August 2, 2019

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Safeguards Rule, 16 CFR part 314, Project No. 145407

Consumer Reports[1] thanks the Federal Trade Commission (FTC) for soliciting comments on proposed changes to the Safeguards Rule.[2] The Safeguards Rule, which went into effect in 2003,[3] requires reasonable security procedures for financial institutions under the Gramm-Leach-Bliley Act (GLBA),[4] including administrative, technical, and physical controls to safeguard consumer data.[5] The proposed changes to the Rule reflect the more prescriptive data security requirements issued through the New York State Department of Financial Services' new cybersecurity rules[6] and the National Association of Insurance Commissioners' Model Law,[7] including explicitly requiring a single chief security officer, maintaining audit trails, and generally requiring two factor authentication and encryption.

[1] Consumer Reports is an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. Consumers Reports works for pro-consumer policies in the areas of financial services and marketplace practices, antitrust and competition policy, privacy and data security, food and product safety, telecommunications and technology, travel, and other consumer issues, in Washington, DC, in the states, and in the marketplace. Consumer Reports is the world's largest independent product-testing organization, using its dozens of labs, auto test center, and survey research department to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

[2] *FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules*, FED. TRADE COMM'N (June 3, 2019), 16 CFR Part 314, Project No. P145407, *available at* https://www.regulations.gov/document?D=FTC-2019-0019-0002.

[3] 67 Fed. Reg. 36,493 (May 23, 2012), *available at* https://www.govinfo.gov/app/details/FR-2002-05-23/02-12952.

[4] 15 U.S.C. § 6801(b), *available a*t https://www.law.cornell.edu/uscode/text/15/6801.

[5] 16 C.F.R. § 314.1, *available at* https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule.

[6] New York State Department of Financial Services, 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies (2016), https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

[7] *Insurance Data Security Model Law*, NAIC Model Laws, Regulations, Guidelines and Other Resources (4th Quarter 2017), https://www.naic.org/store/free/MDL-668.pdf.

We appreciate that the FTC is considering updating the rules in light of the 2017 Equifax data breach and continued data security failures involving financial institutions, including another historic data breach of a major banking institution in 2019.[8] But it's clear that more is needed in order for companies to sufficiently protect the private consumer information they collect and store. The FTC needs stronger enforcement authority to ensure that consumer data is better secured.

The key factor to help prevent future data breaches is to ensure that the potential consequences of a breach properly incentivize companies to keep data secure. The Equifax data breach was one of the worst in United States history, as over 145 million consumers had their data leaked, much of it sensitive data such as Social Security numbers that fraudsters can use to open up new accounts in consumers' names.[9] It's not clear that more specific requirements would have prevented the incident: Equifax's lapses clearly violated the security requirements of the Safeguards Rule by failing to take such basic measures such as patching known security weaknesses in their software architecture, and failing to notice the vulnerability for over four months.[10] And even this historic and preventable breach has failed to spur sufficient change in the industry. Just this week, Capital One announced that a hacker had exploited a security vulnerability to obtain the account information of over 100 million consumers, including names, addresses, bank account information, and thousands of Social Security numbers.[11] In light of these continuing lapses, the FTC should:

- **Press Congress to provide significant penalties for violations of the Safeguards Rule;**
- **Press Congress for appropriate resources for oversight, and require third-party oversight of companies to ensure data security;**
- **Ensure that regulations accommodate differences in the size and circumstances of companies;**
- **Require companies to adopt an incident response plan, including notifying the FTC of security incidents;**
- **Identify specific standards to guide compliance, but make clear that adherence does not constitute a safe harbor; and**
- **Strengthen Safeguards provisions to ensure the strongest possible security.**

[8] Emily Flitter & Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million,* N.Y. TIMES (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.
[9] U.S. House of Representatives Committee on Oversight and Government Reform, 115th Congress, *The Equifax Data Breach Majority Staff Report* at 3, 43 (Dec. 2018), https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf [hereinafter HOUSE OVERSIGHT MAJORITY REPORT].
[10] Fed. Trade Comm'n v. Equifax, Case 1:19-mi-99999-UNA, U.S. District Court for the Northern District of Georgia, Atlanta Division, Complaint for Permanent Injunction and Other Relief at 7-8 (July 22, 2019), https://files.consumerfinance.gov/f/documents/cfpb_equifax-inc_complaint_2019-07.pdf.
[11] *Capital One Announces Data Security Incident*, CAPITAL ONE (July 29, 2019), http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle&ID=2405043.

