Opening Statement of The Honorable Morgan Griffith

Vice Chairman, Subcommittee on Oversight and Investigations

Hearing on "Identity Verification in a Post-Breach World"

November 30, 2017

We are here today to talk about a very important topic: identity verification in a post-breach world. This hearing is especially timely given several events that have taken place since the hearing itself was announced last week, including three newly disclosed data breaches that compromised an additional 58.7 million records, as well as two major shopping days, Black Friday and Cyber Monday. With consumers rushing to take advantage of holiday sales, both in stores and online, the questions and challenges around modern identity verification become even more pressing.

Data breaches have been an increasing problem over the last several years. In fact, it is likely that everyone in this room has had their information included in a recent breach. Between the 57 million accounts compromised in Uber's recently disclosed 2016 breach, the 145 million accounts compromised in Equifax's breach, or the 22 million accounts compromised in the OPM breach, as well as many others, I would argue that it would be difficult to find an American whose information has not been compromised.

While these breaches themselves are troubling enough, they also raise a subtle, more complicated series of questions and issues around the ways in which organizations, including government agencies, banks, healthcare organizations, and retail companies perform identity verification of their citizens and customers.

It's a well understood concept that, to quote the famous cartoon, on the Internet nobody knows you're a dog. This anonymity has many advantages, and is important to many aspects of the modern Internet. However, as the global economy has become more and more digital, and an increasing amount of commerce takes place online, it also creates significant challenges for organizations attempting to

ensure that they provide information and services only to authorized individuals. Because these interactions usually take place on opposite ends of an Internet connection, with participants rarely meeting face to face, the ability of organizations to remotely verify individuals has been a constant struggle.

As a result, for years, many organizations have relied on a type of identity verification known as "Knowledge-Based Authentication" or "KBA." We are all familiar with this process, even if we don't quite know it. For example, some online accounts ask consumers to provide answers to "security questions" such as their mother's maiden name, the make and model of their first car, or the street on which they grew up. Similarly, when consumers attempt to open new credit lines, they are often asked a series of multiple choice questions that may ask who provided a consumer a loan, and in what year. These are all examples of KBA.

The effectiveness of KBA depends on a very important assumption - that information such as birthdays, mother's maiden names, addresses, work histories, and other KBA attributes remain relatively secret. In today's post-breach world, this is a tenuous assumption. Add the wealth of personal information consumers' voluntarily share about their lives through social media and this assumption appears almost laughable.

So what do we do? If modern commerce and many other services, including government services, rely on KBA for identity verification, and that verification is no longer as secure or reliable as it was in the past, we need new strategies and new technologies to ensure that consumers are protected, and economic growth continues. And we need them quickly; with the exponential growth of connected devices and services, it is likely that we will see more data breaches more often, not less.

Luckily, we are not starting from scratch. In the public sector, the National Institute for Standards and Technology (NIST) spent the past several years developing strategies and frameworks for identity verification under their Trusted Identities Group (TIG). As part of this work, NIST's TIG has provided funding to

pilot programs looking to develop, implement, and leverage innovative new technologies that move organizations beyond KBA.

Similarly, in the private sector, many companies and organizations from a wide variety of sectors have come together to create the Fast Identities Online, or FIDO, Alliance. The FIDO Alliance provides a forum for collaboration and cooperation around the development of standards-based, interoperable technologies. These standards are freely available and already deployed in the products of companies like Google and PayPal.

Our witnesses today will not only help us understand the cumulative impact of the dozens of data breaches that have occurred in recent years, but also assess how current practices can and should be improved to protect consumers after their information has been breached.

Today's hearing is the start of what I expect will be a much longer conversation. But it's a necessary conversation to have. As our world becomes ever more connected, identity verification is a challenge that will only continue to grow.