STATE OF NEW YORK
OFFICE OF THE ATTORNEY GENERAL

ERIC T. SCHNEIDERMAN
ATTORNEY GENERAL

DIVISION OF ECONOMIC JUSTICE
BUREAU OF INTERNET & TECHNOLOGY

PREPARED STATEMENT OF KATHLEEN MCGEE
CHIEF OF THE BUREAU OF INTERNET & TECHNOLOGY
NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL

TO THE HOUSE FINANCIAL SERVICES COMMITTEE

OCTOBER 25, 2017

Mr. Chairman, Madam Ranking Member, and other distinguished Members of the Committee:

My name is Kathleen McGee, and I am the Chief of the Bureau of Internet & Technology at the New York State Office of the Attorney General, Eric T. Schneiderman. The Bureau of Internet & Technology is responsible for protecting New Yorkers from existing as well as new and developing online threats.

I am pleased to present this prepared testimony concerning data breaches, which continue to victimize consumers with greater and greater frequency, from small local businesses to giants like Target, Anthem, Yahoo, and now Equifax.

The Equifax data breach was unprecedented in scale and severity, affecting the private information of 145 million Americans, including more than 8 million New Yorkers. Our office acted immediately, launching a formal investigation of Equifax and pressing the company on a number of issues – including a delay in notifying consumers of the breach, a forced arbitration clause in free credit monitoring contracts, and the failure to provide Spanish-language customer service to consumers affected by the breach. Following conversations with our office, Equifax addressed all of those issues and later agreed to provide consumers the ability to lock and unlock their credit file for life.

We also contacted the other major credit bureaus – TransUnion and Experian – to discuss their data security.

We have also been in touch with numerous other state AG's offices – since we states often lead in consumer protection and data breach matters – as well as various federal agencies. While I cannot share details from ongoing investigations, I can say we are getting to the bottom of the Equifax breach and will ensure that all credit bureaus take effective steps to protect the sensitive information that millions of Americans have entrusted to them.

States have a central role in protecting consumers and their data. The New York Attorney General's Office and other state Attorneys General offices have been policing data breaches for nearly two decades.

Indeed, the states led the way on data protection for consumers. When the internet was still relatively new to consumers, states responded with data protection and data breach laws to protect their residents. And as the technology has evolved over the years, state law has evolved with it.

Back in 2002, when the internet was younger and e-commerce was beginning to take off, the state of California enacted the first data breach notification law. It proved to be a tremendous success for consumer protection, and New York and other states soon followed. Today, 48 states plus DC and the U.S. territories all have data breach notification laws. That is the sort of innovation at the state level that our federal system, at its best, promotes.

The states have already adapted those laws as technology and consumers' use of it changed, and as new threats emerged. For example, as email and other online accounts became an increasing part of consumers' daily lives – to make appointments, send confidential documents, and discuss work and personal affairs – account credentials became the "keys to the castle" for consumers' data.

As a result, states amended their laws to add username-and-password combinations as a trigger for breach notification – a key state law innovation. This is just one of many examples. As healthcare records increasingly became digitized, state laws began covering patient data. As companies increasingly used fingerprints to unlock devices, state laws began covering biometric data.

But it is better to prevent breaches before they happen. And states have been equally innovative on this point: enacting legislation requiring companies to implement adequate data security, and updating such laws as technology evolves. And states have a second tool: consumer protection laws, which AGs use to police misrepresentations about data security – as with other consumer products, it can be unlawful for a company to make misrepresentations about data security to consumers.

The New York Attorney General's office, recognizing the importance of this issue for consumers and the need to update New York's law, has proposed legislation to update New York's data security and breach notification laws. And, the New York Department of Financial Services – a separate state agency with jurisdiction over New York's banking and insurance sectors – also has innovated in this area, implementing important data security regulations to protect consumers' financial data.

In light of this background, I would like to make a few key points.

