U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

October 1, 2017

TO: Members, Subcommittee on Digital Commerce and Consumer Protection

FROM: Committee Majority Staff

RE: Hearing entitled "Oversight of Equifax Data Breach: Answers for Consumers"

I. INTRODUCTION

The Subcommittee on Digital Commerce and Consumer Protection will hold a hearing on Tuesday, October 3, 2017, at 10:00 a.m. in 2123 Rayburn House Office Building. The hearing is entitled "Oversight of Equifax Data Breach: Answers for Consumers."

II. WITNESS

- Richard F. Smith, former Chairman and Chief Executive Officer, Equifax, Inc.

III. BACKGROUND

On September 7, 2017, Equifax, Inc. released a public statement that its systems had been breached resulting in the loss of 143 million Americans' personal information.[1] Information taken from the Equifax system included names, Social Security numbers, birthdates, addresses, and in some cases driver's license information. In addition, over 200,000 people had their credit card information stolen, and over 180,000 people had credit dispute documentation stolen.[2] Consumer information for certain U.K. and Canadian residents was also implicated.[3]

Since the public disclosure, Equifax announced that Richard Smith retired as Chairman of the Board and Chief Executive Officer, effective September 26, 2017, but remains an unpaid advisor to the company.[4] Paulino do Rego Barros, Jr., who most recently served as President, Asia Pacific, was appointed interim CEO, and current Board member, Mark Feidler, was designated Non-Executive Chairman.[5] On September 15, 2017, Equifax announced the retirement, with immediate effect, of Chief Information Officer David Webb and Chief Security Officer Susan Mauldin.[6] Mark Rohrwasser was appointed interim Chief Information Officer, and Russ Ayres was appointed interim Chief Security Officer.[7]

[1] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628
[2] Id. According to Equifax, there was no evidence of unauthorized activity on "core consumer or commercial credit reporting databases" which hold more specific information including payment history.
[3] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628
[4] https://investor.equifax.com/news-and-events/news/2017/09-26-2017-140531280
[5] Id.
[6] https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832
[7] Id. Mr. Rohrwasser joined Equifax in 2016 and had led Equifax's International IT operations since that time. Mr. Ayres most recently served as a Vice President in the IT organization at Equifax.

This most recent Equifax breach—affecting nearly 50% of the total U.S. population—is not an isolated, limited incident. It is the fifth largest data breach, according to press reports,[8] and potentially one of the most damaging because of the sensitivity of information stolen including full nine-digit Social Security numbers. Recent data from the Identify Theft Resource Center (ITRC) indicates that as of September 21, 2017, over 1000 data breaches have occurred this year alone, exposing over 163 million records.[9] Data breaches have become so commonplace that data security experts have expressed concerns about "breach fatigue."

Data is a vital asset and hackers, criminals, and nation-states are working to seek out vulnerabilities and overcome cyber-defenses, to acquire and exfiltrate sensitive data, and to exploit that data in ways that may cause substantial financial harms such as fraud or identity theft. According to a Javelin Strategy & Research Study, in 2016, approximately 15.4 million Americans were victims of fraud or identity theft, losing a total of $16 billion to criminals.[10] Synthetic identity theft, a form of application fraud in which criminals use fake personas to abuse credit, cost lenders $6 billion in 2016, according to a published industry analysis.[11]

In the wake of the Equifax data breach, over 30 House and 30 Senate members have sent written letters to Equifax, Inc., as well as the Federal Trade Commission, Consumer Financial Protection Bureau, Securities and Exchange Commission, Social Security Administration, and Government Accountability Office. Separately, over 32 State Attorneys General have sent a letter to Equifax and at least one State Attorney General has filed suit against Equifax.[12]

A. TIMELINE OF EVENTS

Mar. 7	Security flaw reported in Apache Struts software utilized in at least one Equifax website. Apache Struts software patch issued the same day.[13] "Equifax's Security organization was aware of this vulnerability at that time."[14]
May 13	"Equifax believes the unauthorized accesses to certain files containing personal information occurred from May 13 through July 30, 2017."[15]
July 29	"Equifax's Security team observed suspicious network traffic associated with its U.S. online dispute portal web application. . .the Security team investigated and blocked the suspicious traffic that was identified."[16]

