What the Next Congress Should Do to Prevent a Recurrence of the Equifax Data Breach

Prepared for Rep. Elijah E. Cummings and Rep. Eddie Bernice Johnson

Report of the Democratic Staffs of the
Committee on Oversight and Government Reform and
Committee on Science, Space and Technology
U.S. House of Representatives

December 10, 2018

I. BIPARTISAN INVESTIGATION CONFIRMS PREVIOUS FINDINGS ABOUT EQUIFAX BREACH, BUT DISREGARDS DEMOCRATIC REFORMS

On September 7, 2017, Equifax announced that hackers had breached its cybersecurity defenses and obtained the personally identifiable information (PII) of more than 143 million Americans.[1] Equifax is one of the three largest credit bureaus and collects detailed personal information about consumers, including Social Security Numbers, birth dates, addresses, driver's license numbers, and credit card numbers.

Shortly after this announcement, the Committee on Oversight and Government Reform and the Committee on Science, Space and Technology initiated a joint investigation into the cause of and measures to help prevent future breaches.[2] The investigation was a rare bipartisan initiative. The Committees conducted interviews of company executives and reviewed thousands of pages of company documents. In addition, Democratic staff met with consumer advocacy groups.

Unfortunately, Committee Republicans issued a report without including Democratic suggestions to prevent data breaches in the future. This was a missed opportunity to convert the Committees' oversight efforts into concrete reforms that would help prevent future data breaches, hold companies accountable, and protect American consumers and their sensitive personal information.

The Republican report merely reiterated findings by media outlets and analysis by the Government Accountability Office (GAO) about Equifax's cybersecurity vulnerabilities and the company's lack of preparedness to protect breach victims, including the following:

- According to a September 2017 article in *Wired*, attackers entered Equifax's system from mid-March through May 2017 via a web-application vulnerability. Equifax failed to implement a patch to fix it—a patch that had been available since March 2017. In other words, the credit-reporting giant had more than two months to take precautions that would have defended the personal data of 143 million people from being exposed.[3]
- Over a period of 76 days, attackers slowly extracted data from 51 Equifax

---

[1] *Equifax Reveals Hack That Likely Exposed Data of 143 Million Customers*, Reuters (Sept. 7, 2017) (online at www.reuters.com/article/us-equifax-cyber/equifax-reveals-hack-that-likely-exposed-data-of-143-million-customers-idUSKCN1BI2VK).

[2] Letter from Chairman Lamar Smith, Committee on Science, Space and Technology, and Chairman Trey Gowdy, Committee on Oversight and Government Reform, to Richard F. Smith, Chairman and Chief Executive Officer, Equifax (Sept. 14, 2017) (online at https://oversight.house.gov/wp-content/uploads/2017/09/2017-09-14-Smith-Gowdy-to-Equifax-due-9-28.pdf).

[3] *Equifax Officially Has No Excuse*, Wired (Sept. 14, 2017) (online at www.wired.com/story/equifax-breach-no-excuse/).

databases in small increments to avoid detection.[4]

- Equifax misdirected consumers to a fake Equifax website.[5]

- Equifax also failed to provide consumers full protection from new account identity theft.[6]

II. NEW LAWS NEEDED TO THWART FUTURE CONSUMER DATA ATTACKS

Based on the investigation conducted by the Committees, four key legislative reforms proposed by Democrats would help prevent future cyberattacks: hold federal financial regulatory agencies accountable for their consumer protection oversight responsibilities; require federal contractors to comply with established cybersecurity standards and guidance from the National Institute of Standards and Technology (NIST); establish high standards for how data breach victims should be notified; and strengthen the ability of the Federal Trade Commission (FTC) to levy civil penalties for private sector violations of consumer data security requirements. Each legislative proposal is discussed in detail below.

A. Congress should require federal financial regulatory agencies to report on their efforts to fully exercise their existing authorities to protect consumers from cybertheft and to identify areas in which Congress could enhance agencies' authorities to achieve that goal.

Congress has authorized federal financial regulatory agencies to protect consumers by examining the procedures and controls used by banks and credit reporting agencies, but those powers were not fully exercised before the Equifax data breach.

