Prepared Testimony of Tyler Moore
before the U.S. Senate Committee of the Judiciary
Subcommittee on Privacy, Technology and the Law

October 4, 2017

Good afternoon. Chairman Flake, Ranking Member Franken, members of the committee: Thank you for the opportunity to speak with you today on this matter. I am the Tandy Assistant Professor of Cyber Security at The University of Tulsa. I have studied cybersecurity for nearly two decades, and my current research focuses on measuring cybercriminal activity and studying the economic incentives that affect cybersecurity decisions and outcomes.

The recent breach of 145.5 million American consumers' personal information is deeply troubling. It stands out even among prior high-profile breaches not only for the number of Americans affected, but also for the data disclosed: Social Security numbers, addresses and credit histories.

I teach my students that a loss of confidentiality is so damaging because it is irreversible. There is no available countermeasure to make a cybercriminal "unsee" the stolen data. Consumers' information has been compromised, now and forever. And unlike prior breaches where financial information such as credit card numbers have been compromised, it is simply not practical for 145.5 million Americans to be reissued new Social Security numbers, let alone change the home address for their mortgages.

In my brief remarks today, I will describe some of the opportunities for misuse of the breached data by malevolent actors. Then I will discuss who is impacted by the breach and what market failures are at play. Finally, I will conclude by outlining some policy options going forward.

The most straightforward potential harm emanating from this breach is new credit account fraud; cybercriminals could profit by taking out new credit cards, mortgages, etc. New account fraud is pernicious because people often don't find out that they were victimized until they are denied credit due to a lowered credit score from the fraudulently opened accounts. This is only the tip of the iceberg. Social Security numbers and addresses also can be misused by filing fraudulent tax returns en masse. In recent years, the IRS has lost billions of dollars to criminals filing for fake tax refunds using only Social Security numbers and addresses. Expect attempted tax filing fraud to spike in the coming years. As a consequence of this latest data breach, healthcare and entitlement fraud also are susceptible to rise.

The potential for harm goes beyond frauds perpetrated by profit-motivated cybercriminals. Because the breached data includes current physical addresses, victims of stalking and harassment could be tracked down by assailants who previously were unable to identify their targets' whereabouts. Lastly, there is a national security threat if the stolen data were obtained by hostile foreign governments. For instance, by connecting the breached data with the prior breach at the Office of Personnel Management, foreign powers could identify federal workers who may have financial problems uncovered by their credit reports, identify private residences, or more easily impersonate workers with security clearances.

Taking a step back from the myriad potential harms, it is useful to make some observations. First, many of the harms discussed affect people and organizations beyond Equifax. This includes not only the individuals whose data was compromised. It also includes other financial institutions and healthcare organizations that may experience increased fraud. It includes the U.S. government, whose national security may be weakened and whose tax fraud bill may be higher. These are examples of a market failure called a negative externality. When third parties are harmed by the security decisions taken by others, the incentive to invest in countermeasures is weakened. This, in turn, can lead to mismanagement of risk by organizations that are responsible for protecting data confidentiality.

Second, another lurking market failure is the information asymmetry that exists about the true extent and cost of harms. At this point, we know that Social Security numbers and credit reports have been breached. But we don't know how much new fraud has occurred or will be enabled, how many consumer's credit scores will be wrongly downgraded as a result of fraud, how much harassment takes place or how many national security secrets will be compromised. Without an accurate assessment of these costs and who is affected, it is difficult to devise a rational response that encourages more secure outcomes.

Third, we should be mindful of the indirect costs associated with this breach. If people reduce their online participation or their engagement with the financial system because of an erosion of trust, for example, the total drag on the economy could far exceed the direct costs from the harms just presented. In prior research measuring the costs of cybercrime, my colleagues and I found that cybercrimes often resemble copper thefts. Just as the sums spent to repair streetlights whose copper wiring has been stripped and resold often far exceeds the criminals' profits, so do the indirect costs associated with cybercrime dwarf the direct costs.

So, what should we do? Thus far, the main defense available to consumers is to freeze their credit. This is a good start, but it falls short in that most of the harms outlined above would not be stopped by placing a credit freeze.

In the near term, steps should be taken (1) to increase consumers' control over how their data is used and (2) to promote transparency about realized harms. In terms of controlling access to credit reports, we need a comprehensive approach that changes from today's practice of allowing access by default to the more secure approach of denying access by default. In a world where bad actors already know most everyone's name, Social Security number and address, we cannot continue with a system where authentication is based solely on information that has been compromised.

To make a "default deny" system workable, private industry should be challenged to innovate by creating ways to make the process of "unfreezing" as frictionless as possible. Eliminating or reducing fees for credit locks and unlocks is a start. Organizations who profit from collecting personal financial data should not be rewarded financially for failing to protect that data.

The current system of security freezes, while workable for motivated consumers with the financial means to pay, needs to be simplified if it is going to be adopted by everyone. The lightest touch policy intervention is to require that credit be frozen by default, thereby

incentivizing credit bureaus and data brokers to design more secure and usable authentication procedures.

By promoting transparency about the true prevalence and cost of realized harms, we could correct the information asymmetry described above. Companies should be required to disclose breaches of confidentiality as well as the occurrence of fraud, complaints about unauthorized access and how other parties are affected. By gathering this information, firms would gain greater insight into the true costs of cyber insecurity, thereby encouraging more investment when necessary. And policy makers would get a better sense of the true magnitude of the negative externalities at play, which could inform subsequent policy interventions.

Over the longer term, we must move to a more secure way of authenticating people than Social Security numbers and what credit bureaus offer today. Now that all this data has been disclosed, there is no going back. Again, we should look to the private sector to take the lead in innovating new technologies. But there remains a significant coordinating role for government. The National Strategy for Trusted Identities in Cyberspace was a good start, and NIST's Trusted Identities Group continues the push today for the private sector to develop stronger identification and authentication mechanisms. More effort should be devoted to developing robust procedures that respect privacy and can be used by all Americans.

Finally, we must also work to improve resilience to cyberattacks. Perfect security is not possible, but we can take steps to limit the damage attacks cause and to recover more quickly and completely from them. A system that relies on static, unchangeable information like Social Security numbers for authentication is inherently fragile. When breaches do occur, the affected organization should respond in a way that gives affected consumers transparent access to reliable information on how they are impacted and clearly lay out meaningful actions that can be taken to mitigate risks. A robust response can help prevent a damaging loss of consumer confidence.