[8] https://www.usatoday.com/story/tech/2017/09/07/nations-biggest-hacks-and-data-breaches-millions/644311001/
[9] http://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachStatsReportSummary2017.pdf
[10] https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new
[11] http://www.acg.net/synthetic-identity-fraud-cost-banks-6-billion-in-2016-auriemma-consulting-group/
[12] http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-09-19-equifax-lawsuit.html; http://www.mass.gov/ago/docs/press/2017/equifax-complaint.pdf
[13] http://struts.apache.org/announce.html#a20170307-2
[14] https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832
[15] Id.
[16] Id.

July 30	"The Security team continued to monitor network traffic and observed additional suspicious activity. . .In response, the company took offline the affected web application that day."[17]
Aug. 1-2	Three Equifax executives, including the CFO, reportedly sold nearly $2 million worth of stock.[18]
Aug. 2	"Equifax contacted a leading, independent cybersecurity firm, Mandiant, to assist in conducting a privileged, comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted."[19]
Aug. 22	According to the Wall Street Journal, Equifax registered the new domain name www.equifaxsecurity2017.com.[20]
Sept. 7	"As soon as the company understood the potentially impacted population, a comprehensive support package was rolled out to consumers"[21] via dedicated website www.equifaxsecurity2017.com
Sept. 15	Equifax announced the retirement of the Chief Information Officer David Webb and Chief Security Officer Susan Mauldin. Mark Rohrwasser is installed as interim Chief Information Officer, and Russ Ayres as interim Chief Security Officer.[22]
Sept. 26	Equifax announced Chairman and CEO Richard Smith retires, with immediate effect, but remains an unpaid advisor to the company. Paulino do Rego Barros, Jr., who most recently served as President, Asia Pacific is appointed interim Chief Executive Officer.[23]
Sept. 28	Equifax interim CEO Paulino do Rego apologizes in a Wall Street Journal op-ed for the data breach and outlines enhanced consumer protection services to be provided.[24]

B. DATA SECURITY STATUTES AND AUTHORITY

The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) requires a financial institution to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of the information, and to protect against

[17] Id.
[18] https://www.bloomberg.com/news/articles/2017-09-12/dozens-of-senators-seek-probe-of-equifax-executives-stock-sales; https://www.bloomberg.com/news/articles/2017-09-18/equifax-stock-sales-said-to-be-focus-of-u-s-criminal-probe
[19] https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832
[20] https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318?shareToken=st7d9a987129fe43eba2a7852049aab49b&reflink=article_email_share
[21] https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832
[22] Id. Although the Sept. 15 press release indicates "personnel changes are effective immediately," Committee discussions with Equifax have revealed that Susan Mauldin may still be employed by the company until the end of the year.
[23] https://investor.equifax.com/news-and-events/news/2017/09-26-2017-140531280
[24] https://www.wsj.com/articles/on-behalf-of-equifax-im-sorry-1506547253

unauthorized access to or use of information which could result in substantial harm or inconvenience to any customer.[25]

The FTC and financial regulators have established these standards through the "Safeguards Rule" which took effect in 2003.[26] The Safeguards Rule requires financial institutions to have a written information security plan that describes their program to protect customer information.[27] Companies can implement safeguards appropriate to their own circumstances (i.e., taking into account company size, the nature of business activities, and sensitivities of the collected data). As part of its plan, each company must: 1) designate a program manager or team to coordinate its information security program; 2) conduct risk assessment to customer information, and evaluate the effectiveness of the current safeguards for controlling these risks; 3) design and implement a safeguards program that mitigate information risks, and regularly monitor and test it; 4) select service providers that can maintain appropriate safeguards, and make sure contracts with service providers and vendors requires them to maintain safeguards; and 5) evaluate and adjust the program periodically in light of relevant circumstances.

