## Hearings

**Feb 05 2015**

# Getting it Right on Data Breach and Notification Legislation in the 114th Congress

## Chairman Jerry Moran

"This hearing of the Consumer Protection, Product Safety, Insurance, and Data Security Subcommittee is now called to order.

"First, I want to thank my colleagues for their high level of interest in this important topic. I would also like to thank the witnesses for joining us today to provide their valuable expertise on the important and unfortunately timely topic of data security.

"The purpose of this hearing is to examine the merits of a federal data security standard and the need for a preemptive and uniform federal data breach notification.

"We live in a digital world, where consumers have embraced online products and services. Kansans know that they can make purchases, determine their credit score, conduct banking, and examine health care plans all from their mobile phone, computer, or tablet. That is true of consumers across the country and increasingly around the world. But this digital economy creates new risks. In a world where one bad actor can battle against a team of highly-trained experts, we face challenges to make certain consumers are protected and businesses have the tools and incentives to protect their customers from harm.

"For over a decade, Congress – and the Commerce Committee in particular – has been contemplating issues surrounding data security and data breach notification. In 2004, the Committee held its first Congressional hearings to examine the high-profile breach of ChoicePoint, a data aggregation firm. This breach forced the first of many conversations here in Congress. And today we continue that conversation.

"Recent high-profile data breaches as well as the headline-grabbing Sony cyberattack from late

last year are the latest examples that highlight the ongoing and serious cyber threats that Americans and businesses face. And just this morning, we woke up to news of what experts are calling the largest health care breach to date. This time cyber criminals were able to infiltrate the nation's second largest health insurer, Anthem, to steal names, birthdays, medical IDs, Social Security numbers, street addresses, e-mail addresses and employment information, including income data.

"These high-profile breaches are the most severe of what has become a common occurrence in our digital society. As of 2015, the Privacy Rights Clearinghouse has estimated that over 4,400 breaches involving more than 932 million records have been made public since 2005. The Verizon 2014 Data Breach Investigations Report reviewed more than 63,000 security incidents and found 1,367 confirmed data breaches in 2013. On average, that's just shy of four data breaches every day.

"While Congress has developed sector-specific data security requirements for both financial institutions and companies that handle particular types of health information, Congress has been unable to reach a consensus on the development of national data security and data breach notification standards. As a result, states have taken on this task by developing their own standards. As of today, businesses are subject to a patchwork of over 50 different state, district, and territory laws that determine how businesses must notify consumers in the event of a breach incident. In addition, 12 states have enacted laws regarding data security practices.

"The need for federal action becomes clearer each day. Last month, President Obama voiced his support for national data breach notification legislation with strong preemptive language in part because he recognizes the benefits to American consumers and businesses of a predictable, uniform data breach notice. The President's support, along with bipartisan and bicameral congressional interest, has renewed optimism among stakeholders that Congress can develop balanced and thoughtful legislation in the near term.

"Today, we will focus our attention on some of the key questions and topics in this debate, including:

• What are the benefits of a national data breach notification standard?

• Should Congress implement a basic data security standard?

• To whom should the standard apply?

• Should the federal standard preempt state standards?

• What should be the "trigger" for notification – the specific conditions that represent a potential harm to consumers?

• Should there be exemptions and safe harbors? If so, for who?

• Within what time frame should a company be required to notify consumers?

• Should Congress enact new or stronger penalties, enforcement authorities, and remedies?

• What lessons can we learn from states who have implemented their own data breach notification standards?

"I am confident that today's expert panel can share valuable insight to these important questions that can help as Congress works to strike the right balance.

"I would now like to recognize the Subcommittee's Ranking Member, Senator Blumenthal, for five minutes to deliver his opening statement."

Return to Hearing

Browse by: February 2015 GO

Filter by: -- Congress - -- Types -- GO

02/11/15 - **The Connected World: Examining the Internet of Things**

02/10/15 - **Keeping Goods Moving**

02/05/15 - **Current record**

02/04/15 - **The Impacts of Vessel Discharge Regulations on our Shipping and Fishing Industries**

02/04/15 - **Building a More Secure Cyber Future: Examining Private Sector Experience with the NIST Framework**

Home About Hearings Subcommittees Oversight & Investigations Press Room Majority Minority Contact Privacy Policy