GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

November 29, 2017

To: Subcommittee on Oversight and Investigations Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

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

On **Thursday, November 30, 2017, at 10:15 a.m. in room 2322 of the Rayburn House Office Building**, the Subcommittee on Oversight and Investigations will hold a hearing titled "Identity Verification in a Post-Breach World."

The Committee is expected to explore how companies and other recipients of consumer data will be able to verify their identities online when data breaches continue to compromise their personal data.

I. DATA BREACHES HAVE CREATED NEW CHALLENGES FOR VERIFYING IDENTITIES ONLINE

Data breaches have compromised the personal data of millions of Americans, posing significant risks to consumers, as well as challenges for companies, government, and other entities who must verify consumers' identities in providing various services. The 2017 Equifax breach, for example, exposed the personal information – including names, Social Security numbers, birth dates, addresses, and other sensitive data – of as many as 145.5 million Americans.[1] With that information compromised, and because birth dates and Social Security

[1] House Committee on Energy and Commerce, Subcommittee on Digital Commerce and Consumer Protection, *Hearing on Oversight of the Equifax Data Breach: Answers for Consumers*, 115th Cong. (Oct. 3, 2017) (Witness Statement) (docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf); Equifax, *Equifax Announces Cybersecurity Firm Has Concluded Forensic*

numbers are difficult or impossible to change, these consumers are vulnerable to identity theft, fraud, and other crimes.[2]

For instance, the Social Security number has been used not only as way to identify a specific person, but also to "authenticate" that a person is who he or she claims to be.[3] Using compromised information, such as Social Security numbers, as "authenticators" can allow unauthorized access to sensitive information. In 2015, for example, the Internal Revenue Service (IRS) announced that criminals used taxpayer Social Security numbers and other data to access as many as 100,000 tax accounts through the IRS website.[4] In October 2017, security researchers discovered that by using little more than a Social Security number and a date of birth, someone could access salary and employment information that had been collected by Equifax.[5] As data breaches continue to compromise consumers' personal data, questions remain as to how best to verify that users are who they say they are when they access services online.

II. PUBLIC AND PRIVATE EFFORTS TO SECURE IDENTITIES ONLINE

Under President Obama, the White House released the National Strategy for Trusted Identities in Cyberspace – a framework for public and private collaboration on protecting digital identities and improving online transactions. The Obama Administration also created the Trusted Identities Group at the National Institute of Standards and Technology (NIST).[6] NIST has since published technical guidelines to assist federal agencies in securing digital identities.

Investigation Of Cybersecurity Incident (Oct. 2, 2017) (press release) (investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821).

[2] Federal Trade Commission, Consumer Information Blog, *The Equifax Data Breach: What to Do* (Sept. 8, 2017) (www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do); Adam Shell, *Equifax Data Breach Could Create Lifelong Identity Theft Threat*, USA Today (Sept. 9, 2017) (www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/); Kathy Kristof, *Equifax Data Breach and Credit Freeze: Beware These 3 Scams*, CBS News (Sept. 16, 2017) (www.cbsnews.com/news/equifax-data-breach-credit-freeze-phishing-other-scams/).

[3] Jeremy Grant, *Scrapping Social Security numbers won't be enough to protect our identities*, The Hill (Oct. 27, 2017) (thehill.com/opinion/technology/357374-scrapping-social-security-numbers-wont-be-enough-to-protect-our-identities).

[4] The Internal Revenue Service, *IRS Statement on the "Get Transcript" Application* (May 26, 2015) (www.irs.gov/newsroom/irs-statement-on-the-get-transcript-application).

[5] KrebsonSecurity, *Equifax breach Fallout: Your Salary History* (Oct. 08, 2017) (krebsonsecurity.com/2017/10/equifax-breach-fallout-your-salary-history/).

[6] The White House, *National Strategy for Trusted Identities in Cyberspace* (April 2011) (obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf); National Institute of Standards and Technology, Trusted Identities Group (viewed Nov. 27, 2017) (www.nist.gov/itl/tig/about).

To address the challenges associated with the aftermath of breaches compromising personal data, companies have sought to develop more robust ways to verify and authenticate users. The FIDO (Fast IDentity Online) Alliance is an industry consortium that seeks to address the lack of strong authentication among devices. Its mission is to develop technical specifications, operate industry programs to help ensure worldwide adoption, and encourage standardization.[7] Other resources provide users with the opportunity to assess whether their information was compromised in a data breach.[8]

III. EFFORTS TO SECURE DIGITAL IDENTITIES

The objective of identity "proofing" is to establish that a subject is who they claim to be.[9] According to NIST, the proofing process generally includes the presentation, validation, and verification of a set of attributes.[10] For example, a user could present a driver's license as a way to show his or her full name, date of birth, and home address attributes. The entity receiving those attributes would then validate the information against an authorized source, such as a state database. To "verify" that the user is who he or she claims to be, the entity could then match a photo provided by the user with the photo on the driver's license. The applicant would then be said to have been successfully proofed.

According to NIST, digital identity presents a technical challenge because this process involves proofing and authenticating individuals over an open network.[11] The classic paradigm for authentication includes three factors: (1) something you know, e.g., a password, (2) something you have, e.g., an ID badge, and (3) something you are, e.g., a fingerprint or other biometric data.[12]

Online services usually include one factor for authentication, such as a password, and can include another factor such as a one-time text message with a numeric code, or a token that provides an access code. Banks and social media sites may allow users to opt-in for a two-factor authentication capability. However, hackers may be able to bypass weaker two-factor implementations, such as by intercepting codes or taking advantage of account-recovery

---

[7] FIDO Alliance, About the FIDO Alliance (fidoalliance.org/about/overview/).

[8] Have I been Pwned, *Who, What & Why* (haveibeenpwned.com/About).

[9] National Institute of Standards and Technology, Digital Identity Guidelines (NIST SP 800-63-3).

[10] National Institute of Standards and Technology, Digital Identity Guidelines (NIST SP 800-63-3A).

[11] National Institute of Standards and Technology, Digital Identity Guidelines (NIST SP 800-63-3).

[12] *Id.*

systems.[13] It is also possible that accurate responses to account-recovery questions may be readily available since data breaches have exposed personal information.

IV. WITNESSES

The following witnesses have been invited to testify:

Troy Hunt
Information Security Author and Instructor, Pluralsight
Founder, Have I Been Pwned?

Jeremy A. Grant
Managing Director of Technology and Business Strategy, Venable LLP
Former Senior Executive Advisor for Identity Management, National Strategy for Trusted Identities in Cyberspace, National Institute of Standards and Technology

Ed Mierzwinski
Consumer Program Director, U.S. PIRG

[13] *Two-Factor Authentication is a Mess, It was supposed to be a One-Stop Security Fix. What happened?* The Verge (Jul 10, 2017).