The Safeguards Rule also requires companies to assess and address the risks to customer information in all areas of their operation, including three areas that are particularly important to information security: 1) employee management and training; 2) information systems; and 3) detecting and managing system failures.

In addition to developing their own safeguards, companies covered by the rule are responsible for taking necessary steps to ensure that affiliated parties and third-party providers also safeguard customer information in their care.[28]

The Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) limits the use of consumer reports and access to credit data to those who have a legally permissible purpose.[29] Consumer Reporting Agencies (CRAs)—like Equifax—are entities that assemble consumer information for the purpose of issuing consumer reports to third parties. Consumer reports may be provided for particular purposes including making decisions involving credit, insurance, tenant screening, and employment screening. The FCRA requires that CRAs employ "reasonable efforts" to verify the identity of those to whom they supply consumer reports and that the recipient has a permissible purpose to use the report. The Dodd-Frank Act transferred most of the rulemaking responsibilities to the Consumer Financial Protection Bureau (CFPB), but the FTC retains enforcement authority under the FCRA.[30]

---

[25] Financial Services Modernization Act of 1999 (the Gramm-Leach-Bliley Act), Pub. L. 106-102, enacted Nov. 12, 1999.
[26] 16 CFR § 314.
[27] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule
[28] Id.
[29] 15 U.S.C. § 1681, et seq.
[30] https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act

The Federal Trade Commission Act

Section 5 of the Federal Trade Commission Act prohibits "unfair and deceptive acts or practices in or affecting commerce."[31] Section 5 prohibits companies from making deceptive claims regarding privacy or security they provide for consumer information. The Commission also uses Section 5 to enforce against unfair practices that are likely to cause consumers substantial injury that are neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition.[32]

As noted above, the FTC enforces the Safeguards Rule (implemented in GLBA) which sets forth data security requirements for financial institutions within the FTC's jurisdiction, and the FCRA rules dictating that consumer reporting agencies use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information.

The FTC has brought enforcement actions and obtained settlements in approximately 60 cases against businesses that it charged with failing to provide reasonable and appropriate protections for consumers' personal information.[33] Twelve cases have involved Safeguards Rule violations.[34] The FTC "does not require perfect security; that reasonable security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law."[35]

C. STATE DATA SECURITY AND BREACH NOTIFICATION LAWS

Forty-eight States, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification requirements. Twelve States have enacted legislation dealing with commercial data security.[36] The majority of those States have tied the standard to "reasonable" security, recognizing the challenges posed by technology proscriptive mandates. State laws in this area typically define personal information in terms of data that may lead to identifying a specific individual (e.g., a combination of first, middle, or last names; Social

---

[31] 15 U.S.C. § 45.
[32] https://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf
[33] https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf
[34] In August 2017, the online tax preparation service (TaxSlayer, LLC) agreed to settle Federal Trade Commission allegations that it violated the Safeguards Rule by failing to develop a written comprehensive security program until November 2015 (other violations were alleged). https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges
[35] https://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf
[36] Arkansas, California, Connecticut, Florida, Indiana, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah.

Security numbers; State identification numbers) and data that may lead to financial harm (e.g., financial account number; pins; passcodes).

IV. ISSUES

The following issues may be examined at the hearing:

- When did Equifax become aware that hackers had gained access to its computer systems? Over what period of time did the unauthorized access occur? When was senior leadership informed of the breach?

- Did Equifax have a breach response plan in place prior to the hack? If so, was it followed after this breach?

- How many U.S. consumers did the data breach incident affect, and what sensitive personal information was impacted?

- What subsequent details have been revealed as result of the forensic investigation into the breach incident?

- What concrete steps is Equifax taking to prevent a similar breach of its computer systems, and to protect American consumers now as well as in the future?

V. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Melissa Froelich, Paul Jackson or Bijan Koohmaraie of the Committee staff at (202) 225-2927.