National Consumer Law Center (on behalf of its low-income clients)
Allied Progress
California Reinvestment Coalition
Center for Digital Democracy
Center for Economic Integrity (AZ)
Consumer Action
Consumer Federation of America
Demos
Main Street Alliance
Media Alliance (CA)
National Association of Consumer Advocates
National Consumers League
National Fair Housing Alliance
Privacy Rights Clearinghouse
Public Justice Center (MD)
U.S. PIRG
Woodstock Institute

August 2, 2019

Federal Trade Commission
Office of the Secretary
Constitution Center
400 7th St., SW
5th Fl, Suite 5610 (Annex B)
Washington, DC 20024

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

Dear Sir/Madam:

The undersigned consumer and advocacy groups submit these comments in response to the Federal Trade Commission's (FTC) Notice of Proposed Rulemaking (NPRM) regarding amendments to the Standards for Safeguarding Consumer Information ("Safeguards Rule"), 16 C.F.R. Part 314. The Safeguards Rule is promulgated pursuant to the FTC's authority under Section 6801(b) of the Gramm Leach Bliley Act ("GLBA").

We specifically comment on the need to strengthen the Safeguards Rule with respect to consumer reporting agencies ("CRAs"), particularly the "nationwide" CRAs as described in Section 603(p) of the Fair Credit Reporting Act, *i.e.*, Equifax, Experian, TransUnion. We note that elements of the settlements with Equifax over its data breach include provisions of the proposed rule, but also go further. We also comment on the need to strengthen the Safeguards Rule as applied to certain other high-risk sectors, such as tax preparers and financial technology ("fintech") firms.

We appreciate the fact that the FTC has taken steps to improve the Safeguards Rule by adopting some of the concrete and specific requirements of the New York Department of Financial Services' cybersecurity regulations, 23 NYCRR 500 and the National Association of Insurance Commissioners' Model Data Security Law. In general, these changes are positive and helpful, such as requirements to encrypt information, use multi-factor authentication, conduct risk assessments and regular monitoring, maintain audit trials, and designate a Chief Information Security Officer (CISO). These are reasonable and common-sense measures that any company dealing with large amounts of consumer personal information should take.

However, we think the FTC needs to go further and require more detailed and stringent requirements for the nationwide CRAs and certain other financial institutions that present especially high risks because of the valuable nature of the data they hold. These financial institutions should be required to comply with certain detailed security frameworks, including those issued by the National Institute of Standards and Technology (''NIST'') and the Federal Financial Institutions Examination Council (FFIEC). They should also be required to report data security breaches to the FTC.

1. The Need for Stronger Cybersecurity Requirements is Amply Demonstrated by the Equifax Data Breach

As the FTC and most of the American public are well aware, in 2017 a data breach at the nationwide CRA Equifax resulted in the theft of the personal identifying information of 148 million Americans. It was perhaps the worst data breach in American history, not only because it affected over one in two American adults, but it also involved some of the most critical personal information we have – Social Security numbers (which are the golden keys for identity theft), dates of birth, and in some cases drivers' license numbers.

The Equifax data breach was horrifying in scale and damning in the negligence that allowed it to occur. It resulted from the lapses in the very types of security measures that the proposed rule addresses, such as regular monitoring, strong access controls, periodic risk assessment, encryption of consumer information, and designating a single point of oversight and accountability for information security. These lapses were especially galling given that Equifax is a technology company in the very business of collecting information - vast amounts of sensitive financial information - that it then failed to protect using basic, well-known steps such as updating software and installing well-publicized security patches by major software providers.

Indeed, some of Equifax's inadequate security measures are directly addressed by the proposed changes to the Safeguards Rule. A December 2018 report from the House Oversight and Government Reform Committee documents these failures in great depth. The report notes that one of the key factors leading to Equifax's security breach was its aggressive growth strategy, which brought increasing complexity to Equifax's IT systems and expanded data security risks – risks that Equifax failed to adequately address.[1] Such risks presented by acquisitions and

[1] H. Comm. on Oversight and Gov't Reform, 115th Congr., The Equifax Data Breach: Majority Staff Report, December 2018, at 2, https://web.archive.org/web/20181210223114/https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf. {hereinafter "House Equifax Report"]

mergers would be address by proposed Section 314.4(c)(9), which requires financial institutions to adopt procedures for change management. As the Supplementary Information notes, this paragraph means that "a financial institution that acquired a new subsidiary and wished to combine the new subsidiary's network with its own would be required to assess the security of the new network and the effect of adding it to the existing network."[2]