Enormous data breaches involving the sensitive data of consumers are becoming all too common, and the failure to protect personal data causes real harm to consumers. Over 14 million U.S. consumers fell victim to identity theft in 2018, costing them over $3 billion in new account fraud.[12] Victims spend precious time and money repairing the damage to their credit and accounts. Medical identity theft, in which thieves use personal information to obtain medical services, exhausts consumers' insurance benefits and leaves them with exorbitant bills. Tax identity theft occurs when thieves use consumers' Social Security numbers to obtain tax refunds. Fraudulent information on credit reports also causes consumers to pay more for a loan or be denied credit. And breaches take a toll on businesses too—in 2018, the average cost of a breach to companies globally climbed to $3.9 million, a 12 percent increase over the past five years.[13] Despite these clear harms, not enough has been done at the federal level to ensure that companies protect the sensitive consumer data they collect, store and use. As a result, hackers continue to successfully target vulnerable companies—year in and year out, and increasingly from overseas—thus harming consumers and companies alike.

The FTC should press Congress to provide significant penalties for violations of the Safeguards Rule.

A key problem is that the Gramm-Leach-Bliley Act (GLBA) does not provide penalties for failure to comply with the data security requirements. While FTC Chairman Joe Simons has called for Congress to provide for civil penalties to aid in privacy and security enforcement for violations of the FTC Act,[14] the FTC should likewise call for them to be added to the Safeguards Rule. The recent Equifax settlement, in which the FTC, the Consumer Financial Protection Bureau (CFPB), and a number of state attorneys general reached a settlement over the Equifax data breach investigation, highlighted the lack of penalty authority under GLBA and the Safeguards Rule. The $575 million minimum settlement consists mostly of redress to consumers, ordered under Section 13(b) of the FTC Act, rather than penalties.[15] Equifax will also pay an

[12] *2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt*, JAVELIN (Mar. 9, 2019), https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt.

[13] *IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years*, IBM NEWSROOM (July 23, 2019), https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years [hereinafter IBM DATA BREACH STUDY].

[14] Prepared Remarks of Chairman Joseph Simons, Introductory Keynote: American Bar Association Consumer Protection Conference at 2 (Feb. 5, 2019), https://www.ftc.gov/system/files/documents/public_statements/1451379/simons-_nashville-aba-remarks.pdf.

[15] Fed. Trade Comm'n v. Equifax, Case 1:19-mi-99999-UNA, United States District Court for the Northern District of Georgia, Atlanta Division, Stipulated Order for Permanent Injunction and Monetary Judgment (July 22, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_proposed_order_7-22-19.pdf [hereinafter EQUIFAX SETTLEMENT].

additional $175 million to the states, and $100 million in civil penalties to the CFPB,[16] which can assess penalties under the Dodd-Frank Act of 2010.[17]

Given the expertise of the FTC in handling data security cases, it's not sufficient to rely on the CFPB alone to provide appropriate penalties. While even more experts are needed on staff, the FTC has made important strides in recent years between the establishment of the Chief Technologist position advising the Chairman and the creation of the Office of Technology Research and Investigation (OTECH). The FTC has also developed substantial expertise through its long history of prosecuting data security and privacy cases.[18] In contrast, the CFPB has a limited history of data security enforcement actions, with only one major case in addition to the Equifax investigation.[19]

Redress to consumers is important but insufficient to effectively deter wrongdoing. It is necessarily limited to unjust gains at the expense of consumers, which can be difficult to calculate. In contrast, civil penalties will appropriately ensure that companies are penalized per violation of the law and will be properly incentivized to follow it. The penalty amount should be reasonably tied to factors such as the nature of the violation, the types of data compromised, the willfulness of the behavior, and the size of the company, as well as its ability to pay.

Without these penalties, credit bureaus in particular will continue to have insufficient incentives to adopt strong security practices, because it's difficult for consumers to hold these companies accountable. Credit bureaus' primary clients are the lenders who purchase information about consumers, not consumers themselves. Consumers have no say in whether their data is shared with Equifax, even though the company makes hundreds of millions in profits from consumer data every year.[20] Its reckless handling of the breach and its aftermath—including its delay in addressing a known vulnerability, delay in providing breach notices, meager remedies for consumers, inclusion of a forced arbitration provision, and rollout of a defective website—and the fact that Equifax's stock quickly returned to levels close to what they had been before the

