

House Financial Services Committee Hearing on Equifax Data Breach

Overview

On Thursday, October 4, 2017, **Mr. Richard F. Smith**, Former Chairman and CEO of Equifax, [testified](#) before the House Financial Services Committee. The hearing, entitled “Examining the Equifax Data Breach,” was called in the wake of the Equifax data breach that occurred May 13 through July 30, 2017. According to recent reports, the breach of the company’s dispute portal is now estimated to affect more than 145.5 million Americans.

Key Takeaways

- **Calls for Penalties:** Several members of the committee called upon agencies to hold Equifax accountable, including the Federal Trade Commission (FTC) to bring an enforcement action against Equifax for a potential failure to comply with the Safeguards Rule.
- **More Hearings Requested:** Several members called for further hearings with officers who currently work at Equifax and have the ability to implement policy changes at the company. Specifically, the minority party of the committee called for a minority led hearing on Equifax.
- **Increased Attention to Data Security Legislation:** Additionally, expect further data security legislation to be introduced as several members called for legislation that would implement a higher data security and notification standard to replace the patchwork system of state laws currently in place.
- **Bills Introduced:** Bills will target all 3 major credit reporting agencies (CRAs) as well as others holding sensitive information.
 - [H.R.3783](#) — (Cohen D-TN) To amend the Fair Credit Reporting Act to prohibit the use of consumer credit checks against prospective and current employees for the purposes of making adverse employment decisions.
 - [H.R.3766](#) — (Himes D-CT) To amend the Fair Credit Reporting Act to require consumer reporting agencies to place a security freeze on a consumer report without a fee if the consumer reporting agency is subject to a breach of data security, and for other purposes.
 - [H.R.3755](#) — (Waters D-CA) To amend the Fair Credit Reporting Act to improve the consumer reporting system.

Opening Statements

In his opening statement, **House Financial Services Committee Chairman Jeb Hensarling (R-TX)** expressed support for a “consistent national standard for both data security and breach notification” to better protect consumers and hold companies accountable. The Chairman noted that the Committee approved legislation that would achieve those goals in December of 2015 with passage of the Data Security Act, stating the committee should revisit these issues and legislation to ensure agencies are “up to the job.”

In her opening statement, **Ranking Member Maxine Waters (D-CA)** called for an additional hearing to get more answers and questions surrounding the breach and solution for consumers. Rep. Waters stated, “I for one want to make sure that credit reporting agencies do not inappropriately profit off of this incident, by exploiting consumers’ legitimate fears.” She referenced her recently introduced legislation, H.R. 3755, the [Comprehensive Consumer Credit Reporting Reform Act](#). The legislation would “shift the burden of removing credit report mistakes to credit reporting agencies and away from consumers.” The bill would also limit the use of credit reports in employment checks and limiting when CRAs can collect information on consumers.

In his testimony, **Mr. Smith** accepted full responsibility for the breach and apologized to the public. He attempted to detail the timeline of discovery and response to the breach. He acknowledged two failures: a human error for the failure to apply a software patch and a technological error of a system that failed to detect the vulnerability. Mr. Smith identified that the company concluded by late August it was subject to a major breach. Equifax then focused its efforts on notification to consumers; deployment of a website, call centers, and free services; preparation for an increased threat of cyberattacks; and coordination with the FBI and other federal agencies. Despite these efforts, Mr. Smith acknowledged mistakes were made in the remediation rollout. He also used his testimony to announce the January 31, 2018 release of a free lock product to allow consumers to lock and unlock their credit.

Question and Answer Session

CFPB

Rep. Ann Wagner (R-MO) mentioned Director Cordray’s intention to provide accountability following the breach. Mr. Smith testified that he has not had any interactions with the CFPB prior to the breach regarding cyber security and has not had any communication with the CFPB since the breach.

Breach Notification

In response to **Chairman Hensarling’s** questions, Mr. Smith testified that the FBI did not dictate or delay the flow of communication or notification to the public. Rather, Equifax followed recommendations from Mandiant and King & Spalding and noted there was a delay in public notification because it took several weeks to have a clear and accurate understanding of the breach.

Mr. Smith testified that Equifax does not intend to individually notify the 145 million consumers affected through an email or letter. During a line of questioning from **Rep. Josh Gottheimer (D-NJ)**, Mr. Smith indicated the additional 2.5 million consumers that were later identified as having been breached were notified via mail.

