U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

November 28, 2017

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing entitled "Identity Verification in a Post-Breach World"

I. INTRODUCTION

The Subcommittee on Oversight and Investigations will hold a hearing on Thursday, November 30, 2017, at 10:15 a.m. in 2322 Rayburn House Office Building. The hearing is entitled "Identity Verification in a Post-Breach World."

II. WITNESSES

- Troy Hunt, Information Security Author and Instructor, Pluralsight;
- Jeremy Grant, Managing Director of Technology Business Strategy, Venable, LLP; and,
- Ed Mierzwinski, Consumer Program Director, U.S. PIRG.

III. BACKGROUND

In recent years, a series of data breaches originating with companies throughout the financial, healthcare, and commercial sectors have compromised the security of personally identifiable information (PII) for hundreds of millions of individuals across the globe. Recent data from the Identify Theft Resource Center (ITRC) indicates that as of November 15, 2017, over 1,100 data breaches have occurred in the United States in 2017 alone, exposing over 171 million records.[1] The compromised data ranges from more readily available information such as full names, emails, and dates of birth, to more highly sensitive information like addresses, work histories, and driver's license numbers. This information, once stolen, can be sold through online forums and is often used to facilitate identity theft and other related crimes.

While any one of these breaches on its own creates serious policy issues, there now exists the potential for malicious actors to combine multiple stolen data sets into one, thereby enabling them to obtain more complete "packages" of identity information.[2] Given that much of modern commerce relies on a process of remote identity verification known as "knowledge-based authentication" or KBA, through which individuals prove who they are by answering series of

[1] *2017 Data Breach Stats*, IDENTITY THEFT RESOURCE CENTER, Nov. 15, 2017, http://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachStatsReport_2017.pdf.
[2] *The Big Data Breach Suffered by Equifax has Alarming Implications*, THE ECONOMIST, Sep. 16, 2017, http://www.economist.com/news/finance-and-economics/21728956-financial-industry-worries-about-who-next-big-data-breach-suffered.

questions to which only they – in theory – should know the correct responses, this ability to "package" identity information raises even more significant questions about the reliability of traditional KBA practices.

As such, the effectiveness of KBA has, in recent years, been criticized by some professionals in the financial and information security professions. They point out that, between individuals' pervasive use of social media and these massive PII breaches, enough information is readily available on almost any given individual to render the ability to answer a series of knowledge-based questions nearly meaningless as an identity verification mechanism.[3] Indeed, as more data breaches are discovered and disclosed, the weaker KBA appears.

A. Knowledge-Based Authentication

Knowledge-based authentication is a type of multifactor authentication used to verify users' credentials for logins and other transactions. In some cases, KBA is also used for password recovery when consumers are unable to access their accounts. KBA relies on the use of "secret questions" that are either pre-established by the consumer or pulled from a profile associated with the user. The former is considered static KBA and the latter dynamic KBA.[4]

Static KBA allows users to pre-select questions to which only they should know the answer. This includes questions such as "What was the name of your first pet?", "What is your mother's maiden name?", and "Who was your first college roommate?"

Dynamic KBA uses information that is, in theory, more secure and questions are randomly generated based on profiles or public records associated with the consumer. This can include credit histories, housing records, and loan applications. An example of dynamic KBA is "Which company issued your 1997 student loan?"[5] Unlike static KBA, dynamic KBA may give consumers multiple-choice options to answer the questions.

There are issues facing the security of both types of KBA. With the widespread use of social media, consumer's unique identifiers for static KBA are often available to the public. Malicious actors only need to look through Facebook for familial connections, old pictures of friends, and location information to answer many of the questions posed. In the case of dynamic KBA, the large-scale breaches of consumers' credit information, social security numbers, and work histories makes it possible for even the most private financial questions to be answered by someone other than the consumer.

