part 208, Appendix D-2, at I.A, and I.C.1.c..

²¹ 81 Fed. Reg. at 63,437.

²² *Id.*

²³ 16 C.F.R. § 682.1(b).

²⁴ See 16 C.F.R. § 313.3(o)(2)(ii)(B) (excluding from the definition of "personally identifiable financial information" any information that "does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.").

Because such information or data, by definition, does not identify individual consumers, there is no risk of consumer harm in the event such data is compromised. (For the same reasons, CDIA does not believe that the Safeguards Rule should apply to aggregate information, blind data, or otherwise de-identified data.) There is no net benefit in requiring consumer reporting agencies to incur the additional costs and burdens of applying the Disposal Rule to aggregate information, blind data, or otherwise de-identified data when such a change would not address any identified consumer harm or provide consumers with additional protection.

Many consumer benefits result from the use of aggregated, anonymized, or de-identified data. CDIA members and others use aggregate information, blind data, or otherwise de-identified data to develop ever more robust and predictive analytic tools, including credit scores for analyzing consumer behavior and making credit available to underserved populations, and tools designed to prevent and detect fraud and identity theft. Any restrictions on the use of de-identified data for these constructive purposes or new and burdensome requirements with respect to the transmission, storage or disposal of such information could have unintended consequences for the future development of such consumer-friendly innovations.

The FTC also should not define “aggregate information” or “blind data.” The terms “aggregate information” and “blind data” are just examples of “information that does not identify individuals.” The CDIA believes that defining these two illustrative terms would do little to clarify the rule, but would generate confusion about whether other types of de-identified data qualify as “information that does not identify individuals.” The CDIA further notes that no other agency’s disposal rule defines “aggregate information” or “blind data.”

The FTC asks whether it should consider amending the definition of “consumer information” to include “information that can be reasonably linked to an individual.”²⁶ The CDIA is familiar with recent FTC reports that express concern about the effectiveness of aggregating, anonymizing, and de-identifying data in the face of technological advances in data analytics and reverse engineering.²⁷ However, the FTC should not amend the “consumer information” definition to incorporate a “reasonably linked” component.

²⁵ See *In re Trans Union*, Opinion of the Commission 11-12 (Mar. 2000), available at <http://www.ftc.gov/sites/default/files/documents/cases/2000/03/transunionopinionofthecommission.pdf>.

²⁶ 81 Fed. Reg. at 63,437.

²⁷ See FTC, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report 37-38 (Dec. 2010), available at <https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework> (panelists noted that “even where companies take steps to ‘de-identify’ data, technological advances and the widespread availability of publicly available information have fundamentally changed the notion of anonymity”); FTC, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers*, FTC Report at iv (Executive Summary), 19, and 21 (Mar. 2012), available at <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change> (continued...)

As the FTC notes, the concept of information being “reasonably linked to an individual” depends upon changes in relevant technology or market practices.²⁸ The CDIA believes that the adoption of a “reasonably linked” standard tied to changes in technology or market practices would introduce subjectivity and uncertainty into what is currently a clear, simple, and easily understood definition of “consumer information.” For example, one indication of data not being “reasonably linked” to a particular consumer that the FTC has outlined is where the company “takes reasonable measures to ensure that the data is de-identified.”²⁹ The CDIA believes that such a “reasonable measures” standard is opaque and subjective, and thus inappropriate for including in a regulatory definition.

Finally, the CDIA observes that the FTC’s Disposal Rule was promulgated under the authority granted by Section 216 of the Fair and Accurate Credit Transactions Act (“FACT Act”). Section 216(a)(2) of the FACT Act specifically requires the FTC, the federal banking agencies, the National Credit Union Administration, and the Securities and Exchange Commission each to adopt disposal rules.³⁰ In doing so, each agency must “consult and coordinate” so that, to the extent possible, the disposal rules prescribed by each agency are “consistent and comparable” with the rules prescribed by the other agencies.³¹ Per these statutory requirements, the FTC must ensure in this review that its Disposal Rule remains “consistent and comparable” with the rules of the other agencies. Absent a coordinated interagency change in direction, the best way for the FTC to maintain the required consistency and comparability is by retaining the Disposal Rule’s current definition of “consumer information,” not defining “aggregate information” or “blind data,” and refraining from introducing into the rule the concept of information “reasonably linked” to an individual, which is not found in any other agency’s disposal rule.

* * *

[recommendations-businesses-policy-makers](#) (acknowledging a blurring of the distinction between personally identifiable information and non-personally identifiable information and outlining the FTC’s views on when data is not “reasonably linkable” to a particular consumer) (hereafter “*Protecting Consumer Privacy Report*”).

²⁸ 81 Fed. Reg. at 63,437.

²⁹ *Protecting Consumer Privacy Report*, at iv (Executive Summary) and 21.

³⁰ 15 U.S.C. § 1681w(a)(1).

³¹ 15 U.S.C. § 1681w(a)(2).

We appreciate the opportunity to comment on the FTC's requests for public comment regarding possible amendments to its Safeguards Rule and Disposal Rule, and hope the FTC will find these comments useful as it reviews these two rules.

Sincerely,



Eric J. Ellman
Interim President and CEO