For example, the Bureau of Consumer Financial Protection (CFPB) has authority to examine credit reporting agencies, such as Equifax.[7] Under its "Larger Participant Rule," CFPB may "assess compliance with federal consumer financial laws as well as detect and assess additional risks to consumers."[8] In addition, supervision may include requiring reports,

---

[4] Government Accountability Office, *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, (Aug. 2018) (GAO-18-559) (online at www.gao.gov/assets/700/694158.pdf).

[5] The fake website was created by a non-Equifax software engineer to imitate the website Equifax created to provide consumers with information about the security breach. *See Someone Made a Fake Equifax Site. Then Equifax Linked to It*, New York Times (Sept. 20, 2017) (online at www.nytimes.com/2017/09/20/business/equifax-fake-website.html).

[6] U.S. PIRG, *Equifax Breach: One Year Later* (Sept. 6, 2018) (online at https://uspirg.org/reports/usp/equifax-breach-one-year-later).

[7] Consumer Financial Protection Bureau, *CFPB to Supervise Credit Reporting* (July 16, 2012) (online at www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-to-superivse-credit-reporting/).

[8] Bureau of Consumer Financial Protection, *Defining Larger Participants of the Consumer Debt Collection Market*, 77 Fed. Reg. 65775 (Oct. 31, 2012) (online at www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26467.pdf).

conducting examinations, and ongoing monitoring.[9]

Under this authority, CFPB should have been able to assess Equifax's preparedness to prevent data breaches and to notify and respond to victims of identity theft in the event of a data breach. Such examinations would have revealed the severe deficiencies in Equifax's security patch implementation and breach notification protocols. CFPB also may require credit reporting agencies to establish protocols for the types and duration of remedies available to consumers who have been affected by data breaches.

Similarly, bank regulatory agencies have statutory authority to examine third parties that provide services to their supervised banks, including credit reporting agencies.[10] Under federal financial information technology (IT) examination guidance, banking regulators may examine banks and the third parties they contract with to assess their cybersecurity preparedness.[11] Through such examinations, bank regulatory agencies also could have identified Equifax's cybersecurity weaknesses.

These existing authorities were not used effectively with respect to Equifax. Congress should require federal financial regulatory agencies to identify and report to Congress on how they exercise existing authorities to protect consumers from cybertheft. If they believe they do not have adequate authorities under existing law to conduct this work, they should report to Congress on how those authorities could be enhanced to help them carry out those responsibilities.

B. Congress should require all contractors that provide information services to the federal government to comply with cybersecurity standards and guidance established by the National Institute of Standards and Technology.

Equifax was a federal contractor at the time of its data breach, but it was not subject to federal cybersecurity standards that currently apply to Department of Defense (DOD) contractors. Contractors that provide information services to DOD may be subject to NIST's Special Publication 800-171, which requires that they "develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities" and "monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls." They also require updating malware protections and reporting data breaches.[12]

GAO reported that Equifax did not directly notify major federal customers of the 2017 breach prior to its public announcement because its contracts required notification of only those

[9] *Id.*

[10] Under the Bank Service Company Act, banking regulators have statutory authority to examine third parties that provide services to their supervised banks. 12 U.S.C.§1867(c).

[11] Federal Financial Institutions Examination Council, *IT Examination Handbook InfoBase* (online at https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iia-risk-identification/iia3-supervision-of-cybersecurity-risk-and-resources/iia3(a)-supervision-of-cybersecurity-risk.aspx).

[12] NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (June 2015) (online at https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-171.pdf).

breaches directly involving the systems that provided services to the federal government. Internal Revenue Service and Social Security Administration officials reported that they made changes to contracts they had with Equifax to require prompt notification of any future breach.[13]

Congress should require that this guidance be expanded to apply to all contractors providing IT related services to the federal government.

C. Congress should enact a comprehensive federal notification law to govern the process to notify data breach victims, including timeframes, methods, and parties that should be informed when PII is compromised.

Equifax did not notify the public immediately about its breach, but instead allowed more than five weeks to pass before disclosing the breach to customers.[14] A comprehensive federal notification law would clarify the actions entities should take to notify victims after a breach.

