TESTIMONY OF

NATHAN TAYLOR

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

EXAMINING THE CURRENT DATA SECURITY AND BREACH NOTIFICATION REGULATORY REGIME

FEBRUARY 14, 2018

Chairman Luetkemeyer, Ranking Member Clay and members of the Subcommittee, my name is Nathan Taylor, and I am a partner at the law firm of Morrison & Foerster LLP in the firm's Financial Services and Privacy and Data Security practice groups. My practice is focused on helping financial institutions and other companies (*e.g.*, retailers and technology companies) protect the security of sensitive information and respond to the unfortunate security incidents involving that information that inevitably occur. My colleagues and I have represented companies in responding to a number of the largest and highest-profile data breaches in American history. I am pleased to be here today to provide background on the current legal landscape of state "safeguards" laws and breach notification laws, as well as to discuss some of the challenges that companies face in responding to security incidents.

At the outset, I would like to stress that I share your concerns about the critical need to protect American consumers and businesses from the constantly evolving and increasingly sophisticated cybersecurity threats that exist today. Although the word "cybersecurity" was not used in the English language until the late 1980s, it has rapidly become one of the most critical issues for our nation and society. Cybersecurity impacts not only the security of our own sensitive personal information, but also the security of our government, our critical infrastructure, our technology, our national defense, our elections and, in the increasingly Internet-connected world, our way of life.

Congress, including this Committee, has considered the issue of data security and breach notification for 15 years. *See, e.g.*, H.R. 3997, Data Accountability and Trust Act (introduced Oct. 6, 2005), *available at* https://www.congress.gov/bill/109th-congress/house-bill/3997. It goes without saying that during that time the issue of cybersecurity has grown ever more critical. Today, the obligation (if any) under state law to protect sensitive personal information about you depends entirely on where you live. That is, whether there is a state requirement to protect, for example, your Social Security number and financial account information is dictated by the state in which you reside. In addition, even though most states have enacted security breach notification laws, these laws often contain conflicting provisions, which complicates the process of responding to security breaches. Simply put, we need a single, nationwide standard to address what is truly a national issue.

I strongly believe that a single, nationwide standard for data security and breach notification would be good for both American consumers and American businesses. American consumers would benefit if all companies that may handle sensitive personal information about them are subject to the same strong federal standards to protect that information and to provide them with timely notice in the event of a security incident involving that information. American businesses would benefit from being able consistently to apply a single standard to protect sensitive personal information and to respond to the unfortunate, but inevitable, security incidents involving that information. I believe the time for Congress to act on this important issue is now.

Overview of State Safeguards and Security Breach Notification Laws

In order to advise companies on compliance with state law, it is critical to my practice that I have a deep understanding of the various state "safeguards" laws and breach notification laws, as well as related developments in state legislatures around the country. For more than a

decade, I have tracked each new state safeguards law and breach notification law and the many amendments to those laws that have followed. When you review the landscape of state laws that exist today, you find a complex matrix of inconsistent, sometimes duplicative and often contradictory requirements. In my testimony, I will focus on providing an overview of these state laws, including providing examples of how the state laws are either inconsistent or contradict in ways that result in consumers being treated differently based on where in the United States they live.

State Safeguards Laws

As discussed below, only two states have yet to enact breach notification laws. The opposite is true with respect to state requirements to protect information about consumers. Few states impose general obligations on companies to protect sensitive personal information.[1] As a result, whether there is a state obligation to protect sensitive information about a consumer, such as Social Security number or payment card information, depends entirely on the consumer's state of residence. And, more specifically, unless the consumer lives in one of several states, most businesses that handle sensitive information about the consumer are not subject to a state requirement to protect that information.

State Safeguards Laws

Only 15 states impose general requirements that businesses must protect sensitive personal information. Most of these state safeguards laws impose only high-level security obligations, typically a general obligation to take reasonable steps to secure data or to maintain reasonable security controls to protect data. For example, the California safeguards law provides that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b). These safeguards laws also typically include obligations for the secure disposal of information.

