Prepared Testimony of Richard F. Smith
before the U.S. House Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

October 3, 2017

Chairman Latta, Ranking Member Schakowsky, and Honorable Members of the Subcommittee, thank you for the opportunity to testify today.

Preliminary Statement

I am here today to recount for this body and the American people, as best I am able, what happened when Equifax was hacked by a yet unknown entity and sensitive information of over 140 million Americans was stolen from its servers, and to outline the remediation steps the company took. We at Equifax clearly understood that the collection of American consumer information and data carries with it enormous responsibility to protect that data. We did not live up to that responsibility, and I am here today to apologize to the American people myself and on behalf of the Board, the management team, and the company's employees.

Let me say clearly: As CEO I was ultimately responsible for what happened on my watch. Equifax was entrusted with Americans' private data and we let them down. To each and every person affected by this breach, I am deeply sorry that this occurred. Whether your personal identifying information was compromised, or you have had to deal with the uncertainty of determining whether or not your personal data may have been compromised, I sincerely apologize. The company failed to prevent sensitive information from falling into the hands of wrongdoers. The people affected by this are not numbers in a database. They are my friends, my family, members of my church, the members of my community, my neighbors. This breach has impacted all of them. It has impacted all of us.

I was honored to serve as the Chairman and Chief Executive Officer of Equifax for the last 12 years, until I stepped down on September 25. I will always be grateful for the opportunity to have led the company and its 10,000 employees. Equifax was founded 118 years ago and now serves as one of the largest sources of consumer and commercial information in the world. That information helps people make business and personal financial decisions in a more timely and accurate way. Behind the scenes, we help millions of Americans access credit, whether to buy a house or a car, pay for college, or start a small business. During my time at Equifax, working together with our employees, customers, and others, we saw the company grow from approximately 4,000 employees to almost 10,000. Some of my proudest accomplishments are the efforts we undertook to build credit models that allowed and continue to allow many unbanked Americans outside the financial mainstream to access credit in ways they previously could not have. Throughout my tenure as CEO of Equifax, we took data security and privacy extremely seriously, and we devoted substantial resources to it.

We now know that criminals executed a major cyberattack on Equifax, hacked into our data, and were able to access information for over 140 million American consumers. The

information accessed includes names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers; credit card information for approximately 209,000 consumers was also stolen, as well as certain dispute documents with personally identifying information for approximately 182,000 consumers.

Americans want to know how this happened and I am hopeful my testimony will help in that regard. As I will explain in greater detail below, the investigation continues, but it appears that the breach occurred because of both human error and technology failures. These mistakes – made in the same chain of security systems designed with redundancies – allowed criminals to access over 140 million Americans' data.

Upon learning of suspicious activity, I and many others at Equifax worked with outside experts to understand what had occurred and do everything possible to make this right. Ultimately we realized we had been the victim of a massive theft, and we set out to notify American consumers, protect against increased attacks, and remediate and protect against harm to consumers. We developed a robust package of remedial protections for each and every American consumer – not just those affected by the breach – to protect their credit information. The relief package includes: (1) monitoring of consumer credit files across all three bureaus, (2) access to Equifax credit files, (3) the ability to lock the Equifax credit file, (4) an insurance policy to cover out-of-pocket costs associated with identity theft; and (5) dark web scans for consumers' social security numbers. All five of these services are free and without cost to all Americans. Equifax also recently announced an important new tool that has been under development for months that will allow consumers to lock and unlock their credit files repeatedly, for life, at no cost. This puts the control of consumers' credit information where it belongs – with the consumer. We have also taken steps to better protect consumer data moving forward.

We were disappointed with the rollout of our website and call centers, which in many cases added to the frustration of American consumers. The scale of this hack was enormous and we struggled with the initial effort to meet the challenges that effective remediation posed. The company dramatically increased the number of customer service representatives at the call centers and the website has been improved to handle the large number of visitors. Still, the rollout of these resources should have been far better, and I regret that the response exacerbated rather than alleviated matters for so many.

How It Happened

First and foremost, I want to respond to the question that is on everyone's mind, which is, "How did this happen?" In my testimony, I will address both what I learned and did at key times in my role as CEO, and what I have since learned was occurring during those times, based on the company's ongoing investigation. Chronologically, the key events are as follows:

On March 8, 2017, the U.S. Department of Homeland Security, Computer Emergency Readiness Team ("U.S. CERT") sent Equifax and many others a notice of the need to patch a particular vulnerability in certain versions of software used by other businesses. Equifax used

that software, which is called "Apache Struts," in its online disputes portal, a website where consumers can dispute items on their credit report.

