Statement of Ranking Member Grassley of Iowa
Senate Committee on the Judiciary Hearing,
"Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime"
Tuesday, February 4, 2014.

Mr. Chairman, thank you for holding today's hearing to examine the well-publicized recent commercial data breaches. We're still learning all the details, but it's clear these and other breaches have potentially impacted millions of consumers nationwide.

Today we have the opportunity to learn about the challenges that both industry and law enforcement face in combatting cyber-attacks from well organized criminals. The witnesses have a unique ability to provide us various important perspectives as we consider the government's role in securing sensitive data and crafting a breach notification standard.

I hope to learn where the Committee's expertise could be helpful in combatting future attacks. Furthermore, I'd like to use this hearing to explore areas of common ground, so we can determine what might be accomplished quickly.

In most cases, thankfully, businesses are able to prevent the relentless attacks against their networks. This is due to comprehensive security programs coupled with law enforcement's diligent work. However, the data breaches at Target and Neiman Marcus demonstrate that even companies with vast resources can suffer serious attacks with the potential to harm their customers.

One defensive tool that's been discussed is updating payment card technology. Retailers and card issuers are preparing to transition away from decades-old technology. This is a positive step in the right direction. However, it's a bit troubling that it's taken so long to implement this technology. Many fraudulent transactions might have been prevented had this occurred already. But this alone won't provide complete security, as I'm sure we'll hear today.

Criminal hackers aren't quitters. They continue to find ways to break into company networks. As the Federal Bureau of Investigation has warned, attacks like those recently suffered will continue. So companies must be vigilant in defending their systems, as well as in taking steps after an attack to warn customers and limit the damage.

Unfortunately, it may be days, weeks, or months before a business realizes it's been attacked. And if a hacker can breach a large business's security system, then it's obvious that smaller businesses are threatened as well. It's important we remain mindful of the differences in businesses and the resources they have available as we go forward.

It's been a couple of years since the committee last considered data security legislation. In that time, we've learned a lot about this subject thanks to the broader cybersecurity conversation. The proposals offered by the Administration and Congress, along with other government initiatives, can be helpful for us as we consider how to proceed on legislation.

Currently, there are at least four pieces of data security and breach notification legislation in the Senate, with possibly more to come as other committees begin their work. While these bills would establish national security standards, they take different approaches. This offers us the chance to examine the effects of each, which is a good thing.

In the past, I've expressed concern with approaches that don't provide businesses the flexibility they need to secure their data. We must avoid creating a one-size-fits-all security requirement, particularly if it fails to account for businesses of different sizes and resources. An inflexible approach could lead to businesses focusing on merely completing a checklist of requirements in order to avoid liability, instead of doing what makes sense to secure customer information in their particular circumstances.

On this point, I hope to learn how the government can better partner with the private sector and law enforcement to strengthen data security. The government has a strong interest to work together with industry, given the impact cyber-attacks have on the Nation's economy.

Fostering a greater public-private approach to cybersecurity was recognized in last year's Executive Order from the President on Improving Critical Infrastructure Cybersecurity. The Executive Order stated that strengthening cybersecurity can be achieved through government partnership with private business.

As a result of the Executive Order, we should review the National Institute of Standards and Technology ongoing partnership with owners of critical infrastructure. This partnership will create standards, guidelines, and best practices for businesses to implement on a voluntary basis.

There's already bipartisan support for this approach. Senators Rockefeller and Thune have introduced a bill to enshrine the National Institute of Standards and Technology role in creating a cybersecurity framework. This is just one model for government action focused on securing critical infrastructure. It's worth considering how this approach might work in this particular context.

The recent breaches also draw attention to the need for a uniform, federal notification standard. There's been little suggestion that the public failed to receive news about these recent breaches. However, we once again see the difficulties faced with a patchwork of state laws. Companies must ensure compliance, while also investigating ongoing threats.

I've supported creating a federal notification standard to replace the laws in 46 states and the District of Columbia. It makes sense. If done correctly, it would ease compliance costs for businesses, particularly since the current laws are ever changing. A federal standard would also ensure consumers are notified of breaches that could result in financial harm or identity theft.

But if the standard for notification is crafted too broadly or the penalties for failure to notify are too harsh, there's a risk for consumer over-notification. Businesses may choose to issue notice of even trivial breaches. Just as there's a potential for harm when a victim is not notified of a breach, over-notification can lead to harm or apathy.

Further, a notification law must recognize the resources available to different businesses. While companies like those before us today were quickly able to comply with existing law, many smaller businesses would face a more difficult experience.

There's widespread support for a national breach notification standard. As a result, we should ask whether it's appropriate to separate this issue from other aspects of the ongoing data security debate. This might provide the chance to take action quickly, as we continue work on other issues.

Thank you again, Mr. Chairman. I look forward to exploring these issues and working with you and others.