It is important to note that several of these 15 states do, in fact, have detailed safeguards laws that include specific security requirements, often modeled, at least in part, on the safeguards rule issued by the Federal Trade Commission pursuant to Section 501(b) of the Gramm-Leach-Bliley Act. *See* Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1436–1437 (1999); 16 C.F.R. pt. 314. For example, the Massachusetts data security rules and the Oregon safeguards law contain detailed safeguards provisions, including requirements to maintain risk-based information security programs that include safeguards designed to protect sensitive personal information against cybersecurity risks, to designate an individual to be responsible for overseeing and appropriately to oversee services providers who will have access to sensitive information. *See* 201 Mass. Code Regs. § 17.03; Or. Rev. Stat. § 646A.622. The Massachusetts data security rules and the Nevada safeguards law also include technology-specific requirements, such as

[1] The following discussion addresses state safeguards and disposal laws that apply to any business handling sensitive information relating to residents of the relevant states. It does not address state requirements that apply only to specific sectors, such as the financial sector. *See, e.g.*, N.Y. Comp. Codes R. & Regs. tit. 23, §§ 500.0 – 500.23 (rules for financial institutions subject to the authority of the New York Department of Financial Services); N.J. Stat. §§ 56:8-196 – 56:8-198 (security requirements for health insurance carriers).

requiring the encryption of data that is maintained on certain devices (*e.g.*, laptops) or that is transmitted electronically in certain ways (*e.g.*, over the Internet). 201 Mass. Code Regs. §§ 17.04(3), (5); Nev. Rev. Stat. § 603A.215(2).

In contrast, 35 states impose no obligation for companies to protect sensitive personal information, other than the secure disposal of information noted below.

State Disposal Laws

Although having a far narrower focus, 17 states, in addition to those noted above, have enacted laws that require the secure disposal of sensitive personal information that a business will no longer retain. For example, the Arizona disposal law prohibits a person from "knowingly discard[ing] or dispos[ing] of records or documents without redacting the information or destroying the records or documents if the records or documents contain" sensitive personal information. Ariz. Rev. Stat. § 44-7601(A). These state disposal laws, however, do not impose any obligation to protect the security of information *before* it will no longer be retained.

The Importance of a Single, National Standard for Data Security

If you are an American, where you live should not dictate whether there is a legal obligation to protect sensitive personal information about you. In my view, this point is not controversial. Most people would agree that a consumer's Social Security number and financial account information, among other things, are sensitive and, if in the wrong hands, could be misused in ways that cause the consumer harm. The sensitivity of this information and the related risks associated with its misuse are the same for all Americans, regardless of where they live.

Today, however, only a small minority of states impose substantive security requirements for the protection of sensitive personal information. While it is true that for many companies operating on a nationwide basis, the few detailed state safeguards laws (*e.g.*, the Massachusetts data security rules) often become the *de facto* national standard. That is, companies operating on a nationwide basis often develop a single compliance strategy that attempts to incorporate the security requirements of all applicable state safeguards laws. However, practical considerations typically drive that result, not the law. And, companies that maintain information on consumers in just a few states may not be subject to any substantive state security requirements at all.

In my view, this is not an equitable or appropriate result. Regardless of whether a consumer lives in, for example, Walnut Creek, California, Nampa, Idaho, Abilene, Texas or Norristown, Pennsylvania, sensitive personal information about the consumer should be protected. A single, national standard for security would accomplish that result, to the good of all Americans. This would also benefit American businesses by leveling the playing field to ensure that all companies are subject to robust requirements, while simplifying the compliance process so that a company can focus on a single federal law as opposed to disparate and often inconsistent state laws.

Overview of State Breach Notification Laws

To date, 48 states, as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted breach notification laws.[2] These laws ostensibly share the same purpose—ensuring that consumers receive notice of security incidents involving sensitive personal information about them so they can take steps to protect themselves from harm. In this regard, each state law's consumer notification trigger is based, at least in part, on some form of unauthorized, unlawful or illegal access to, or acquisition or use of, certain types of sensitive personal information.