Another failure by Equifax was the lack of clear lines of authority regarding data security in its corporate structure. The House Oversight Report discusses this deficiency in detail in sections entitled "Equifax IT Management Structure Lacked Accountability and Coordination" and "Equifax's Organizational Structure Allowed Ineffective IT Coordination."[3] In particular, Equifax had both a Chief Security Officer (who reported to the Chief Legal Officer) and a Chief Information Officer. As a result, "the IT and Security organizations were siloed, meaning information rarely flowed from one group to the other…. Communication and coordination between these groups was often inconsistent and ineffective."[4] If there had been a single CISO at Equifax as required by proposed § 314.4(a), 148 million Americans might have avoided having their Social Security numbers, dates of birth and other critical information stolen.

Encryption is an element that was sorely lacking at Equifax too, something which proposed § 314.4(c)(4) requires. The House Oversight report notes that hackers found credentials that were unencrypted, which enabled them to access 48 databases. In turn, this access allowed the hackers to locate on 265 occasions personally identifiable information that was also unencrypted.[5] Not only do the proposed changes to the Safeguards Rule require encryption, proposed § 314.4 (c)(6) would require multi-factor authentication for credentials to access consumer information. If Equifax had protected access to the data of 148 million Americans with multi-factor authentication, there likely would never have been a breach.

Finally, one of the most critical lapses was the failure to install a security patch for a known vulnerability in the Apache Struts software.[6] Such a lapse could have been prevented if Equifax had been abiding by the measure required by proposed § 314.4 (e)(3) to ensure that information security personnel be provided with ongoing information about security updates.

We also note that many of the elements of the proposed rule are incorporated into the Equifax settlement with the FTC,[7] such as a written Information Security Program, a qualified employee to oversee the program, and annual assessments of the program. These elements should apply to all of the nationwide CRAs.

---

[2] 84 Fed. Reg. at 13167.
[3] House Equifax Report at 55-60.
[4] *Id* at 60.
[5] *Id.* at 32-33.
[6] *Id.* at 2.
[7] Stipulated Order for Permanent Injunction and Monetary Judgment, FTC v. Equifax, (N.D. Ga. July 22, 2019).

2. The FTC Should Develop a Category of Larger or Riskier Institutions, Including Nationwide CRAs, That Are Subject to Heightened Requirements Under the Safeguards Rule

While the proposed amendments to the Safeguards Rule are a positive step forward and would address some of the failures by Equifax that led to its 2017 data breach, there should be more required of financial institutions that hold such vast amounts of sensitive consumer information. Frankly, Equifax was simply the unlucky one to be targeted by successful hackers. Some of the issues flagged by the House Oversight report, such as outdated legacy systems, also likely exist at the other two nationwide CRAs. In fact, Experian had its own large-scale data breach first in 2015, although it was small by Equifax standards, affecting "only" 15 million consumers.[8] Indeed, all three nationwide CRAs share certain antiquated legacy systems, such as the 25-year old e-OSCAR system built to handle disputes.

Thus, the FTC should develop a category of financial institutions that are subject to heightened requirements under the Safeguards Rule either because of their size or the greater risk posed by the sensitive nature of information that they hold. We note that the proposed rule exempts smaller institutions that maintain information for less than 5000 consumers, thus setting the precedent for having the opposite category of larger or riskier financial institutions that handle the personal information of tens or even hundreds of millions of consumers.

A category for larger or risker institutions would be somewhat akin to the "larger participant" concept under the Dodd-Frank Act, 12 U.S.C. § 5514, which are companies that are subject to supervision by the Consumer Financial Protection Bureau due to their size, the type of activity they engage in, and/or the risk they pose. Creating a category of larger or riskier institutions is both logical and necessary, given that they deal with greater amounts or more sensitive information.