On March 9, Equifax disseminated the U.S. CERT notification internally by email requesting that applicable personnel responsible for an Apache Struts installation upgrade their software. Consistent with Equifax's patching policy, the Equifax security department required that patching occur within a 48 hour time period. We now know that the vulnerable version of Apache Struts within Equifax was not identified or patched in response to the internal March 9 notification to information technology personnel.

On March 15, Equifax's information security department also ran scans that should have identified any systems that were vulnerable to the Apache Struts issue identified by U.S. CERT. Unfortunately, however, the scans did not identify the Apache Struts vulnerability. Equifax's efforts undertaken in March 2017 did not identify any versions of Apache Struts that were subject to this vulnerability, and the vulnerability remained in an Equifax web application much longer than it should have. I understand that Equifax's investigation into these issues is ongoing. The company knows, however, that it was this unpatched vulnerability that allowed hackers to access personal identifying information.

Based on the investigation to date, it appears that the first date the attacker(s) accessed sensitive information may have been on May 13, 2017. The company was not aware of that access at the time. Between May 13 and July 30, there is evidence to suggest that the attacker(s) continued to access sensitive information, exploiting the same Apache Struts vulnerability. During that time, Equifax's security tools did not detect this illegal access.

On July 29, however, Equifax's security department observed suspicious network traffic associated with the consumer dispute website (where consumers could investigate and contest issues with their credit reports). In response, the security department investigated and immediately blocked the suspicious traffic that was identified. The department continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, they took the web application completely offline that day. The criminal hack was over, but the hard work to figure out the nature, scope, and impact of it was just beginning.

I was told about the suspicious activity the next day, on July 31, in a conversation with the Chief Information Officer. At that time, I was informed that there was evidence of suspicious activity on our dispute portal and that the portal had been taken offline to address the potential issues. I certainly did not know that personal identifying information ("PII") had been stolen, or have any indication of the scope of this attack.

On August 2, consistent with its security incident response procedures, the company: 1) retained the cybersecurity group at the law firm of King & Spalding LLP to guide the investigation and provide legal and regulatory advice; 2) reached out, though company counsel, to engage the independent cybersecurity forensic consulting firm, Mandiant, to investigate the suspicious activity; and 3) contacted the Federal Bureau of Investigation ("FBI").

Over the next several weeks, working literally around the clock, Mandiant and Equifax's security department analyzed forensic data seeking to identify and understand unauthorized activity on the network. Their task was to figure out what happened, what parts of the Equifax network were affected, how many consumers were affected, and what types of information was accessed or potentially acquired by the hackers. This effort included identifying and analyzing available forensic data to assess the attacker activity, determining the scope of the intrusion, and assessing whether the intrusion was ongoing (it was not; it had stopped on July 30 when the portal was taken offline). Mandiant also helped examine whether the data accessed contained personal identifying information; discover what data was exfiltrated from the company; and trace that data back to unique consumer information.

By August 11, the forensic investigation had determined that, in addition to dispute documents from the online web portal, the hackers may have accessed a database table containing a large amount of consumers' PII, and potentially other data tables.

On August 15, I was informed that it appeared likely that consumer PII had been stolen. I requested a detailed briefing to determine how the company should proceed.

On August 17, I held a senior leadership team meeting to receive the detailed briefing on the investigation. At that point, the forensic investigation had determined that there were large volumes of consumer data that had been compromised. Learning this information was deeply concerning to me, although the team needed to continue their analysis to understand the scope and specific consumers potentially affected. The company had expert forensic and legal advice, and was mindful of the FBI's need to conduct its criminal investigation.

A substantial complication was that the information stolen from Equifax had been stored in various data tables, so tracing the records back to individual consumers, given the volume of records involved, was extremely time consuming and difficult. To facilitate the forensic effort, I approved the use by the investigative team of additional computer resources that significantly reduced the time to analyze the data.

On August 22, I notified Equifax's lead member of the Board of Directors, Mark Feidler, of the data breach, as well as my direct reports who headed up our various business units. In special telephonic board meetings on August 24 and 25, the full Board of Directors was informed. We also began developing the remediation we would need to assist affected consumers, even as the investigation continued apace. From this point forward, I was updated on a daily – and sometimes hourly – basis on both the investigative progress and the notification and remediation development.