Nonetheless, these state laws are far from uniform. In fact, they vary significantly in terms of their requirements, including scope, the types of personal information covered, notice content requirements and related obligations. These inconsistencies can lead to results that are unfair to consumers and unduly burdensome to businesses. If multiple companies experience the same type of breach involving the same exact facts except that the information involved in the different breaches relates to residents of different states, some consumers may receive notice, while others may not. And for those receiving notice, the notices may include different content and be provided in different forms at different times.

To give a sense of the ways in which the 52 breach notification laws can be inconsistent and/or conflict, the following provides a high-level discussion of two aspects of state breach notification laws: (1) requirements for the content of a consumer breach notice; and (2) notification requirements for incidents involving electronic/computerized data vs. data in paper form. There are many other meaningful differences that I could discuss, but the following are illustrative.

Content Requirements for a Consumer Breach Notice

Of the 52 laws, only 22 impose requirements for what the consumer must be told about the incident (*i.e.*, the types of information that must be included in a breach notice).[3] The notice content requirements typically focus on providing consumers with information about the nature of the incident, the types of information involved in the incident and steps consumers can take to protect themselves from harm. For example, the West Virginia law requires that a breach notice include a description of the types of information that were involved in the incident, a telephone number or website that the individual can use to contact the entity that experienced the breach and learn more about the incident, information on how a consumer can place a security freeze or fraud alert and toll-free telephone numbers and addresses for the major consumer reporting agencies. W.V. Code § 46A-2A-102(d)(1).

Some states require that a breach notice include information that is uniquely specific to residents of those states, such as contact information for state government entities. For example, the North Carolina law requires that a breach notice include "[t]he toll-free numbers, addresses,

[2] The following discussion addresses state breach notification laws that apply to any business handling sensitive information relating to residents of the relevant states. It does not address state breach notification requirements that apply only to specific sectors, such as health insurers. *See, e.g.*, Conn. Gen. Stat § 38a-999b.

[3] Two states impose requirements for the content of certain, but not all, breach notices. *See, e.g.*, 73 Penn. Stat. § 2302 (providing standards for the content of a telephonic notice).

and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft." N.C. Gen. Stat. § 75-65(d)(7). Although there often are significant differences from state to state in terms of the specific content required in a breach notice, the most common content requirement is that a breach notice must include a basic description of the incident. *See, e.g.*, Haw. Rev. Stat. §§ 487N-2(d)(1).

Some states go beyond the content of the notice and impose requirements for how that content must be presented, such as requiring that a notice be clear and conspicuous. *See, e.g.*, Mich. Comp. Laws § 445.72(6)(a) (requiring notice to "be written in a clear and conspicuous manner"). For example, the California law requires, among other things, that a notice "be written in plain language," include a specific title (*i.e.*, "Notice of Data Breach"), include specific headings (*e.g.*, "What Happened") and be written in "no smaller than 10-point type." Cal. Civ. Code § 1798.82(d)(1).

Although the state laws are far from consistent with respect to the required content for a breach notice, the Massachusetts law provides the most dramatic example of how state breach laws can conflict in material ways that complicate the process of responding to a breach. Specifically, the Massachusetts law *prohibits* a business from including in a breach notice "the nature of the breach or unauthorized acquisition or use." Mass. Gen. Laws § 93H-3(b). That is, a business that is required to provide notice to a Massachusetts resident about a breach involving sensitive information relating to the individual *may not* tell the individual basic information about the incident. As discussed below, while the Massachusetts content prohibition may be viewed as an outlier, it nonetheless complicates how companies respond to "nationwide" breaches.

Computer vs. Paper Breaches

Of the 52 laws, 43 apply only with respect to breaches involving computerized or electronic data that contains sensitive personal information. *See, e.g.*, Va. Code § 18.2-186.6 (defining a breach, in pertinent part, as "the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information"). The remaining nine state laws apply with respect to different forms of data beyond computerized data.

