Opening Statement of the Honorable Michael Burgess
Subcommittee on Commerce, Manufacturing, and Trade
Hearing on "What are the Elements of Sound Data Breach Legislation?"
January 27, 2015

(As Prepared for Delivery)

The purpose of today's hearing is to move one step closer to a single, federal standard on data security and breach notification.

Increasingly, our personal details—which we need to verify financial transactions—are converted into data and uploaded to networks of servers that can't be protected with a simple lock and key.

We benefit immensely from the quick access and command this system gives us—the world's merchants are at our fingertips.

And yet such a dynamic environment brings with it a dynamic and evolving set of risks. As our options multiply, so must our defensive measures.

Those defensive measures must adapt quickly. As several commentators have noted in testimony before this subcommittee, it is no longer a matter of if a breach occurs, but when.

Even so, questions remain as to whether businesses are doing enough to prevent security breaches.

This is why I believe federal legislation should include a single—but flexible—data security requirement. Now, about twelve states have already implemented such a requirement on commercial actors that are not banks or health care providers.

A single requirement across the states would give companies some confidence that their methods are sound in handling electronic data, an inherently interstate activity.

Moreover, it would put all companies on notice that if you fail to keep up with other companies and if you aren't learning from other breaches, you will be subject to federal enforcement.

Indeed, too many resources are spent trying to understand the legal obligations involved with data security and breach notification. Certainty would allow those resources to be spent on actual security measures and notifications to affected consumers.

As we discuss the necessary elements of a data breach bill, there are a few considerations I want to mention.

First, there is a limited window for us to act. Criminal data breaches have grabbed headlines for about a decade, but a consensus solution has thus far eluded federal legislators.

This Committee is calling for action, the President is calling for legislation with a national breach notification regime, and the Senate has legislation with a national standard.
But most importantly, consumers are calling for legislation—the time to act is now.

Second, this legislation is limited to this Committee's jurisdiction; the surest way to deny consumers the benefits of federal data security legislation is to visit areas beyond our jurisdiction.

Specifically, the health care and financial sectors have their own regimes. If we aim to rewrite rules for those sectors then it will be years before a bill is signed into law.

That is not to say that we will ignore those issues. But they may need to be taken up separately.

Third, our aspiration at this point is for legislation with bipartisan support and I believe that is achievable.

With this hearing, I aim to understand the policy points where stakeholder compromise is possible. We are seeking to find agreement not only between the two sides of the aisle, but also between stakeholders with divergent interests.

The sooner we understand the very most important principles, the smoother negotiations will go over the next couple months.

###