Larger/risker institutions should include:

> i. Nationwide CRAs and any CRAs that earn more than $7 million in annual receipts from consumer reporting. The nationwide CRAs are especially vulnerable given that they hold vast amounts of extremely valuable financial information pertaining to over two-thirds of Americans – information that is a lucrative target for identity theft and other activities harmful to consumer interests. The $7 million threshold for other CRAs is the same as that used by the CFPB for designating larger participants in the consumer reporting market.[9]
>
> ii. Tax preparation companies (including their franchisees) that earn more than $7 million in annual receipts from tax preparation activities. Tax preparers hold the extremely critical financial information about consumers in the form of tax returns. They are already subject to strict requirements regarding the disclosure of information under Section 7216 of the Internal Revenue Code. However, Section 7216 does not have any data safeguard or security requirements. Stricter requirements under the FTC Safeguards

[8] House Equifax Report at 18.
[9] 12 C.F.R. § 1090.104(b).

rules would work hand in hand with the disclosure restrictions of I.R.C. § 7216 to ensure taxpayer information is not unlawfully disclosed.

iii. Financial technology companies that engage in financial activities, including lending, payment services, and holding deposits. Without a bank charter, these institutions thus are not subject to the data security requirements of the banking regulators but should be given their financial activity.

Larger/riskier financial institutions should be required to do more in terms of safeguarding consumer information. They should be required to:

i. Deploy reasonable technical measures and corporate governance processes that satisfy or exceed all relevant data security policy recommendations contained in the NIST Cybersecurity Framework. We note that the private class action settlement in the Equifax data breach requires that company to comply with NIST standards.[10]

ii. Comply with FFIEC guidance that supplements the Interagency Guidelines Establishing Standards for Safeguarding Customer Information issued by the prudential banking regulators, such as the FFIEC's Information Technology Examination Handbook, topical bulletins that include information security components, and other guidance documents, such as the Cybersecurity Assessment Tool.

iii. Have an incident response program which requires compliance with state law requirements and applies a breach notification obligation only when state law lacks it. Larger/riskier institutions should also be required to report data security breach incidents to the FTC.

3. **Technical issues**

a. CRAs should be explicitly covered by the Safeguards Rule

The Safeguards Rule should explicitly state that CRAs are "financial institutions" covered by the Rule. While the FTC has made proclamations that CRAs are "financial institutions,"[11] it would be preferable to include CRAs specifically in the Rule, given the heightened need for them to be governed by data security requirements. Many other types of financial institutions that are arguably less prone to high-risk security breaches are explicitly covered by the Rule, such as check printers and travel agents.

---

[10] Settlement Agreement and Release, In re: Equifax Inc. Customer Data Security Breach Litigation, Case 1:17-md-02800 (N.D. Ga. July 22, 2019), Exhibit 2.

[11] *See* Hearing on Improving Data Security at Consumer Reporting Agencies: Hearing Before the Subcomm. on Economic and Consumer Policy of the H. Comm. on Oversight and Reform, 11_th Congr. (2019) (written testimony of Andrew Smith, Director of FTC Bureau of Consumer Protection, stating "the Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ('GLB Act'), requires certain non-bank financial institutions – including CRAs – to safeguard nonpublic personal information"); Trans Union LLC v. F.T.C., 295 F.3d 42 (D.C. Cir. 2002)(FTC permissibly determined that a CRA is a "financial institution" subject to the rulemaking authority of the FTC under the Act).

b. The FTC rightfully rejected the CRAs' request for consumer report information to be excluded from coverage.

We appreciate the fact that the FTC rejected the request of Consumer Data Industry Association (CDIA) to remove the statement in § 314.1(b) that "This 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." CDIA had objected to this language because it resulted in application of the Safeguards Rule to the consumer reporting information in the CRA databases, which CDIA believed was "unnecessary and burdensome."[12]

CDIA was essentially arguing that CRAs should not be subject to the Safeguards Rule and its data security requirements. Such a position would be especially egregious in hindsight given the Equifax data breach.

* * * * *

Thank you for the opportunity to submit these comments. If you have any questions about them, please contact Chi Chi Wu, National Consumer Law Center (cwu@nclc.org or 617-542-8010).

National Consumer Law Center (on behalf of its low-income clients)
Allied Progress
California Reinvestment Coalition
Center for Digital Democracy
Center for Economic Integrity (AZ)
Consumer Action
Consumer Federation of America
Demos
Main Street Alliance
Media Alliance (CA)
National Association of Consumer Advocates
National Consumers League
National Fair Housing Alliance
Privacy Rights Clearinghouse
Public Justice Center (MD)
U.S. PIRG
Woodstock Institute

[12] Comment of Consumer Data Industry Association re Safeguards Rule, 16 CFR 314, Project No. P145407 and Disposal Rule, 16 CFR part 682, Project No. 165410, November 21, 2016.