[16] *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, FED. TRADE COMM'N (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.
[17] 12 U.S.C. § 5565, *available at* https://www.law.cornell.edu/uscode/text/12/5565.
[18] *Privacy and Data Security Update: 2018*, FED. TRADE COMM'N (Jan. 2018-Dec. 2018), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.
[19] *See, e.g.*, *CFPB Takes Action against Dwolla for Misrepresenting Data Security Practices*, CONSUMER FIN. PROTECTION BUREAU (Mar. 2, 2016), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.
[20] Equifax, Inc., Annual Report (Form 10-K), at 33 (Feb. 21, 2019), *available at* https://www.sec.gov/Archives/edgar/data/33185/000003318519000007/efx10k20181231.htm ($299.8 million in net income in 2018).

breach,[21] make clear that the penalty for violating the law was insufficient to change their behavior.

When the California Consumer Privacy Act (CCPA) goes into effect in 2020, data security will improve significantly for California residents. The bill provides liquidated damages in the event of a negligent data breach—up to $7,500 per intentional violation.[22] While there is a GLBA carve-out in the privacy provisions of the CCPA, financial institutions remain covered by the negligent data breach provision.[23] But all consumers, not just those in California, deserve strong protections against data breaches. Therefore, the FTC should press Congress to ensure that these protections apply across the US.

The FTC should press Congress for appropriate resources for oversight, and require third-party oversight of companies to ensure data security.

The FTC should press Congress for appropriate resources to carry out its mandate. While the FTC conducted nationwide sweeps to check compliance with the Safeguards Rule the year after it went into effect,[24] the agency likely lacks the resources necessary to maintain those levels of oversight. The FTC is woefully understaffed: the FTC has just over a thousand employees in total, and is tasked with overseeing giants like Google and Facebook.[25]

The FTC should also use its existing authority to increase oversight of financial institutions for compliance with the Safeguards Rule. While the proposed rules appropriately require the chief security officer to attest to its compliance with the Safeguards Rule each year,[26] outside verification is needed as well. The recent FTC settlement subjects Equifax to third party assessments, to ensure that the data security program is appropriately devised and monitored.[27] Larger companies and those holding particularly sensitive information, such as the nationwide consumer reporting agencies (NCRAs), tax preparation companies, and financial technology, or "fintech" companies, should be required under the Safeguards Rule to establish third party assessments in order to better incentivize compliance.

[21] HOUSE OVERSIGHT MAJORITY REPORT, *supra* note 9, at 16.
[22] Cal. Civ. Code, 1798.155(b).
[23] Cal. Civ. Code, 1798.145(e).
[24] HOUSE OVERSIGHT MAJORITY REPORT, *supra* note 9, at 24.
[25] Tony Romm, *The Agency in Charge of Policing Facebook and Google is 103 Years Old. Can It Modernize?* WASH. POST (May 4, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech.
[26] 84 Fed. Reg. 13,170 (April 4, 2019).
[27] EQUIFAX SETTLEMENT, *supra* note 18, at 19.

The FTC should ensure that regulations accommodate differences in the size and circumstances of companies.

It the context of data security, companies should engage in risk balancing to determine the appropriate amount of investment for security, and requirements should be appropriate to the size of the company. Stronger requirements for Equifax and other NCRAs, tax preparation companies, and fintech companies are warranted.[28] As the House Oversight Committee noted, the very size of CRAs like Equifax and the amount of data accumulated put greater data security responsibilities on them: "Due to the intrusive amount of data held by CRAs, these companies have an obligation to have best-in-class data protection and cybersecurity practices and tools in place."[29]At the same time, it makes sense to exempt companies that collect data on fewer than 5,000 people from some of the requirements in the proposed rule, as long as they are still required to perform assessments, design and implement a written security program qualified information security personnel, and monitor the activity of authorized users, as proposed by the FTC.[30]

The FTC should require companies to adopt an incident response plan, including notifying the FTC of security incidents.

The FTC is correct in proposing to require companies to adopt an incident response plan.[31] In addition, companies should be required to report security incidents to the Commission in order to improve enforcement efforts. Recent research indicates that a rapid response helps limit the damage of a data breach. According to a recent data breach report, "[C]ompanies in the study who were able to detect and contain a breach in less than 200 days spent $1.2 million less on the total cost of a breach."[32] Equifax's slow response to the data breach also highlights the need for these requirements. Further, the FTC should also clarify in the rule that complying with the incident response plan does not relieve companies from the responsibility to comply with stronger state requirements.

The FTC should point to specific standards to guide compliance, but make clear that adherence to the standard does not constitute a safe harbor.