---

[3] *4 Big Problems with Knowledge Based Authentication*, NUDATA SECURITY, INC., Oct. 10, 2013, https://nudatasecurity.com/blog/risk-based-authentication/4-big-problems-with-knowledge-based-authentication/.
[4] Margaret Rouse, *Knowledge-Based Authentication (KBA)*, TECHTARGET SEARCHSECURITY, Feb. 2015, http://searchsecurity.techtarget.com/definition/knowledge-based-authentication.
[5] *Knowledge Based Authentication (KBA) – Out-of-Wallet Questions*, IDOLOGY, https://www.idology.com/knowledge-based-authentication/knowledge-based-authentication-kba.

B. Public and Private Sector Efforts to Address KBA Issues

i. The National Strategy for Trusted Identities in Cyberspace and the Trusted Identities Group

In recognition of the growing issues with KBA and other associated identity verification challenges, the National Institute for Standards and Technology (NIST) was tasked with developing a framework for secure, reliable online identity verification known as the National Strategy for Trusted Identities (NSTIC). NIST released the NSTIC in April 2011, focusing on the ability to establish convenient, efficient, secure, and innovative identity verification technologies in ways that acknowledged and protected privacy concerns.[6]

After the NSTIC's release, NIST transitioned the effort, along with its statutorily-mandated "Digital Identity Guidelines, Enrollment and Identity Proofing"[7] to a group known as the "Trusted Identities Group" (TIG). The NSTIC, Digital Identity Guidelines, and other associated NIST efforts now form the primary basis for the government's efforts to leverage more secure, reliable identity verification technologies.[8] As part of these efforts, the TIG provides funding to companies and organizations seeking to develop innovative new technologies and strategies that meet the NSTIC's goals.[9]

ii. The Fast Identities Online (FIDO) Alliance

Many companies and organizations in the private sector have similarly recognized the inherent risks of KBA, and have created the Fast Identities Online (FIDO) Alliance to collectively explore, develop, and implement more secure, reliable identity verification technologies. Its membership includes large technology companies such as Amazon and Google, hardware companies such as Intel, Qualcomm, and Lenovo, as well as several banks and healthcare companies, among others.

This broad, diverse membership has enabled the FIDO Alliance to propose and develop standards that are deployable across multiple sectors, and that – most importantly – are interoperable.[10] In addition, the Alliance provides its standards for free; companies and organizations looking to leverage them may do so free of charge, and without joining the FIDO

---

[6] *National Strategy for Trusted Identities in Cyberspace*, THE WHITE HOUSE, April 2011, https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf.
[7] Paul A. Grassi & James L. Fenton. *Digital Identity Guidelines, Enrollment and Identity Proofing*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, June 2017, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf.
[8] *Trusted Identities Group – Projects*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://www.nist.gov/itl/tig/projects.
[9] *Trusted Identities Group – Pilots*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://www.nist.gov/itl/tig/pilots.
[10] *Download Specifications*, THE FIDO ALLIANCE, https://fidoalliance.org/download/.

Alliance.[11] As a result, FIDO-compatible technologies are deployed throughout many well-known platforms and companies, including PayPal, Google, Dropbox, and more.[12]

C. Conclusion

While the challenges to identity verification in a post-breach world are well-known, and while both the public and private sectors have recognized the resulting issues and begun efforts to address them, significant work remains. Witnesses at this hearing will provide an overview of the problem, including an in-depth exploration and examination of the data breaches that have created the current climate, as well as provide a discussion of current public and private sector efforts and potential next steps.

IV. ISSUES

The following issues may be examined at the hearing:

- The potential for malicious actors to combine breached data sets to create more complete profiles of individuals.
- The effectiveness of KBA in protecting consumer's private information.
- Potential alternatives to KBA in remote identity verification and best practice recommendations for companies throughout the public and private sector.

V. STAFF CONTACTS

Please contact Jessica Wilkerson or John Ohly of the Committee staff at (202) 225-2927 with any questions.

---

[11] *Id.*
[12] *FAQ's*, THE FIDO ALLIANCE, https://fidoalliance.org/faqs/.