Written Testimony of
John Miller

Vice President, Global Policy and Law
Information Technology Industry Council (ITI)

Before the
Subcommittee on Financial Institutions and Consumer Credit
U.S. House Committee on Financial Services

"Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime"

March 7, 2018

Written Testimony of:
John Miller
Vice President, Global Policy and Law

Information Technology Industry Council (ITI)

Before the:
Subcommittee on Financial Institutions and Consumer Credit
U.S. House Committee on Financial Services

"Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime"

March 7, 2018

Chairman Luetkemeyer, Ranking Member Clay, and Members of the Subcommittee, thank you for the opportunity to testify today on the *Discussion Draft of H.R. ___, the Data Acquisition and Technology Accountability and Security Act* (hereinafter, the "discussion draft"). My name is John Miller, and I am the Vice President for Global Policy and Law at the Information Technology Industry Council (ITI). ITI, the global voice of the tech sector, represents over 60[1] of the world's leading information and communications technology (ICT) companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, internet companies, and companies using technology to fundamentally evolve their businesses. Privacy and cybersecurity policy are rightly a priority for governments and our industry, and we share common goals of protecting the privacy of individuals' data, improving cybersecurity, and maintaining strong consumer protections.

Cybersecurity and network and data protection technologies are critical to ITI members. Facilitating the protection of our customers, including governments, businesses, and consumers, and securing and protecting the privacy of our customers' and individuals' data are core drivers for our companies. Further, organizations across a variety of sectors often choose

[1] See ITI membership list at http://www.itic.org/about/member-companies.

to address risks to data and other cybersecurity risks today through the use of sophisticated third-party services providers, including some ITI companies, who offer innovative security technology, services, and risk management expertise, which may otherwise be lacking within those organizations. Consequently, ITI has been a leading voice in advocating for effective approaches to both privacy and cybersecurity.

I would like to begin my remarks by commending you, Chairman Luetkemeyer and Congresswoman Maloney, for the transparent and inclusive process through which you and your staffs have worked to develop this discussion draft. We share your goal of developing a uniform, preemptive, consumer protective data security and breach notification regime, and appreciate the openness with which you have not only listened to but considered our priority issues. Congress and the business community have worked for more than a dozen years to develop a regime that balances the concerns of all stakeholders, and this effort moves us closer to realizing that shared goal. We also recognize that compromises in this arena must be made, and we do not wish the perfect to be the enemy of the good. In that spirit of compromise, ITI supports many of the provisions in the discussion draft, but we also offer several recommendations aimed at further improving, refining, and clarifying the draft language.

I will focus the balance of my testimony on four areas: (1) the environmental backdrop and context calling for a streamlined federal data breach notification standard; (2) summarizing the positive principles reflected in the breach notification portion of the discussion draft; (3) assessing the security safeguards section of the discussion draft; and (4) offering recommendations to further improve, clarify, and refine the discussion draft.

Environmental Backdrop and Context

Our companies are not only data security solutions providers but are also stewards of sensitive customer data. As such, we have dual interests in seeing Congress adopt a federal data security

and data breach notification regime – both as third-party solutions providers and as covered entities. While companies across the digital ecosystem invest tremendous resources in defending their infrastructures, networks, and systems and protecting their customers' information, the defenders are engaged in an ongoing virtual arms race with attackers seeking to breach those systems and compromise that data. So, the reality facing organizations today is they must race to keep up with increasingly sophisticated and well-resourced hackers – ranging from criminals to nation-states – who are scheming to stay one step ahead of their victims. Unfortunately, the percentages do not favor the defenders, who must be successful every time to avoid a breach. Instead, the odds favor the attackers, who only need to be successful once to execute a successful breach. And when a breach of sensitive personally identifiable information (PII) occurs, we believe there should be a streamlined and uniform process to notify consumers in cases where there is a significant risk of identity theft, financial harm, or material economic loss.

There are currently 52 different breach notification regimes in 48 states and four U.S. territories.[2] And while there is no vacuum of consumer protection under this patchwork – consumers across the country have for years received notifications pursuant to these laws – the scope of legal obligations following a data breach is broad and complex because each of these notification laws varies by some degree, and some directly conflict with one another. The significant variances among these state and territory laws include the timeline for notification, the circumstances requiring notification, how notification should be effectuated, and what information should be included in a notification. Similarly, there is an expanding, convoluted patchwork of state data security laws. Today, there are more than a dozen laws regulating how data must be secured, ranging from requiring reasonable procedures appropriate to the

[2] The District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands each adopted a data breach notification law. South Dakota and Alabama have not yet enacted breach notification laws.

sensitivity of the data, to more prescriptive, compliance-based "check the box" approaches.[3] Federal data breach notification legislation offers the opportunity to streamline the notification requirements into a single, uniform procedure, and to enhance the security landscape by incentivizing the adoption of security principles by entities in all 50 states that are flexible, risk-based, remain "evergreen," and are adaptable to ever-changing threats.

Notification of Breaches Involving Sensitive PII

ITI has long advocated for federal data breach notification legislation that achieves the important goals of reducing consumer confusion, enabling faster consumer notification, and avoiding over-notification and consumer desensitization. ITI developed principles representing the elements a data breach notification bill must include to achieve these goals.[4] The principles are attached to this testimony as Exhibit A. The discussion draft reflects the majority of these principles, including:

- Preempts the patchwork of existing laws and thereby reduces consumer confusion by ensuring consistency in notices, enables businesses to notify consumers faster than is possible under the patchwork of 52 different state and territory notification laws and avoids adding a 53rd standard to the inconsistent regulatory landscape;
- Creates an exception for information that is not in readable or usable form (such as via encryption);
- Recognizes the importance of avoiding over-notification by appropriately limiting the definition of "personal information" to data, which, if obtained by a criminal, could result in concrete financial harms;
- Recognizes that certain industries are already subject to breach notification requirements and does not impose an overlapping regulatory regime on those sectors;
- Allows notification to be effectuated by methods that are appropriate to each company-customer relationship;
- Recognizes the need for flexibility for companies and their third-party vendors to determine who should notify consumers in the event of a breach (consumers are often

[3] Arkansas, California, Connecticut, Florida, Indiana, Kansas, Maryland, Massachusetts, Minnesota, Nevada, New Mexico, Oregon, Rhode Island, Texas, and Utah each adopted a law related to the security of personal information.
[4] See https://www.itic.org/dotAsset/e03b1f88-4661-4b5a-a105-6cc6df1eb028.pdf

unaware of these third-party relationships and requiring a notification from the unknown third party to the consumer will create unnecessary confusion);

- Does not impose criminal penalties on victims of criminal hacks; and
- Recognizes both the danger of alerting hackers to vulnerabilities before they have been remediated (and risking potential further harm to consumers) and the risk of confusing or alarming consumers unnecessarily if companies are forced to notify prematurely – before a forensic investigation has been completed – under an arbitrary timeline. the discussion draft also permits companies to heed law enforcement requests to delay notification to allow for proper investigation of the incident or pursuit of criminal actors.

On balance, the breach notification section of the discussion draft offers much-needed regulatory clarity and certainty, which is critical for businesses that devote tremendous resources to data security and legal compliance.

Safeguarding Sensitive Personal Information

In the context of the data breach debate, the procedures often labeled "data security" are ultimately indistinguishable from risk management controls and best practices that are characterized as ''cybersecurity" measures in other contexts. ITI has long advocated for the adoption and deployment of effective cybersecurity and data security measures by stakeholders across the digital ecosystem. ITI has actively participated in efforts to develop cross-sectoral, ecosystem-wide cybersecurity approaches grounded in sound risk management principles, international standards, and consensus best practices. ITI also supports efforts that are voluntary, leverage public-private partnerships, foster innovation in cybersecurity and data protection through their flexible application, and are scalable for organizations of all sizes and sophistication.

The threat landscape constantly evolves and so too must data protection and security measures. Any cybersecurity regulatory regime must complement – not replace – an organization's existing risk management processes and program. Most importantly, ITI is a strong advocate of avoiding redundant or conflicting siloed approaches that complicate security

efforts for organizations and create inefficiencies by redirecting resources from securing their enterprise to static compliance programs. A company must be able to protect the information it holds in a manner that is reasonable and appropriate to the nature of its business and the sensitivity of the data it handles. The security program by which an organization chooses to secure data should be voluntary, based on effective risk management and provide companies with the ability to adapt rapidly to emerging threats, technologies, and business models.

The security safeguards section is consistent with a number of key security principles which, if followed in isolation, seem to provide effective guidance for an organization seeking to better protect information. For instance, § 3(a)(1) in the discussion draft calls for the development and implementation of "reasonable" security measures designed to protect the security of personal information from unauthorized acquisition, § 3(a)(2) calls for those safeguards to be flexible and appropriate to the particular size, resources and capabilities, and sensitivity of the data held by the covered entity, and § 3(a)(3) reflects the common elements of a risk management based approach to security, including core risk management functions such as Identify, Protect, Detect, and Respond. However, when considered as a whole, the security safeguards section is critically flawed in at least two respects.

First, the section creates a multi-layered set of requirements, setting forth a "reasonable security" standard in § 3(a)(1), and then prescribing a set of specific and in some cases rigid security requirements in § 3(a)(3). This structure exposes organizations to a regulatory "double jeopardy" of sorts, where they can employ all of the specific prescribed elements in § 3(a)(3) and yet still be found to have not implemented reasonable safeguards under the reasonableness standard in § 3(a)(1). We do not believe the bill should provide regulators with the unfettered discretion to decide whether "just" complying with the safeguards in §§ 3(a)(3)(A) through (E) is "reasonable enough."

Second, § 3(a) (2) appropriately mandates that security safeguards be flexible, and appropriate to the particular characteristics of a covered entity, including its size, scope of business, available resources and security costs, and the sensitivity of the data it handles. Yet, § 3(a)(3) conflicts with this acknowledged need for flexibility. For instance, the requirement in § 3(a)(3)(A) that all covered entities designate a single employee to maintain safeguards ignores the fact that such a requirement might be completely inappropriate for a startup or small business, or even a larger organization that might choose instead to hire a service provider to provide managed security services.

In short, while the safeguards section gets much right in calling for organizations to adopt reasonable, flexible, and risk management-based approaches to security, it ultimately undermines its potential effectiveness in aspiring to require reasonableness and flexibility by also prescribing what that should look like in a sometimes rigid and inflexible manner, and ultimately providing regulators, rather than organizations, with the discretion to determine what security measures are reasonable.

Recommended Modifications

We appreciate that the discussion draft reflects a great number of our data breach notification priorities. Below, we offer several recommendations that will provide the business community with the clarity and certainty it requires in a regulatory regime that allows for the imposition of significant monetary penalties.

First, the timeline for notification should reflect the realities of completing an investigation and putting in place the apparatus necessary to notify very large numbers of consumers. An "immediate" notification is not only infeasible, it constitutes a bad security practice that puts consumers at risk of further harm if notification is required before vulnerabilities have been rectified, even if the "preliminary" investigation of the "who" and the "what" has been

completed. If vulnerabilities are not remediated before notification is triggered, consumers will undoubtedly be subject to further harm by would-be thieves who are alerted to the vulnerabilities by public notice. The discussion draft must allow companies to restore the reasonable integrity, security, and confidentiality of the data system *before* notifying consumers. Additionally, "immediately…and without unreasonable delay" are competing concepts – juxtaposing them as in the discussion draft is confusing and counterproductive. We recognize the urgency required for notification and recommend utilizing language from one of the existing state laws to convey such urgency. For instance, both New York and California require consumer notification "in the most expedient time possible and without unreasonable delay."[5]

Second, the language under § 4(c)(1) that requires third parties to notify covered entities whose data "has or may have been compromised" must be amended to "has been compromised." As drafted, § 4(c)(1) imposes an obligation on third parties to notify covered entities of breaches that "may have occurred" involving data that "may have been compromised." This proposed requirement ignores the fact that cloud providers and other third parties deal with security incidents daily, ranging from minor to significant, often at very large volumes. These organizations cannot and should not be expected to notify customers based on a guess as to what "may" have happened. Further, the discussion draft imposes requirements on third parties who "suspect" a breach but have not confirmed it. Third parties frequently suspect breaches may have happened but upon investigation determine that no breach has occurred. These types of theoretical, rather than factual, inquiries would waste significant resources (of both third parties and covered entities) better devoted to implementing risk management controls or responding to actual compromises of data, lead to over notification, and serve no discernible purpose. We propose the discussion draft be amended to provide that third parties

[5] N.Y. Gen. Bus. Law § 899-aa; Cal. Civ. Code § 1798.29.

should be required to notify only when hard evidence indicates that a compromise in fact occurred and resulted in exfiltration of the covered entities' data.

Third, the discussion draft must include a heightened burden of proof for regulators if the security measures remain layered by a reasonableness standard. Where a company complies with the enumerated elements of §3(a)(3), we recommend the Federal Trade Commission (FTC) or State Attorneys General be required to prove non-compliance with § 3(a)(1) – failure to "maintain reasonable administrative, technical, and physical safeguards" – through clear and convincing evidence. By mandating compliance with the enumerated safeguards under § 3(a)(3), the government mandates what a reasonable security program looks like and directs covered entities to focus on those specific practices. Where a company relies on the government's directions, follows this mandate, and still suffers a security breach at the hands of a criminal hacker, it is reasonable to require the FTC or an Attorney General to demonstrate through additional proof that the company's practices were nevertheless unreasonable. This heightened evidentiary standard would not render compliance with the enumerated safeguards optional, nor would it preclude the enforcement agency from finding that a company failed to implement reasonable safeguards; it would simply require a more thorough showing than a preponderance of the evidence by the FTC or an Attorney General that a company who complied with the enumerated safeguards nevertheless lacked reasonable safeguards.

Fourth, to clarify when a company will be considered a third party versus a covered entity, the definition of "covered entity" should be amended to read "any person, partnership, corporation, trust, estate, cooperative, association, or other entity that *owns or licenses* personal information." As drafted, the definitions focus on the entity's activity rather than the entity's relationship to the data. Consequently, entities acting as third parties will in most if not all instances simultaneously be considered covered entities because both definitions use the verbs (or variants of the verbs) "accesses," "maintains," "stores," and "handles" personal

information. This result is problematic because the discussion draft imposes different requirements on covered entities versus third parties, and the current overlapping definitions will in some instances cause third parties to be subject to both sets of divergent requirements for the very same activity. The proposed edits will clarify what is required of these entities in situations in which a breach of personal information they do not own or license occurs (when acting as third parties) versus what is required after a breach of personal information that they themselves own or license (as covered entities).

Fifth, the discussion draft permits unlimited civil penalties arising from a single incident. Most data breaches are the result of criminal acts, and breached entities are therefore the victims of a crime. Organizations can and should do their part to protect consumer data from unauthorized access, but uncapped civil penalties are seemingly punitive in nature and thus not appropriate to impose on an organization that has been victimized by criminal hackers or more sophisticated attackers, such as nation states. Further, data breaches are already extremely costly for companies, even before factoring in fines and penalties, when one considers the immediate response expenses of investigating and remediating the breach, notice to consumers and appropriate agencies, communications and media fees, reputational costs, loss of consumer trust, impaired goodwill, lost revenue, legal fees, and operational impacts. , Any federal data breach law must contain reasonable penalty caps to avoid crippling fines that, on top of the myriad other reputational and response expenses, would risk putting companies out of business, including large publicly-traded companies who have a fiduciary duty to their shareholders. Further, the absence of reasonable penalty caps will make it much more difficult for companies to obtain cyber insurance – precisely the type of responsible behavior we should seek to advance through data security and breach notification legislation.

Sixth, the economic loss consideration in the risk standard should be amended to reference material economic loss. Without this clarification, companies would be liable for the most

minute of losses – for instance, the cost of a stamp to send a signed letter to a financial institution certifying one is not responsible for fraudulent charges is an economic loss – encouraging frivolous lawsuits that drain significant resources that are better invested in ongoing security risk management practices.

Seventh, the delay in notification permitted pursuant to a request by law enforcement – specifically by the U.S. Secret Service, the FBI, or State law enforcement – should be expanded to include requests by national security agencies such as the Department of Homeland Security or the National Security Agency, particularly given the rising number of incidents involving nation states, as well as the capacity of those agencies to render aid to companies that are victims of such attacks.

Eighth, the definition of "personal information" should be amended to exclude the words "alone or" in § 2(10)(A)(ii). Standalone financial account numbers in combination with merely a person's name cannot be used to obtain credit, withdraw funds, or engage in financial transactions.

Ninth, substitute notice should be permitted in instances when notification will be required for greater than 1,000,000 individuals, or when notification will result in excessive cost to the organization. In either event, individual notification will result in draining resources that should more appropriately be committed to remediation of the vulnerability and continuing the capital-intensive efforts to secure personal information.

Conclusion

ITI and our member companies appreciate the Committee's attention to this matter and its effort to develop a compromise solution to advance data breach legislation that provides for a single, rational federal breach notification standard, and incentivizes the adoption of

reasonable, flexible, risk-based data security practices. As ITI continues to gather feedback on the discussion draft of the *Data Acquisition and Technology Accountability and Security Act* from its member companies, we look forward to sharing that feedback with the Committee. Thank you again for the opportunity to testify today, and I look forward to your questions.

Exhibit A

Data Breach Notification Principles

The Information Technology Industry Council (ITI) strongly supports efforts to establish a commonsense, uniform national breach notification regime to help consumers when there is a significant risk of identity theft or financial harm. We are committed to working with Congress to enact meaningful legislation that establishes a national data breach notification process that is simple and consumer-driven. As the committees of jurisdiction in the House and Senate work to develop their respective bills, we urge Members to include the following key elements:

1. Federal Preemption. ITI supports the creation of a strong federal breach notification law. Effective federal preemption of the multitude of state notification laws will allow businesses to notify consumers more quickly when a breach of sensitive personal data occurs by easing the confusion and duplication that results from the current patchwork of competing, and often conflicting, state requirements. With almost every state now having enacted data breach notification laws, it is important that the role of the states be carefully defined in federal legislation.

2. Inaccessible, Unusable, Unreadable, or Indecipherable Data. Data may be unusable due to the absence of critical pieces, obfuscation, encryption, redaction, anonymization, or expiration by its own terms. Effective security practices and methods change over time and new technologies continue to evolve which enable data to be rendered unusable. An effective "unusable data" provision would make clear that notification is not required when there is a reasonable determination that data is rendered inaccessible, unusable, unreadable, or indecipherable. It is important that federal legislation not single out or give preference to one method of rendering data unusable as a means to avoid notification. Such action could create a false sense of security and create a compliance basement which may reduce the development and use of diverse and innovative security tools. ITI supports legislation that recognizes such technologies with technology-neutral and method-neutral language and that allows businesses to determine whether or not data may be used for the purposes of committing identity theft or financial harm.

3. Effective Harm-Based Trigger. Federal breach notification legislation must recognize the delicate balance between over- and under-notification with respect to when notices should be sent to consumers. ITI strongly believes notification should only be required after organizations determine the unauthorized acquisition of sensitive personal data could result in a significant risk of identity theft or financial harm. Expanding the types of harm to vague or subjective concepts such as "other unlawful conduct" creates confusion and will result in over-notification. Additionally, efforts to lower the threshold to a reasonable risk of identifity theft or financial harm will expose consumers and businesses to the numerous costs associated with over-notification. Further, the definition of a data breach should clearly tie an "unauthorized acquisition of sensitive personal information" to the risk of identity theft or financial harm. Not all data breaches are nefarious nor do they create a risk to consumers. Failing to recognize this in the definition of a data breach would expose organizations to possible enforcement action by government entities, including state attorneys general, for unauthorized breaches, regardless of the risk of identity theft or financial harm.

4. Reasonable Scope of Legislation. The protection of consumer information across industries is a complex statutory and regulatory puzzle. It is important that federal breach notification legislation does

not create unworkable and overlapping regulatory regimes for commercial and financial services industries. Entities that are already subject to any existing federal data breach requirements in a sector-specific law should continue to be required to comply with those laws and should not be subject to additional regimes.

5. Flexible Manner of Notification. Federal data breach notification requirements must accommodate both traditional companies that communicate with customers by mail, telephone, or fax and online companies that communicate predominantly through electronic communication (e.g., electronic mail). Consumers trust that companies will notify them in a manner that is consistent with previous communications and expect that will be done in an expedient and timely manner. A consumer receiving a telephone call from their email provider outlining a breach and urging action would be justifiably suspicious.

6. Third Party Requirements. Many organizations contract with third parties to maintain or process data containing personal information. Consumers may be unaware of these third-party relationships and requiring a notification from the third party to the consumer may create unnecessary confusion. In the event of a data breach of any third party system, the third party should be required to notify the consumer-facing company of the breach. The consumer-facing company and the third party should then have the flexibility to determine which entity should notify consumers. Additionally, legislation should not require notification of a broad range of third parties other than the consumer and credit reporting bureaus in the event of an actual or likely breach.

7. No Private Right of Action. An effective breach notification requirement and an efficient enforcement framework provides the best protection for consumers and will avoid unnecessary and frivolous litigation. Legislation should also prohibit the use of government regulatory enforcement action in private litigation asserting non-preempted state or other causes of action.

8. No Criminal Penalties. Most data breaches are the result of criminal acts, and therefore, breached entities are the victims of a crime. Organizations can and should do their part to protect consumer data from unauthorized access, but they should not be subject to criminal sanctions for being victimized by criminal hackers.

9. Discovery, Assessment, Mitigation, and Notice. Federal legislation must allow organizations to redress the vulnerability and conduct thorough investigations of suspected data breaches before notifying customers or government agencies. Unless the vulnerability is addressed prior to making the incident public, the organization and its customers are susceptible to further harm. Notifying customers will be counterproductive should the alleged breach prove false or if the breach does not create a risk of identity theft. A tremendous amount of forensics, decision-making, and legal work is required before ascertaining the nature and scope of a breach, assessing the risk of harm, and determining the appropriate form of notification. Recognizing the sophistications of today's hackers, and the challenging nature of a post-data breach forensic investigation, federal legislation must provide realistic, flexible, and workable time requirements, as well as recognize the need to cooperate with law enforcement in their criminal investigations.