



COMMITTEE ON  
**ENERGY & COMMERCE**  
DEMOCRATS  
RANKING MEMBER FRANK PALLONE, JR.

**FOR IMMEDIATE RELEASE**  
November 30, 2017

**CONTACT**  
[CJ Young](#) — (202) 225-5735

## **Pallone Opening Remarks at Identity Verification Hearing**

**Washington, D.C.** – *Energy and Commerce Ranking Member Frank Pallone, Jr. (D-NJ) delivered the following opening remarks today at a Subcommittee on Oversight and Investigations hearing on “Identity Verification in a Post-Breach World:”*

Thank you, Mr. Chairman. So much of our lives today are online. Companies in virtually every sector of the economy collect vast amounts of personal data about consumers. These companies know they are targets for malicious attacks, and all too often, they fail to protect the valuable consumer information they collect and store.

Just this past week for example, the ride service company, Uber, revealed that it had been hacked – more than a year ago. This breach reportedly exposed the personal information of 57 million riders and drivers. This security breach is yet another example of a company that failed to protect the data of its customers, and then failed to come clean about their security breach – in this case for more than a year.

Then there was the Equifax data breach, which compromised the personal data of more than 145 million Americans. What’s worse, the Equifax breach compromised personal data like Social Security numbers and birth dates that are difficult or impossible to change.

Consumers affected by the Equifax breach are vulnerable – particularly because these identity verifiers can give someone access to other sensitive information. This Committee is still waiting for answers to questions we asked Equifax both before and after our hearing on the breach. This is unacceptable.

This is also unacceptable to the American people because when companies fail to protect consumer data, consumers pay the price – sometimes years after a breach.

As data breaches continue to compromise our personal information, it is important that we explore how consumers and the holders of consumer information can verify that individuals are who they say they are online.

For example, how many times has each of us been asked to provide the last four digits of our Social Security number to get access to other information? But how do we protect

---

consumers' digital identities, especially after the Equifax data breach exposed the Social Security numbers of nearly half the U.S. population?

And as companies suggest that they may move to behavioral and biometric verifiers, are we comfortable with how much more personal information will be collected and used? Are we comfortable with trusting that companies will keep this data secure? These are important questions now facing the world of digital commerce. According to the Identity Theft Resource Center, as many as 1,190 data breaches have occurred so far this year.

Any data breach exacerbates the issues the public is facing in verifying their identities and authenticating access online. Hackers and other malicious actors erode the trust we have online by using the data they have been able to glean about each and every one of us. That's not good for business, and it's certainly not good for consumers.

I want to thank our witnesses for being here today to discuss the latest in identity verification and the challenges of protecting people's data. I believe that unless we act and pass meaningful legislation, we'll continue to see more data breaches and the unfortunate ripple effects resulting from them.

Thank you, and I yield back.

###

---

[democrats-energycommerce.house.gov](https://democrats-energycommerce.house.gov) | [Twitter](#) | [Facebook](#) | [Instagram](#) | [YouTube](#) | [Flickr](#)