Written Testimony of Mark Begor
Chief Executive Officer of Equifax Inc.
U.S. Senate Committee on Homeland Security & Government Affairs
Permanent Subcommittee on Investigations
March 7, 2019

Chairman Portman, Ranking Member Carper and distinguished members of the Subcommittee, thank you for the opportunity to be here today. I am Mark Begor, Chief Executive Officer of Equifax, a role that I accepted in April 2018 after 37 years in senior leadership roles at General Electric and Warburg Pincus. With me today is Jamil Farshchi, who joined Equifax in February 2018 as our Chief Information Security Officer (CISO), reporting directly to me. Mr. Farshchi is a seasoned security expert and brings significant and relevant information security experience to Equifax, having previously served in senior information security roles at The Home Depot, Time Warner Inc., Visa, Los Alamos National Laboratory and NASA.

While I was not a part of the Equifax team when the cybersecurity incident occurred in 2017, I certainly recognize the disruption and impact that the cyberattack caused for U.S. consumers and our customers — and I deeply regret what happened. I also understand that our regulators and lawmakers undoubtedly felt, and continue to feel, a strong duty to ensure that the financial ecosystem is functioning in a way that benefits consumers and safeguards their personal data.

Cybercrime—targeting individuals, our nation's businesses and our government—is one of the greatest threats facing our country today. U.S. corporations are continually attempting to combat criminals that operate outside the rule of law and attempt to extract data for their own gain. In 2018 alone, it is reported that over 1,200 data breaches occurred at U.S. companies. These attacks are no longer just a hacker in the basement attempting to penetrate a company's security perimeter but instead are carried out by increasingly sophisticated criminal rings or, even more challenging, well-funded nation-state actors or military arms of nation-states. These attacks on U.S. businesses are attacks on U.S. consumers and attacks on America. Fighting these attackers will require partnership and cooperation among government, law enforcement and private business. Since discovering the breach in 2017, we have been committed to transparency and open best-practice sharing with our competitors, with our customers, with the U.S. Government and across U.S. industry. This war is getting more challenging and more sophisticated and will not end.

We have cooperated with the Subcommittee and appreciate the significant time and resources it has spent in conducting its investigation. At your request, Equifax has undertaken an extensive production of documents, responded to dozens of interrogatories, and produced and coordinated both internal and external experts to brief your staff. It has been our intent to be transparent with you and with the public about the circumstances surrounding our breach.

As we have previously shared with the Subcommittee, the cybersecurity incident announced on September 7, 2017 occurred because criminals exploited a vulnerability on Equifax's online

consumer dispute portal to steal information. Our forensic review estimated that the criminals stole certain personally identifiable information of approximately 148 million consumers. Although the data stolen was sensitive, including names, social security numbers and dates of birth, there is no evidence that the perpetrators accessed the financial credit report information of any consumer. Of note, to date, we have not identified any evidence indicating that the information stolen from Equifax in 2017 has been sold or any evidence of increased identity theft. We continue to monitor the dark web and other sources for evidence of the stolen data being used in a criminal fashion.

While I was not with Equifax when the cyberattack occurred or when it was announced, I understand that both technology failures and human errors contributed to the breach. However, the fact that Equifax did not have an impenetrable information security program and suffered a breach does not mean that the Company failed to take cybersecurity seriously. Before the cyberattack, I understand that the Company's security program was well-funded and staffed, based on a robust set of policies, standards, and procedures, and supported by general and specialized training. The program also leveraged strong administrative and technical safeguards overseen by a CSO and was subject to regular, ongoing review through external and internal assessments.

In April 2018 when I joined Equifax, I made a personal commitment internally and externally to build a culture within Equifax where security is a part of our DNA and committed that Equifax would be an industry leader in data security. I am proud of the leadership, cultural enhancements and investments that Equifax has made over the past 18 months and our progress toward being an industry leader in data security.

In those 18 months, we've had a meaningful refreshment of our Board of Directors, with four new directors (including me) joining the Board. The Board is regularly updated by our CISO about cybersecurity matters and our security transformation progress. Equifax has a mindset that everyone at the Company must have an understanding of and appreciation for the role they play in keeping our environment secure — and the Board is no exception. In fact, our CISO has developed a Board Cyber Audit Framework that consists of a set of programmatic and operational metrics so that directors can better understand where the company stands with respect to cybersecurity and so that any issues that arise are treated with the proper urgency. Equifax intends eventually to share this framework with other companies as a tool to leverage with their own boards to increase awareness about important cyber topics that boards and management teams regularly face.

Last year, we made senior-level appointments on my leadership team to help round out our strong security, data governance, IT and risk management teams. As already noted, I joined Equifax in April of last year. I have a deep understanding of the financial system and the importance of credit reporting agencies to that system, having served as CEO of GE's retail credit card business as well as a Director of FICO. In addition to hiring Mr. Farshchi as CISO, we also appointed Bryson Koehler, the former Chief Technology Officer at IBM Watson and Cloud Platform, as our new Chief Technology Officer. We have made other significant additions to

our team, including Nick Oldham as Chief Privacy and Data Governance Officer and Kent Lindner to lead our Enterprise Risk and Compliance functions.

These leadership changes are helping drive accountability from the top down as we work to strengthen our holistic culture of security. But to truly transform into an industry leader, we must embed security into everything we do — from product development, to our merger and acquisition strategies, to our incentive compensation plans. To that end, in 2018, we implemented a company-wide security goal in our annual bonus for the 3,900 bonus eligible employees across the company. This sort of 'shared-fate' mindset reinforces accountability and properly incentivizes our workforce — regardless of role or department — so that security is viewed as a responsibility not only of the security team, but also of the entire company.