For example, the Alaska, Hawaii, Massachusetts, North Carolina and Washington laws apply with respect to breaches of sensitive personal information in any form. *See, e.g.*, N.C. Gen. Stat. § 75-65(a) (requiring notification regarding breaches involving "personal information in any form (whether computerized, paper, or otherwise)"). The Rhode Island law applies with respect to breaches involving personal information in computerized or paper form. R.I. Gen. Laws § 11-49.3-3(a)(8) (defining "personal information," in pertinent part, as unencrypted data and data "in hard copy, paper format"). The Indiana and Iowa laws are unique in that they apply to breaches involving computerized data and computerized data that have been transferred to another medium, such as paper. Ind. Code § 24-4.9-2-2(a); Iowa Code § 715C.1(1). Finally, the Wisconsin law is simply silent as to the form of data covered by the statute. *See* Wis. Stat. § 134.98.

Practical Challenges in Responding to a Breach

In the context of discussing the requirements of state breach notification laws, it is important to note some of the practical challenges that a company can face in responding to a significant breach, particularly one involving some type of computer or electronic intrusion. Even for companies who respond diligently and expeditiously, all the steps involved in investigating the incident, restoring the security of systems and preparing the response take time.

It is critical to highlight that a company's first indication of a breach (with the benefit of hindsight) is often fairly innocuous. At that time, the company may not realize that it is under attack. In my practice, I have seen many incidents that "begin" with an anomalous fact that is not itself indicia of a breach, such as, for example, a company receiving an IT alert that the performance of a server has slowed or that a server is nearing its storage capacity. And there are instances where the attackers feint to distract the company with a "decoy" attack, such as ransomware or a denial of service attack that requires a response from the company, but is not the ultimate goal of the attacker. Of course, there are also incidents where the first fact that the company learns creates a strong suspicion that data has been stolen, such, as for example, a call from the Federal Bureau of Investigation informing the company that information related to the company has been found online or on devices seized by law enforcement (*e.g.*, for sale on the "dark web").

Even when a company believes that an attacker has likely penetrated its defenses, the company has to investigate to determine the scope and extent of the breach, including, for example, determining whether data was actually stolen (which is not always the case). The resulting forensic investigation must attempt to recreate the attacker's steps to determine, among other things, what systems, applications and databases were accessed by the attacker, what commands were run, what changes were made and what data was stolen. This process grows more complex when the attacker has had prolonged access to systems or when the impacted systems are vast. While confirming the basic facts of what happened may seem simple in principle, it involves a detailed forensic review and analysis combing through logs, artifacts and other evidence, much like trying to recreate a crime scene.

Separate and apart from any steps that a company may take to determine whether consumer data has been stolen, the most important aspect of a company's initial response to a breach is its efforts to ensure that the attacker has been removed from its systems, as well as to address and remediate any issues or vulnerabilities that were exploited by the attacker in the first instance. This need becomes even more immediate when the breach will become public, thereby making the company a target for other attackers.

Even where a company believes that data has been stolen, it is often difficult to determine the exact data elements involved and the consumers to whom that information relates. For example, attackers often exfiltrate data from a company's systems in a highly encrypted format. As a result, the effort to confirm which data was stolen often involves a process of recreating the attacker's searches to determine the types of data the attacker likely accessed. This is often complicated by the fact that a company is recreating the attacker's steps at a later point in time, after the underlying data set has changed. Regardless, this is a critical step that companies take very seriously because the ramifications are significant. Specifically, a company needs to be

able to determine the specific data stolen so that it can ensure that the right consumers are notified. A company does not want to incorrectly notify a consumer that her data was lost and create unwarranted concern or confusion when the consumer is actually not at risk.

When a company determines that notice to consumers is required or otherwise appropriate, its work is only beginning. Particularly for large breaches, there are a number of critical steps that a company must take in order to provide notice to consumers. These steps include engaging third-party vendors (*e.g.*, a company to offer credit monitoring to consumers), preparing mailings (*e.g.*, validating mailing addresses, deduplicating the mailing list and printing letters and envelopes), preparing FAQs to be able to respond to consumer questions, setting up toll-free telephone numbers and arranging for sufficient call center capacity, to name just a few. This already complex process is made more difficult by the fact that a company must ensure that its various steps comply with the requirements of 52 different breach laws.