First, it would be a big mistake for Congress to preempt states' ability to legislate and innovate in this area. The law must be able to keep pace with the ever-increasing rate of change

in technology. States have proven the ability to act quickly in that regard – from both legislative and enforcement perspectives. In contrast, bills have been proposed in Congress for many years but, for one reason or another, enactment has proven elusive. Even if a federal law were enacted, it could prove difficult to amend and would fall far behind new technologies that will inevitably continue to emerge. Thus, even a federal law providing the most stringent protections based on current state requirements will leave consumers more and more vulnerable over time.

Second, when it comes to enforcement, states occupy a leading role today and must continue to do so.

Our office has issued data breach reports in recent years that show an alarming increase in data breaches. Indeed, in 2016 we received 1,300 data breach notices – up 60% from the year before. This Committee is likely aware of the megabreaches, such as the Target breach involving 40 million credit card numbers and the Anthem breach involving over 78 million records including Social Security Numbers. In those instances, New York and other states used a well-established process to coordinate enforcement efforts against companies that violated consumer trust with inadequate data security. As a result, the states obtained not just data security reforms through injunctive relief, but also large civil penalty recoveries that are essential to deterring other companies from violating consumer trust through lax security practices.

Less well-known, yet equally important, are the enforcement actions our office takes in response to smaller breaches that occur by the hundreds each year in New York and other states. One recent case illustrates the point. A small company outside Buffalo, New York misconfigured a web server, which led to the disclosure of 500 employment applications with Social Security Numbers in Google search results. Our office found out through a tip, contacted the company immediately, and got the applications removed from search results within days.

Even if a federal agency were provided with the most comprehensive data security law and the considerable resources needed for serious enforcement, it is unlikely that a federal agency would be as responsive as our office and our sister state AG's offices to breaches involving local businesses and relatively small numbers of local consumers. These breaches may be smaller than a Target or an Equifax – but the victims are no less in need of law enforcement protection. Smaller breaches like these are the rule, not the exception.

Further, with years of first-hand experience policing data security in our state, we know how to distinguish between breaches that a company should have prevented with better security versus breaches that could not have been avoided despite the company's reasonable security practices. By virtue of this experience, and our knowledge of conditions within our local communities and industries, we can avoid both underenforcement that would leave consumers unduly vulnerable and overenforcement that would create undue burdens on local businesses.

For all of these reasons, I respectfully urge this Committee to ensure that any legislation it considers meets the following requirements, which are vital to protecting states' innovative role in consumer data protection:

- Any new federal requirements should not preempt state law, but instead should expressly set a floor—not a ceiling—on data security standards and protocols in the event of breaches. States must be able to innovate in the areas of data security and breach notification and pass stronger and more up-to-date laws than the federal standard.

- As with several other federal consumer protection laws, any federal requirements must be enforceable by state attorneys general in addition to a federal agency, and any federal penalties or other monetary relief must be recoverable by the states as well.

- To the extent any preemption language is included, beyond the floor/ceiling issue discussed above, the language must be drawn carefully to avoid unintended severe consequences. Some preemption language can be so broad that it might be interpreted to set aside state laws concerning personal privacy or computer crimes, and that would be a serious problem for constituents.

These or similar provisions for joint federal and state enforcement authority are already included in other federal laws and have proven successful. For example, the New York AG's office has coordinated with the FTC on several investigations into violations of the federal Children's Online Privacy Protection Act, or COPPA, to stop invasive tracking on major child-focused websites.

The vast majority of state AGs' offices have similarly called on Congress to avoid preempting state action on data security, as recently as 2015, when a broad bipartisan group of 45 state AGs joined in asking Congress to oppose then-pending data security bills with harmful preemption provisions.

Our office continues to enforce data security protections on behalf of New Yorkers and to work with New York's state lawmakers to continually update those protections. We appreciate your Committee's efforts to complement those efforts at the federal level while ensuring that work at the state will continue successfully.