Another component of our culture change includes a concerted effort to attract and cultivate the best and brightest cybersecurity talent because, ultimately, our success or failure hinges on our people. In 2018, we added nearly 1,000 full-time IT and security professionals to our workforce. We sought highly-specialized, technical talent that will help Equifax develop a world-class security organization.

We recognize that part of being an industry leader in data security is being transparent about our learnings over the past 18 months and actively sharing the best practices that we are collecting as we implement change. Nearly every day we read about new data breaches in the media, impacting a wide-range of industries and companies. All security practitioners stand to benefit from information sharing and open dialogue. Therefore, in 2018 we established a number of meaningful cyber forums and partnerships that ultimately will raise the bar for the entire security community. We founded ATLAS, a public-private sector initiative aimed at sharing threat intelligence and thought leadership, and we were invited to join the World Economic Forum's Centre for Cybersecurity. We also joined the Better Identity Coalition and are taking a leadership role in policy discussions to reduce reliance on the Social Security number and to support a secure digital identity. We plan to continue this level of investment and initiative in 2019 and beyond.

The last part of our plan to implement meaningful change in our organization includes the technical improvements we are making to strengthen the maturity of Equifax's security program. We are dramatically increasing our security and technology spending by an incremental $1.25 billion between 2018 -2020 and will spend approximately $1 billion per year during this timeframe to transform our technology and security into industry-leading capabilities.

In 2018, we enhanced our core information security competencies, matured the program to address current and future environmental changes, and began to regain consumer and customer trust. Among our most important achievements were the following:

- Implemented a 24 x 7 x 365 follow-the-sun Security Operations Center, enabling Equifax to better respond to cyber incidents in real time and in many cases with local resources.

- Established a data discovery program and deleted unnecessary data and records, reducing the footprint of high-risk systems.
- Reinstated the majority of compliance certifications that were suspended as a result of the cybersecurity incident.
- Deployed updated identity and access management controls with enhanced security being applied to thousands of privileged, administrative and service accounts and restricted administrative privileges on hundreds of endpoints.
- Completed penetration testing of hundreds of externally-facing applications – those with the highest propensity for being attacked.
- Increased code security scanning, with each code scan representing an opportunity for developers to identify and remediate security flaws prior to moving their code into production.
- Created technical assurance measures to validate control effectiveness.

We will continue our record levels of investment in our security and technology in 2019 and 2020. Heading into 2019, our technical project portfolio looks to further increase maturity by executing against key security considerations such as controls assurance, acquisition integration and cloud services. We will continue to be transparent about our lessons learned.

In addition to setting a goal of being an industry leader in data security, Equifax has been working diligently to support U.S. consumers. When Equifax announced the cyberattack, Equifax's response was guided by a desire to do everything it could—going well beyond the requirements of data breach notification laws and doing more than other companies facing major breaches had done—to help consumers. While the rollout of these services was not flawless, Equifax worked diligently and invested substantial resources to mitigate any impact on consumers. Since the 2017 incident, Equifax has spent more than $80 million on supporting consumers.

At the time the incident was announced, Equifax rolled out a suite of services to assist consumers, including a call center staffed 18 hours a day, seven days a week and a dedicated, consumer-facing website. We offered all American consumers—regardless of whether they were affected by the incident—the opportunity to enroll for one year, for free, in our TrustedID Premier service, an identity theft protection and credit file monitoring service. TrustedID Premier included three bureau credit file monitoring, identity theft insurance, internet scanning for Social Security numbers, the ability to lock and unlock Equifax credit reports and copies of Equifax credit reports. In November 2018 when that service was nearing its conclusion, Equifax voluntarily decided to extend the protection for another year.

Equifax also has taken an industry-leading role to give consumers more control over personal credit data. In January 2018, Equifax launched the Lock & Alert™ service to allow consumers to quickly lock and unlock their Equifax credit reports for free, for life, using a simple mobile application that we developed. Additionally, following the 2017 incident, Equifax provided U.S. consumers the ability to freeze and unfreeze their Equifax credit files for free, and, in

September 2018, we successfully implemented the national security freeze requirements included in S.2155, the "Economic Growth, Regulatory Relief, and Consumer Protection Act."

At the same time, Equifax took an extra step and unveiled a new online consumer enrollment center called myEquifax™ to make it easier and more convenient for consumers to manage their credit information online. To date, more than 600,000 consumers have taken advantage of myEquifax to more easily manage their security freezes or fraud alerts. Our roadmap for myEquifax includes significant additional investments to help consumers process and manage disputes on their credit reports, including sending proactive alerts to consumers on the progress of their disputes. This new service will help give consumers transparency and peace of mind that their disputes are being handled promptly and with urgency. We are investing an additional $50 million in 2019 and 2020 to enhance our consumer facing capabilities and will continue our focus on ensuring that we are consumer friendly at every touchpoint.

To close, I would like to assure the Subcommittee that Equifax is committed to working collaboratively with Congress as we continue to find ways to combat cyber crime. I have been clear since I joined Equifax last April that we are committed to becoming an industry leader in security and to becoming more consumer-friendly. We are investing unprecedented amounts in technology and security, as well as enhancing our processes to make it easier for consumers to manage their credit reports. And, as you have heard, we are bringing the best resources and people to Equifax. Every U.S. company, consumer and government agency is facing a relentless attack by cyber criminals. This is a war that will not end. Continued investment in industry-leading data protection technologies and open collaboration to share best practices are our only defenses.

While we still have more work to do, please know that we remain open to sharing best practices with our peers and partners and to making sure that the millions of consumers who need credit to power their financial dreams are treated fairly and with respect and that they have a consistently positive experience with Equifax.

Thank you again for the opportunity to provide this testimony, for your dedication to your constituents and for your focus on protecting American businesses and consumers from cyber attacks.