

**Prepared Statement by Senator Chuck Grassley of Iowa
Chairman, Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law, Hearing on
Hearing on Equifax: Continuing to Monitor Data-Broker Cybersecurity
October 4, 2017**

Thank you Chairman Flake for holding this timely and important hearing. I know this isn't an unfamiliar subject to you. In fact, last Congress you held a hearing in this subcommittee examining the data broker industry's security standards for protecting personal information. I appreciate your hard work and the bipartisan approach that you and Senator Franken have taken in examining this important issue.

Today's hearing continues this committee's long-standing history involving data breach and data security. We've held hearings to examine past data breaches and spent years working on legislation to establish a uniform, national data security and breach notification standard. While our progress in Congress has been slow, criminal hackers continue to find ways to break into even the most secure systems.

Unfortunately, data breaches and cyber-attacks are going to happen. It's a matter of when, not if. Most Iowans I hear from recognize this fact. But recognizing reality doesn't mean we must accept it and give up. We all must work to prevent future attacks and limit the harm from those that do occur.

Additionally, we must appreciate the fact that not all data breaches are the same. The information and risk of harm can greatly vary from one breach to another. For example, the past breaches at Target and Neiman Marcus, which this committee held a hearing to examine, involved financial information such as credit and debit cards. Of course this is information that absolutely must be protected and secured. If it falls in the wrong hands it can create a lot of problems for individuals. But the Equifax data breach is different. And it's important that consumers and policymakers recognize this distinction, because the threat landscape has changed.

The information hackers obtained or gained access to in the Equifax breach is the most sensitive personal information used by thieves to commit identity theft. Let that sink in. A credit card number or bank account information can be changed with a phone call. But you can't change your social security number and date of birth. Anyone who's ever applied for a loan, a credit card, a job, or opened a bank account knows you have to provide a social security number and date of birth to verify your identity. Thus, if someone has this information they can do the same and take over your identity. They can become you. And you won't know it happened until it's too late.

Granted, it may be months or even years before a consumer suffers identity theft – if at all – as a result of the Equifax breach. Yet no one will be able to prove their identity was stolen due to this particular breach. We live in a world of data breaches, so good luck locating your identity thief's

source. The status quo has changed with respect to protecting individuals from identity theft. Most Americans are clearly now at risk of real harm and not mere nuisance.

What can and should we do? It's long past time for a uniform national data security and breach notification standard. I've been working with Senator Feinstein and a bipartisan group of Senators on this issue for years. I remain committed to getting a good bill put together and over the finish line. But that's just one step.

This breach should be a wakeup call to the new identity theft threat landscape we now face. All of us—policymakers, businesses, and consumers, must start thinking differently than we have in the past.

We need to look at ways of empowering consumers to limit or prevent identity theft from occurring in the first place. One tool that's been found to be effective is a credit freeze. But credit freezes are costly and can be difficult for consumers to control. In the age of smartphones and other devices, where consumers can turn things on and off with the tap of a button, this shouldn't be the case. I look forward to learning more about the tools available to help consumers, and the security threats faced by industry and consumers in light of this breach.

Mr. Chairman, thank you again for holding this hearing. I encourage us all to figure out ways to work together to strengthen the ability of consumers to protect and control access to their credit information and identity.