While it can be helpful to point to specific standards, such as those issued by the National Institute of Standards and Technology (NIST) and Federal Financial Institutions Examination Council (FFIEC), in order to guide compliance, it's important to make clear that adhering to a

[28] Comments of National Consumer Law Center, Re: Safeguards Rule, 16 C.F.R. part 314, Project No. P145407 at 3-4 (Aug. 2, 2019).
[29] HOUSE OVERSIGHT MAJORITY REPORT, *supra* note 9, at 15.
[30] 84 Fed. Reg. 13,170 (April 4, 2019).
[31] *Id*. at 13,169.
[32] IBM DATA BREACH STUDY, *supra* note 13.

standard does not shield companies from liability in the event of a security failure. Threats are constantly evolving, and companies should have the flexibility to respond to new developments. They should work to stay ahead of new threats, and be held accountable for failure to do so.[33]

The FTC should strengthen Safeguards provisions to ensure the strongest possible security.

Appropriately, the FTC is working to maintain a process-based, rather than prescriptive, approach to data security, in order to allow practices to evolve in response to new threats. However, in a few circumstances, the proposed rules should be strengthened further to ensure appropriate protections. Specifically, companies should be required to regularly monitor service providers with respect to their data security compliance, and internal access to information should be strictly limited. Finally, companies should be allowed to retain data only as long as it is needed for the business purpose for which it was collected, and the risk of potential exposure should be weighed against the rationale for retaining.

Service providers should be kept to a stronger standard. The Safeguards Rule already directs companies to select service providers that are capable of keeping data secure, and to require compliance with data security procedures in their business contracts.[34] And, the proposed rules would require companies to periodically assess service providers and their safeguards. Instead, companies should be required to regularly assess service providers and their safeguards, and carefully monitor companies for compliance, particularly as security breaches by service providers are all too common.[35] For example, Amazon Web Services hosted the database that was breached in the recent Capital One incident.[36]

Further limit internal access to information. Companies should be required to implement further controls to reduce the number of people with access to the personal information in order to more sufficiently protect the personal data they store and control. While the proposed rule requires companies to limit information to authorized individuals,[37] the rule should go further. Consumer Reports has long called for limiting the uses of data in internal processes unless reasonably necessary.[38] This should be clarified in the Safeguards Rule. The more opportunities there are to leak, disclose, or mishandle the data, the more likely that a security incident will occur.

Limit data retention. Finally, there should be stronger limits on how long companies can retain the data. The proposed rule stipulates that companies can keep data as long as there is a

[33] 84 Fed. Reg. 13,160 (April 4, 2019).
[34] 16 C.F.R. § 314.4 (d).
[35] *See, e.g., Breach at Cloud Solution Provider PCM Inc.*, KREBS ON SECURITY (June 27, 2019), https://krebsonsecurity.com/2019/06/breach-at-cloud-solution-provider-pcm-inc/.
[36] *Capital One Data Breach Compromises Data of Over 100 Million*, *supra* note 8.
[37] 84 Fed. Reg. 13,175 (April 4, 2019).
[38] *State Laws Restricting Private Use of Social Security Numbers*, CONSUMERS UNION (Nov. 28, 2007), https://advocacy.consumerreports.org/research/state_laws_restricting_private_use_of_social_security_numbers/.

legitimate business purpose for doing so.[39] Instead, data should be retained only as long as it is needed for the business purpose for which it was collected, and the risk of potential exposure should be weighed against the rationale for retaining. The longer companies retain data, the more likely it is that it will be breached or misused. This became clear following the Capital One data breach, which involved data collected as far back as 2005.[40] This more tailored standard will give companies the flexibility they need to retain data in order to provide services requested by the consumer, while still putting important limits on retention.

Conclusion

Congressional action is needed to better protect consumer data. While the FTC has proposed helpful additions to the Safeguards Rule, the agency simply does not have the authority and resources necessary to ensure that companies properly maintain consumer data. Furthermore, as noted above, the FTC should refine its proposal to strengthen security further. As shown by the plethora of data breaches affecting financial institutions in recent years, companies need better incentives to protect consumer data from inadvertent disclosure. Without swift and decisive action from Congress, the wave of data breaches over the last few years will only increase and consumers will continue to feel the brunt of the ill effects of these repeated breaches.

Respectfully Submitted,

Maureen Mahoney
Policy Analyst
Consumer Reports

[39] 84 Fed. Reg. 13,175 (April 4, 2019).
[40] *Capital One Data Breach Compromises Data of Over 100 Million*, *supra* note 8.