On September 1, I convened a Board meeting where we discussed the scale of the breach and what we had learned so far, noting that the company was continuing to investigate. We also discussed our efforts to develop a notification and remediation program that would help consumers deal with the potential results of the incident. A mounting concern also was that when any notification is made, the experts informed us that we had to prepare our network for exponentially more attacks after the notification, because a notification would provoke "copycat" attempts and other criminal activity.

By September 4, the investigative team had created a list of approximately 143 million consumers whose personal information we believed had been stolen, and we continued our planning for a public announcement of a breach of that magnitude, which included a rollout of a comprehensive support package for consumers. The team continued its work on a dedicated website, www.equifaxsecurity2017.com, where consumers could learn whether they were impacted and find out more information, a dedicated call center to assist consumers with questions, and a free credit file monitoring and identity theft protection package for all U.S. consumers, regardless of whether they were impacted.

I understand that Equifax kept the FBI informed of the progress and significant developments in our investigation, and felt it was important to notify the FBI before moving forward with any public announcement. We notified the FBI in advance of the impending notification.

On September 7, 2017, Equifax publicly announced the breach through a nationwide press release. The release indicated that the breach impacted personal information relating to 143 million U.S. consumers, primarily including names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.

These are the key facts as I understand them. I also understand that the FBI's investigation and Equifax's own review and remediation are ongoing, as are, of course, numerous other investigations.

Protecting U.S. Consumers Affected by the Breach

From the third week in August, when it became clear that our worst fears had come true and Equifax had experienced a significant breach, my direction was to continue investigating but first and foremost to develop remediation to protect consumers from being harmed and comply with all applicable notification requirements, based on advice of outside cybersecurity counsel and Mandiant. Significantly, a major task was the need to deploy additional security measures across the entire network because we were advised that as soon as Equifax announced the hack, there would be a dramatic increase in attempted hacking. There were three main components to Equifax's plan: 1) a website where consumers could look up if they were affected by the breach and then register for a suite of protective tools; 2) a call center to answer questions and assist with registration; 3) the package of tools themselves that the company was offering to everyone in the country. The task was massive – Equifax was preparing to explain and offer services to every American consumer.

First, a new website was developed to provide consumers with additional information – beyond the press release – about the nature, extent, and causes of the breach. This was extremely challenging given that the company needed to build a new capability to interface with tens of millions of consumers, and to do so in less than two weeks. That challenge proved overwhelming, and, regrettably, mistakes were made. For example, terms and conditions attached to the free solutions that Equifax offered included a mandatory arbitration clause. That provision – which was never intended to apply in the first place – was immediately removed as

soon as it was discovered. (I was informed later that it had simply been inadvertently included in terms and conditions that were essentially "cut and pasted" from a different Equifax offering.)

The initial rollout of Equifax's call centers had frustrating shortcomings as well. Put simply, the call centers were confronted by an overwhelming volume of callers. Before the breach, Equifax had approximately 500 customer service representatives dedicated to consumers, so the company needed to hire and train thousands more, again in less than two weeks. To make matters worse, two of the larger call centers in Florida were forced to close for a period of time in the wake of Hurricane Irma. The closure of these call centers led to a reduction in the number of available customer service representatives and added to the already significant wait times that callers experienced. Many needlessly waited on hold or were otherwise unable to have their questions answered through the call centers, which I deeply regret. My understanding is that the call centers are now fully functional. The number of customer service representatives, which is now over 2,500, continues to increase, and I am informed that wait times have decreased substantially.

Beyond the website and the call centers, the company also developed a comprehensive support package for all American consumers, regardless of whether they were directly affected by the incident or not, that includes free: 1) credit file monitoring by all three credit bureaus; 2) Equifax credit lock; 3) Equifax credit reports; 4) identity theft insurance; and 5) Social Security Number "dark web" scanning for one year. Importantly, enrolling in the program is free, and will not require consumers to waive any rights to take legal action for claims related to the free services offered in response to the cybersecurity incident or for claims related to the cybersecurity incident itself.

Despite these challenges, it appears that Equifax's efforts are reaching many people. As of late September, the website had received over 420 million hits. And similarly, as of late September, over 7.5 million activation emails have been sent to consumers who registered for the program.