For example, Congress could consider a tiered notification approach that would require an initial public notification when an entity has determined that a breach has occurred, followed by subsequent updates until a full cybersecurity investigation is completed. H.R. 3896, the Secure and Protect Americans' Data Act, includes other potential notification requirements, including:

- expeditious and practical notification of a breach to individuals if PII is compromised;
- notification to agencies with jurisdiction if a certain threshold of persons affected is reached; and
- the use of various communication methods, including mail, email, phone, and posting on the entity's website.[15]

Other bills include accountability by third parties to notify the entities for which they are collecting or otherwise handling PII if the third party experiences a breach.[16] Delayed notifications to accommodate for law enforcement or national security investigations also should be considered.

D. Congress should amend the Federal Trade Commission Act to strengthen civil penalty enforcement authority for violations of personal information

[13] Government Accountability Office, *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach* (Aug. 2018) (GAO-18-559) (online at www.gao.gov/assets/700/694158.pdf).

[14] Staff Report of Senator Elizabeth Warren, *Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information* (Feb. 2018) (online at www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf).

[15] H.R. 3896 (online at www.congress.gov/bill/115th-congress/house-bill/3896).

[16] H.R. 3975 (online at www.congress.gov/bill/115th-congress/house-bill/3975) and S. 2124 (online at www.congress.gov/bill/115th-congress/senate-bill/2124).

and data security requirements.

In the three years before the Equifax data breach, the company spent only about 3% of its operating revenue on cybersecurity—less than the company spent on stock dividends.[17] Since the breach, Equifax has invested hundreds of millions of dollars in new, upgraded data security infrastructure, including new tools, technologies, and equipment.[18]

Equifax also has worked to apply best practices in its data management procedures—including data encryption and data segmentation. As part of these upgrades, Equifax increased its IT staffing, enhanced its cybersecurity expertise, and procured additional equipment. According to the company's new chief information and security officer, Equifax executives now understand the critical importance of security and risk management.[19]

Equifax's failure to deploy necessary security patches to prevent this massive data breach constitutes an unfair practice under Section 5 of the Federal Trade Commission Act, which is defined as action that could pose substantial injury to consumers that is not reasonably avoidable by consumers themselves.[20]

Under existing law, FTC and the violator may enter into a consent order that sets forth steps to resolve the violations.[21] However, FTC is restricted to imposing civil penalties only if the violator fails to comply with its consent order.[22]

Democratic and Republican-appointed FTC chairmen have testified that Congress should provide FTC authority to assess civil penalties for violations of personal information and data security requirements, and not merely for non-compliance with consent orders agreed to after those violations.[23] For example, Joe Simons, the current FTC Chairman appointed by President Trump, recently explained that Section 5 "does not provide for civil penalties, reducing the Commission's deterrent capability."[24]

---

[17] Staff Report of Senator Elizabeth Warren, *Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information* (Feb. 2018) (online at www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf).

[18] *Equifax CISO Jamil Farshchi's Three-Act, 'Shared Fate' Security Plan*, Cyberscoop (July 13, 2018) (online at www.cyberscoop.com/jamil-farshchi-equifax-ciso-apache-struts/).

[19] *Id*.

[20] 15 U.S.C § 45(n).

[21] 15 U.S.C § 45(m).

[22] *Id*.

[23] *Prepared Statement of the Federal Trade Commission on Protecting Personal Consumer Information From Cyber Attacks and Data Breaches*, Senate Committee on Commerce, Science and Transportation (Mar. 26, 2014) (online at www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf).

[24] *Prepared Statement of the Federal Trade Commission: "Oversight of the Federal Trade Commission,"* House Committee on Energy and Commerce, Subcommittee on Digital Commerce and Consumer Protection (July 18, 2018) (online at www.ftc.gov/system/files/documents/public_statements/1394526/p180101_ftc_testimony_re_oversight_house_0718 2018.pdf).

Civil penalties would incentivize private sector companies to prioritize and invest in continually upgrading and deploying modernized IT solutions and applying cybersecurity best practices. Companies that fail to proactively make adequate cybersecurity modernizations and upgrades—applying relevant NIST-cybersecurity standards, for instance—could be cited for unfair practices and face significant legal and financial penalties.