MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

September 13, 2017

The Honorable Maureen K. Ohlhausen
Acting Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Acting Chairwoman Ohlhausen,

I write you in the wake of reports that one of the nation's three major credit reporting agencies has suffered one of the largest, and potentially most impactful, breaches in recent history. According to reports, Equifax in May of this year experienced a breach affecting as many as 143 million consumers, with highly sensitive information such as Social Security numbers, driver's license records, birthdates, addresses, and credit histories potentially at risk. This information – critical to opening a new bank account or taking out a loan – will expose Americans to identity theft, tax fraud, extortion, and other risks.

By streamlining and routinizing the collection of consumer reports and credit history, the Fair Credit Reporting Act in part enshrined the nation's major credit reporting agencies' role as arbiters of Americans' access to credit, and even employment and residential opportunities. At the same time, Congress sought to ensure that these firms "exercise their grave responsibilities" with a "respect for the consumer's right to privacy," including through "reasonable procedures…with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information[.]"[1] And Congress directed the Federal Trade Commission ("Commission" or "FTC") to enforce key aspects of the law, including by treating violations of the FCRA as unfair or deceptive practices under the Commission's Section 5 authority.

Today's digital economy, in which data increasingly represents a key input, has only amplified the reach of these firms, and provided them with incentives to collect and centralize ever-growing amounts of sensitive personal information, and to commercialize this data in opaque ways. The volume and sensitivity of the data potentially involved in this breach raises serious questions about whether firms like Equifax adequately protect the enormous amounts of sensitive data they gather and commercialize.

As someone who has worked for several years with stakeholders and a bipartisan group of lawmakers on legislation to establish a comprehensive, nationwide and uniform data breach standard, I recognize Congress's unfinished work in this area. I am hopeful that this recent

[1] 15 USC §§ 1681(a)(4) and (b).

development will help galvanize action among my colleagues in Congress to safeguard American consumers and our nation's economic security.

At the same time, aspects of this breach raise questions about the data security practices of Equifax that implicate the Federal Trade Commission's existing authority. In particular, press reports and cybersecurity experts have identified a number of security lapses, including in the days following Equifax's disclosure of the breach, that potentially indicate a pattern of security failings.

While the precise details of the "website application vulnerability" exploited in the Equifax breach are not yet known, experts have pointed to a wide range of other lapses by Equifax – including in the wake of the breach – that indicate exceptionally poor cybersecurity practices. For instance, experts have pointed to an exceedingly broad attack surface, with thousands of domains and subdomains managed by Equifax across hundreds of network hosts. And security experts have identified a range of antiquated, unpatched, or otherwise vulnerable systems maintained by Equifax.

Equifax's post-breach actions also raise serious concerns about the company's data security practices. For instance, Equifax chose to register a new domain, Equifaxsecurity2017.com – but not in its own name. Reports also catalogued a litany of security mistakes, including use of potentially insecure content management software and improperly configured web encryption.[2] These, and other lapses, resulted in a range of popular web browsers flagging Equifax's site as a potential phishing or scam site.

Equally alarming have been Equifax's procedures for handling customer inquiries. In order for a concerned consumer to determine if they may have been impacted, Equifax requires the consumer to submit their last name and *six* digits of their Social Security number. The security of this procedure is as questionable as its efficacy: researchers noted that entering the last name "Test" and the Social Security numbers "123456" returned a confirmed breach.

Similarly alarming, when concerned consumers elect to place a credit freeze with Equifax – something the Commission encourages them to do – the PIN that Equifax assigns to that consumer is a simple, non-unique timestamp (formatted as, for instance, "0910170930" for a user that submitted a request at 9:30AM on the 10th of September). Separately, experts have noted that Equifax's central website, where American consumers go to set up credit account monitoring, features cross-site scripting vulnerabilities that would enable an attacker to execute malicious code to, for instance, redirect submitted form data (such as the Social Security number the Equifax site requests) to an attacker.[3]

Taken as a whole, and given past breaches by other major credit bureaus, these lapses may potentially represent a systemic failure by firms currently incentivized to collect and store highly sensitive identification and financial data for Americans. The volume and sensitivity of the data

---

[2] Dan Goodin, "Why the Equifax Breach Is Very Possibly the Worst Leak of Personal Info Ever," Ars Technica (Sept. 8, 2017), *available at*: https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/.

