ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

November 1, 2017

The Honorable Bob Latta
Chairman
Digital Commerce and
Consumer Protection Subcommittee
2125 RHOB
Washington D.C. 20515

The Honorable Janice Schakowsky
Ranking Member
Digital Commerce and
Consumer Protection Subcommittee
2125 RHOB
Washington D.C. 20515

Re: Hearing on Securing Consumers' Credit Data in the Age of Digital Commerce

Dear Chairman Latta and Ranking Member Schakowsky:

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 35,000 dues-paying members and well over 1 million followers on social networks, we focus on promoting policies that benefit both creators and users of technology. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

There is very little doubt that Equifax's negligent security practices were a major contributing factor in the massive breach of 145.3 million Americans' most sensitive information. In the wake of the breach, EFF has the following policy suggestions for the subcommittee to consider in order to reduce the possibility of a future catastrophic breach and just as importantly, ensure that victims of these data breaches are made whole when a company is negligent with their sensitive data.

Congress Should Create a Victims Advocate to Assist Americans and Produce Empirical Data on the Financial Harms of Breaches

When almost half of the country has been victimized by a data breach, it's time for the federal government to begin devising a support structure for the victims. While the focus rightfully is on Equifax and it's negligent security, Congress should dedicating resources for victims. If a consumer's information is compromised, there is a complex process to wade through to figure out who to call and what kind of protections to place on one's credit information. A position should be created within the Executive branch and should be given the necessary prominence to direct federal resources for victim's assistance.

More importantly, this position would be in-charge of producing rigorous research reports on financial harms these data breaches inflict on the American public. This information will be critical federal courts have established a high bar for plaintiffs to sue negligent companies like Equifax. Under the *Spokeo* decision, the judiciary has effectively kept most data breach cases out of litigation because plaintiffs are not able to prove their harm in a

concrete manner[1]. Federal research and data analyzing the financial harm Americans have faced will help bridge that gap. If legal representation for victims can point to empirical data demonstrating that their clients have been harmed, then companies like Equifax will face the appropriate liability for their conduct and be held accountable for their failures to secure data.

Congress Should Avoid Creating New Criminal Laws

A kneejerk reaction to a significant breach like Equifax is to think that we need additional criminal laws aimed at those who are responsible. But the reality is, new criminal punishments would not have done anything to ensure that Equifax applies crucial security patches when they are available. This is because Equifax is solely at fault for the breach as they had ample opportunity to remedy the situation before it happened. Rather than expand criminal penalties Congress should incentivize protecting the data.

In our public interest litigation practice representing security testers, it is our experience that the laws that exist today hinder security researchers who wish to keep the public informed. For instance in Equifax's case, a security researcher had warned the company about its security vulnerabilities *months before* the actual breach happened; yet the company didn't do anything to fix them[2]. The security researcher couldn't go public with the findings without risking significant civil and criminal liability. Without a meaningful way for security testers to raise problems in a public setting, companies have little reason to keep up with the latest security practices and can use the law to suppress embarrassing disclosures. If Congress enhances or expands criminal penalties for unauthorized access under laws like the Computer Fraud and Abuse Act (CFAA), we'd all be worse for it. Rather, companies and the law should favor security audits by outside parties and publication of their findings to keep the public informed.

Protect Victims' Day in Court

As noted above, it is already a challenge for those seeking a remedy for data breach harms to get into court at all. For too many people impacted by data breaches, they learn to their great dismay that somewhere in the fine print of the agreement they had to click on or are otherwise subject to a waiver of their legal rights. While the mandatory arbitration clauses Equifax originally pursued received substantial negative press attention to pressure the

---

[1] Cindy Cohn & Amul Kalia, *Will Equifax Data Breach Finally Spur Courts (and Lawmakers) to Recognize Data Harms?*, DEEPLINKS BLOG, available at https://eff.org/deeplinks/2017/09/will-equifax-data-breach-finally-spur-courts-and-lawmakers-recognize-data-harms.

[2] Lorenzo Franseschi-Bicchierai, *Equifax Was Warned*, MOTHERBOARD, available at https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning.

company to desist, Congress should ensure that victims are entitled to all of their legal rights.

Prohibiting companies like Equifax from impairing any legal remedy in exchange for generally weak assistance like credit monitoring is essential given the scale of harm and likely repeat harms into the future. Failing to protect victims' ability to seek damages to their fullest will result in companies receiving a substantial windfall of reduced liability while inflicting catastrophic losses on the American public.

Congress Should Establish a Floor for Data Breach Laws

Any federal laws that are passed in response to data breaches should be the foundation upon which state's can build upon according to their needs. This would allow states to effectively update their laws and enforcement power on behalf of their citizens while yielding the extra benefit of assisting people that live in other states.

For example, California has one of the strongest data breach notification law in the country and EFF was actively engaged in its creation. Given the size of the state it effectively serves as a national notice system. By the time a company has to comply with California's law, the company has infrastructure in place to notify the rest of the country. States have a tendency to be capable of responding quickly to changing data collection practices and Congress should not pass a law that would gut their ability to do so.

Federal Trade Commission Needs to Have Rule-making Authority

Federal regulators have little power to ensure that entities like Equifax aren't negligent in their security practices. We rely on credit agencies to get essential services in our lives—apartments, mortgages, credit cards, just to name a few—yet the fact that they don't have to abide by a basic framework of standards to protect our sensitive information is detrimental to data security.

Congress needs to empower an expert agency like the Federal Trade Commission (FTC), which has a history and expertise in data security[3], by restoring its rule-making authority to set security standards and enforce them. FTC's current limitation to only get involved in matters of unfair dealing and deceptive conduct are inadequate to address the increasingly sophisticated technological landscape and collection of personal data by third parties.

[3] FEDERAL TRADE COMMISSION, *Data Security*, available at https://www.ftc.gov/datasecurity

Create a Fiduciary Duty for Credit Bureaus to Protect Information

We live under a system where we need to rely on credit bureaus to execute even the most basic financial transactions. Very few of us chose to have our most sensitive information be hoarded by an entity like Equifax that we have no control over. Congress has the power to ensure that a credit bureau has special obligations and create a fiduciary duty for the bureaus to protect an individuals data. Without obligations to the individual to have adequate security practices, we will see more breaches on the scale of Equifax.

Free Credit Freezes, Not Credit Monitoring Services

It's become almost standard practice to offer data breach victims credit monitoring services. In reality, these services offer little protection to victims of data breaches[4]. Many of them are inadequate in the alerts they send consumers, and more fundamentally, there's little utility in being informed of improper usage of one's credit information *after* it's already been exploited. Consumers will still potentially have to spend hours to get their information cleared up with the various credit bureaus and entities where the information was used fraudulently. Instead, Congress should focus on ensuring that victims of data breaches get access to free credit freezes, which are much more effective in preventing financial harm to victims of data breaches.

We thank the subcommittee for holding this hearing and beginning the long process of investigating what happened and hopefully moving forward on legislation to improve the data security of all Americans. EFF stands ready support those efforts.

Sincerely,

Electronic Frontier Foundation

[4] KREBS ON SECURITY, *Are Credit Monitoring Services Worth it?*, available at https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/.