Equifax also recently announced a new service that I understand will be available by January 31, 2018, that will allow consumers to control their own credit data, by allowing them to lock and unlock their credit files at will, repeatedly, for free, for life. I was pleased to see the company move forward with this plan, which we had put in motion months ago, and which I directed the company to accelerate, as we were constructing the remedial package in response to the breach.

The hard work of regaining the trust of the American people that was developed over the course of the company's 118 year history is ongoing and must be sustained. I believe the company, under the leadership of Lead Director Mark Feidler, and interim CEO Paulino do Rego Barros, Jr. will continue these efforts with vigor and commitment.

How to Protect Consumer Data Going Forward

It is extremely important that notwithstanding the constant threat of cybercriminals, the American people and the Members of this Subcommittee know that Equifax is doing everything

in its power to prevent a breach like this from ever happening again. Since the potential breach was discovered, those inside and outside the company have worked around-the-clock to enhance the Company's security measures. While I am limited in what I can say publicly about these specific measures, and going forward these questions are best directed to new management, I want to highlight a few steps that Equifax has already taken to better protect consumer data moving forward, including the website developed to respond to the hack, and some changes still to come.

In recent weeks, vulnerability scanning and patch management processes and procedures were enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies on application and web servers has been accelerated. The company is also implementing additional network, application, database, and system-level logging. These are just a few of the steps Equifax has taken in recent weeks to shore up its security protocols.

Importantly, Equifax's forensic consultants have recommended a series of improvements that are being installed over the next 30, 60, and 90 day periods, which the company was in the process of implementing at the time of my retirement. In addition, at my direction a well-known, independent expert consulting firm (in addition to and different from Mandiant) has been retained to perform a top-to-bottom assessment of the company's information security systems.

Beyond the recent technological enhancements, Equifax has also made several strategic personnel changes at the highest levels of the company. Accountability starts at the top and I, therefore, decided to step down as CEO and retire early to allow the company to move forward. Before I retired, our Chief Information Officer and Chief Security Officer also left the company. Equifax's interim appointments for each of these positions, including Paulino do Rego Barros, Jr., the interim CEO, are ready, able and qualified to step into their new roles and to help consumers, and the company, recover from this regrettable incident.

It is my hope and expectation that, at the conclusion of the investigation, we will have an even more complete account of what happened, how future attacks by criminal hackers can be deterred and suspicious activity curbed more quickly, and most importantly, how consumers' concerns about the security of their personal data can be alleviated.

Toward a New Paradigm in Data Security

Where do we go from here? Although I have had little time for reflection regarding the awful events of the last few weeks, this humbling experience has crystalized for me two observations: First, an industry standard placing control of access to consumers' credit data in the hands of the consumers should be adopted. Equifax's free lifetime lock program will allow consumers, and consumers alone, to decide when their credit information may be accessed. This should become the industry standard. Second, we should consider the creation of a public-

private partnership to begin a dialogue on replacing the Social Security Number as the touchstone for identity verification in this country. It is time to have identity verification procedures that match the technological age in which we live.

The list of companies and government agencies that have suffered major hacks at the hands of sophisticated cybercriminals is sadly very long, and growing. To my profound disappointment, Equifax now finds itself on that list. I have stepped away from a company I have led and loved and help build for more than a decade. But I am not stepping away from this problem and I am strongly committed to helping address the important questions this episode has raised. Part of that starts today, as I appear at this hearing and others voluntarily to share what I know. Going forward, however, government and the private sector need to grapple with an environment where data breaches will occur. Giving consumers more control of their data is a start, but is not a full solution in a world where the threats are always evolving. I am hopeful there will be careful consideration of this changing landscape by both policymakers and the credit reporting industry.

Conclusion

Chairman Latta, Ranking Member Schakowsky, and Honorable Members of the Subcommittee, thank you again for inviting me to speak with you today. I will close by saying again how so sorry I am that this data breach occurred. On a personal note, I want to thank the many hard-working and dedicated people who worked with me for the last 12 years, and especially over the last eight weeks, as we struggled to understand what had gone wrong and to make it right. This has been a devastating experience for the men and women of Equifax. But I know that under the leadership of Paulino and Mark they will work tirelessly, as we have in the past two months, to making things right.

I realize that what I can report today will not answer all of your questions and concerns, but I can assure you and the American public that I will do my level best to assist you in getting the information you need to understand this incident and to protect American consumers.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu