

**Statement of the Honorable Mary Bono Mack**  
**Subcommittee on Commerce, Manufacturing and Trade**  
**“Sony and Epsilon: Lessons for Data Security Legislation.”**

**June 2, 2011**

*(Remarks Prepared for Delivery)*

With nearly 1.5 billion credit cards now in use in the United States – and more and more Americans banking and shopping online – cyber thieves have a treasure chest of opportunities today to “get rich quick.” Why crack a vault when you can hack a network?

The Federal Trade Commission estimates that nearly nine million Americans fall victim to identity theft every year, costing consumers and businesses billions of dollars annually – and those numbers are growing steadily and alarmingly.

In recent years, sophisticated and carefully orchestrated cyber attacks – designed to obtain personal information about consumers, especially when it comes to their credit cards – have become one of the fastest growing criminal enterprises here in the United States and across the world.

Just last month, the Justice Department shut down a cyber crime ring – believed to be based in Russia – which was responsible for the online theft of up to \$100 million. The boldness of these attacks and the threat they present to unsuspecting Americans was underscored recently by massive data breaches at Epsilon and Sony.

In some ways, Sony has become ground zero in the war to protect consumers’ online information. The initial attacks on Sony’s PlayStation Network and online entertainment services – which put some 100 million customer accounts at risk – were quickly followed by still more attacks at other Sony divisions and subsidiaries.

Since then, the company – to its credit – has taken some very aggressive steps to prevent future cyber attacks, such as installing new firewalls...enhancing data protection and encryption capabilities... expanding automated software monitoring...and hiring a new Chief Information Security Officer.

These are all important new safeguards, but with millions of American consumers in harm’s way, why weren’t these safety protocols already in place?

For me, one of the most troubling issues is how long it took Sony to notify consumers...and the way in which the company did it – by posting an announcement on its blog. In effect, Sony put the burden on consumers to search for information instead of providing it to them directly. That cannot happen again.

While I remain critical of Sony’s initial handling of these data breaches – as well as its decision not to testify at our last hearing...and that goes for Epsilon as well – it’s clear that since then the company has been systematically targeted by hackers and cyber thieves who are constantly

probing Sony's security systems for weaknesses and opportunities to infiltrate its networks.

So today, let's not point fingers. Instead, let's point the way – a better, smarter way – to protect American consumers online. As I have said, you shouldn't have to cross your fingers and whisper a prayer when you type in a credit card number on your computer and hit "enter." E-commerce is a vital and growing part of our economy. We should take steps to embrace and protect it – and that starts with robust cyber security.

As Chairman of this Subcommittee, I believe the lessons learned from the Sony and Epsilon experiences can be instructive. How did these breaches occur? What steps are being taken to prevent future breaches? What's being done to mitigate the effects of these breaches? And what policies should be in place to better protect American consumers in the future?

Most importantly, consumers have a right to know when their personal information has been compromised, and companies have an overriding responsibility to promptly alert them.

These recent data breaches only reinforce my long-held belief that much more needs to be done to protect sensitive consumer information. Americans need additional safeguards to prevent identity theft, and I will soon introduce legislation designed to accomplish this goal. My legislation will be crafted around three guiding principles:

First, companies and entities that hold personal information must establish and maintain security policies to prevent the unauthorized acquisition of that data;

Second, information considered especially sensitive, such as credit card numbers, should have even more robust security safeguards;

And finally, consumers should be promptly informed when their personal information has been jeopardized.

The time has come for Congress to take decisive action. We need a uniform national standard for data security and data breach notification, and we need it now.

While I remain hopeful that law enforcement officials will quickly determine the extent of these latest cyber attacks, they serve as a reminder that all companies have a responsibility to protect personal information and to promptly notify consumers when that information has been put at risk. And we have a responsibility, as lawmakers, to make certain this happens.