[3] Zack Whittacker, "Equifax's Credit Report Monitoring Site Is Also Vulnerable to Hacking," ZDNet (Sept. 12, 2017), *available at*: http://www.zdnet.com/article/equifax-freeze-your-account-site-is-also-vulnerable-to-hacking/.

involved – information critical to identity management and access to consumer credit – distinguishes this breach from many other breaches of consumer data. And in contrast to other breaches, where consumers might respond to the perceived lack of data security by taking their business elsewhere, those affected by last week's breach in most cases do not have a direct consumer relationship with Equifax.

The implications of a breach of this magnitude are sobering, as this identifying data forms the basis for consumer credit and other financial transactions. Congress foresaw this threat in 1970, noting that failures of this industry could "undermine the public confidence which is essential to the continued functioning of the banking system."[4] In ways similar to the financial service industry's systemic risk designation, I fear that firms like Equifax may illustrate a set of institutions whose activities, left unchecked, can significantly threaten the economic security of Americans.

I respectfully request that you respond to the following questions:

1. Equifax is currently under a consent decree with the Commission for violations of the Fair Credit Reporting Act related to improper handling of consumer information.[5] Does that consent decree provide the Commission with additional remedies in the context of Equifax's data security practices?

2. Given the current inability of consumers to cease doing business with a credit reporting agency which displays an arguably cavalier attitude toward cybersecurity, should the Fair Credit Reporting Act be amended to provide the Commission authority to issue rules requiring credit reporting agencies to establish a way for consumers to "opt out" of having their information stored by a particular credit reporting agency?

3. In many cases, Equifax collects and maintains sensitive information about consumers as a service to other businesses. Under state data breach notification statutes, a breached service provider need only inform the business it provides service to about the breaches it suffers, and has no obligation to provide public notice that it incurred the breach. In recent breach incidents involving third-party service providers, some companies (e.g., Heartland, Experian, Anthem, etc.) have provided public notice that their breach affected consumers. Would the FTC support legislation that requires all entities suffering a breach of security that creates a significant risk of financial harm, to make public notice of that breach in order to ensure a more timely and effective form of notice?

4. Do you interpret the Fair Credit Reporting Act to include heightened data security standards and/or requirements, given Congress's unique concern about the "confidentiality, accuracy…and proper utilization" of this highly sensitive data?

---

[4] 15 U.S.C. §1681.

[5] Federal Trade Commission Press Release, "FTC Approves Final Order Settling Charges Against Equifax Information Services LLC," (March 15, 2013), *available at*: https://www.ftc.gov/news-events/press-releases/2013/03/ftc-approves-final-order-settling-charges-against-equifax.

5. The Commission has suggested that consumers place a credit freeze with the three major credit bureaus.[6] Does the Commission consider a timestamp to be a sufficiently strong PIN for unfreezing a consumer's account?
    a. Has the Commission issued guidance to credit reporting agencies on adequate security and data protection measures associated with credit freezes?
    b. Should this guidance be updated in light of security concerns with the site Equifax maintains to process credit monitoring and freeze requests?

6. Should Congress limit the ability of credit reporting agencies to sell data outside specific contexts, such as credit, banking, and employment inquiries?

7. Does the Commission hold lapses in data security practices *in response to a breach* to a higher standard than data security practices related to the breach itself?

8. Do adequate incentives to use reasonable data security practices, or penalties to deter unreasonable data security practices, exist to counter-balance the profit incentives to collect, centralize, and maintain large quantities of highly sensitive personal information of American consumers?

The American people deserve to know that their government is serious about learning from and responding to this truly concerning incident, and that it is taking all appropriate steps to help ensure it cannot happen again. Your response will be critical to this process, and I look forward to receiving that within the next two weeks. If you should have any questions or concerns, please contact office.

As always, I appreciate your service in this important role. Thank you for your timely consideration of this matter.

Sincerely,

Mark R Warner

MARK R. WARNER
United States Senator

---

[6] Federal Trade Commission, "The Equifax Data Breach: What to Do," (Sept. 8, 2017), *available at*: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.