PRESS RELEASE

# SubDCCP Examines Consumer Data Security Practices Across Credit Reporting Industry

11.01.17

*This morning's witness panel at their seats as the hearing gets underway*

**WASHINGTON, DC –** The Subcommittee on Digital Commerce and Consumer Protection, chaired by Rep. Bob Latta (R-OH), today held a **hearing** to examine consumer data security practices, trends, and areas for improvement across the credit reporting industry.

**Chairman Latta began the hearing by asking the question on everyone's minds**, "Considering the size and scope of the Equifax breach consumers are confused, and rightfully skeptical, about what they should be doing to protect themselves. … What should we tell our constituents about how the credit reporting industry is securing their sensitive data?"

**Energy and Commerce Committee Chairman Greg Walden discussed** "the host of laws already on the books," saying, "The Gramm-Leach-Bliley Act prohibits financial institutions from disclosing non-public information without the consumer's consent. That's a law. The Fair Credit Reporting Act deems the unauthorized disclosure of consumer reports to be an 'unfair or deceptive act or practice.' That's a law. The Dodd Frank Act created an entirely new federal bureaucracy, the Consumer Financial Protection Bureau, and charged it, among other duties, with the task of protecting consumer financial information.

Despite these new and sweeping powers, the Bureau seemed completely unaware that the company had failed to implement the necessary software patch that could have saved Americans' data from hackers."

**Francis Creighton, President & CEO of the Consumer Data Industry, the trade association representing the three nationwide credit bureaus, touched on what companies are actively doing to protect consumers' credit data**, "We're fighting this war on a daily basis. We're getting attack non-stop from nation states, as one of our witnesses was mentioning, from criminals, and many others. We monitor, we test our system, we try to do data minimization and encryption, inside and while the data is in transit, to make sure that if in fact somebody is in the system the information is not useable and to try to keep them out of the system in the first place."

**Anne Fortney, Partner Emeritus, Hudson Cook LLP, commented on the regulatory environment surrounding the Equifax breach,** "The fact that there's been a security breach in general does not mean there's a violation of law. From what we've read, Equifax did not take appropriate measures to prevent the breach. The Fair Credit Reporting Act, if there's any credit reporting information involved, would come into play. There are civil penalties, as well as the FCC's authority to prevent future violations. The Gramm-Leach-Bliley rules also require Equifax to safeguard data on consumers that it holds, and there can be penalties there as well."

**James Norton, Founder and President of Play-Action Strategies LLC, noted the cybersecurity challenges facing the private sector,** "The private sector's cybersecurity problems cannot be blamed solely, or even mostly, on a lack of federal regulation. Instead, a root cause of the problems is a failure of organizations, private sector and governmental, to establish a culture of cybersecurity awareness. Organizations should not assume that employees understand cybersecurity and, as such, must be diligent about training employees on their role in keeping information protected."