Breach Investigation

Chairman Hensarling questioned the timeline of events that led to the breach. Mr. Smith testified that Equifax was notified of the vulnerability on March 8th. On March 9th Equifax disseminated communication about the patch within the company to those who needed to know. However, the individual responsible for patching process did not communicate to the person responsible for closing the patch. Then on March 15th the scanner did not detect the Apache vulnerability. Human error and technological error led to failure of the patch.

Rep. Kyrsten Sinema (D-AZ) inquired how the attackers were able to operate within Equifax's network without drawing attention to themselves. Mr. Smith noted the attackers were fairly sophisticated and did not trigger any file size or speed transfer alarms within the company's environment.

Rep. Claudia Tenney (R-NY) asked if Equifax took measures to coordinate with the other credit bureaus upon learning of the breach. Mr. Smith responded that Transunion and Experian were not notified before the public announcement on September 7th.

Rep. Randy Hultgren (R-IL) and **Rep. David Kustoff (R-TN)** asked if Equifax had pre-existing protocols in place to be prepared for a breach. Mr. Smith indicated they did have a crisis management playbook for many different scenarios, including a breach. In the protocol, there were no determination of actions based on the size of the breach.

Rep. David Scott (R-GA) called for an investigation from the Department of Justice, the CFPB, and the SEC to restore the public's confidence in the company and make sure "Equifax comes out clean and standing tall."

Rep. Keith Rothfus (R-PA) pressed on why Equifax is not willing to release the scope of the insurance coverage the company had in case of a breach. Mr. Smith argued that when you disclose such a number "it puts a target out there...for lawsuits."

Stock Sale

Rep. Brad Sherman (D-CA) questioned Mr. Smith regarding the sale of stock around the same time the company learned of the data breach. Mr. Smith testified that there is a clearing process for officers that they properly followed. **Rep. French Hill (R-AR)** asked if the company's general counsel had ever before cancelled the window for stock sales for certain officers due to a material non-public information effect. Mr. Smith confirmed "there were a few times, yes."

Rep. Warren Davidson (R-OH) questioned whether it was a mistake to not cancel pending trades, even if they had been ordered prior to the discovery of the breach.

Remediation Products

Ranking Member Waters and Rep. Lacy Clay (D-MO) asked how long consumers will have access to free services and protections. Mr. Smith discussed Equifax's free locking and unlocking product to allow consumers to control access to their data, which consumers will have access for life.

Rep. Luke Messer (R-IN) questioned if the information consumers provide when registering for the free remediation products will be shared and used for marketing purposes. Mr. Smith stated it is not Equifax's intent to cross-sell or up-sell consumers that are seeking to use the free services.

Data Protection

Mr. Smith stated that Equifax has conducted forensic reviews, remediation plans, and consultations to develop long term security improvement plans. Mr. Smith advocated for a public-private partnership to strengthen cyber security as well as to develop a different method of identification other than Social Security Numbers.

Rep. Carolyn Maloney (D-NY) discussed the Safeguards Rule that governs CRAs and whether the FTC will enforce this rule, stating this was a foreseeable, announced risk by the Department of Homeland Security (DHS). As the Safeguards Rule requires a patch management system to fix a vulnerability, she expressed outrage that Equifax failed to implement a fix in the face of an announced risk.

Arbitration

Rep. Brad Sherman said Equifax was hoping to “trick” consumers to forgo their right to sue disguised as a website advertised as a way to help consumers. Mr. Smith testified it was never intended to include the arbitration clause, rather it was a standard clause and was removed within 24 hours. **Rep. Scott** and **Rep. Gottheimer** also criticized Equifax on the use of the arbitration clause.

Effects on Lending

Rep. Nydia Velazquez (D-NY) as Ranking Member of Small Business Committee expressed concerns about the impact this breach will have on 29 million small businesses in the country. Mr. Smith responded that small business owners would be able to access Equifax’s free lock product and testified that the small business database Equifax housed was not compromised in the breach.

In response to questioning from **Rep. Andy Barr (R-KY)**, Mr. Smith testified that if every consumer froze their credit, as opposed to the lock option being offered by Equifax, it could have a devastating effect on access to credit. “A lock is far more user friendly,” Mr. Smith said.

Solving for Future Breaches

Rep. Bill Foster (D-IL) questioned whether data brokers should be required to have insurance to ensure consumers receive remuneration in the event of a breach. Mr. Smith responded that such a solution is not the answer.

Rep. Tom Emmer (R-MN) urged lawmakers to not make a snap-reaction to urge for more regulation, noting the cost of compliance may take resources away from more innovative efforts to prevent cyber-attacks. Mr. Smith did not believe more regulation would have addressed the shortcoming in the Equifax breach.