The Importance of a Single, National Standard for Breach Notification

Although virtually all states have breach notification laws, these laws contain many meaningful differences. These differences impact whether (if at all) a consumer receives a breach notice, what the breach notice says, when it is sent to the consumer and even how it is sent. In addition, the many differences complicate the process that a company must go through to respond to a breach involving sensitive information relating to Americans residing around the country or within multiple states.

Take, for example, the issue of the content of a breach notice discussed above. In providing notice to Americans throughout the country for a "nationwide" breach, a company can send a single notice to residents of all states other than Massachusetts and include in that notice all of the content required by the various states other than Massachusetts. The notice will often highlight certain content as being for residents of specific states, such as contact information for a state Attorney General. The company will then send a different and separate notice to residents of Massachusetts. This Massachusetts notice will omit any discussion of what happened to the consumer's information, as well as any content required by other states. Not only does this complicate the notification process, but it also has the adverse effect of ensuring that all Americans do not receive the same information about the same breach.

While many companies that experience "nationwide" breaches create strategies designed to treat all consumers equally from a notice standpoint regardless of where they live (to the extent permitted by law), this is not a requirement. For example, a company experiencing a nationwide breach could elect to comply with each of the 52 laws separately and develop state-specific notices based solely on each law's requirements (if any).

For every "nationwide" breach, however, there are thousands of breaches that involve information relating to residents of one state or several states. In this regard, for breaches involving sensitive information relating to residents of a single state (or several states), companies typically look to the law of that single state and craft their responses and consumer notices to comply with the relevant law. As a result, if two companies experience the same type of breach with the same facts and involving the same types of sensitive personal information, some consumers may receive notice, while others do not, solely because of where the consumers

live. And for those consumers who do receive notice, the consumers may receive different information, not because the facts may necessitate a different notice, but because the consumers live in a state that has no content requirements or the state's content requirements differ from those of other states.

Similar to my views on state safeguards laws, this is not an equitable or appropriate result. If a consumer's Social Security number is lost or stolen and the consumer is at risk of harm as a result of the incident, the consumer should receive notice, at the same time, in the same form and with the same content, regardless of whether he or she lives in, to use my earlier example, Walnut Creek, California, Nampa, Idaho, Abilene, Texas or Norristown, Pennsylvania. A single, nationwide standard for breach notification would accomplish that result. In the process, American businesses would benefit significantly. Specifically, a company would be able to craft a response strategy that is designed to comply with a single federal standard without having to address the nuances and inconsistencies of 52 different laws. This would allow companies to respond faster, to the benefit of the American consumer.

The Path Forward

I would like to reiterate my strong belief that a single, nationwide standard for data security and breach notification would be good for both American consumers and businesses. American consumers would benefit by receiving the same protections for sensitive personal information about them regardless of where they may live. American businesses would benefit from a single standard that can be applied consistently to protect sensitive personal information and to respond to the unfortunate, but inevitable, security incidents. This is a national issue, and I believe that the time is now for Congress to act.

With respect to drafting legislation to address this important issue, I believe any legislation that this Committee considers should, at a minimum, address the following four principles:

(1) A federal bill should include strong, yet flexible and scalable, data protection standards for all companies that handle sensitive personal information;

(2) A federal bill should require notification to consumers in the event of a breach that puts consumers at risk of harm;

(3) A federal bill should recognize existing federal standards on data security and breach notification, including under, for example, Title V of the Gramm-Leach-Bliley Act, and deem entities subject to those standards to be in compliance with the legislation if they comply with their existing federal obligations; and

(4) A federal bill should preempt state safeguards laws and breach notification laws to ensure that all Americans receive the same level of protection regardless of where they live.

* * * *

Thank you for the opportunity to speak with you today. I would be happy to address any questions that you may have.