Information Technology Industry Council

Written Testimony of
Yael Weinman

Vice President, Global Privacy Policy and General Counsel
Information Technology Industry Council (ITI)

Before the
Subcommittee on Commerce, Manufacturing, and Trade

U.S. House Committee on Energy & Commerce

Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015

March 18, 2015

Information Technology Industry Council

Summary of Testimony of Yael Weinman

Federal data breach notification legislation offers the opportunity to develop a single uniform standard, and should achieve the important goals of reducing consumer confusion, enabling faster consumer notification, and avoiding over-notification and consumer desensitization. ITI developed principles containing the elements a data breach notification bill must include to achieve these goals. We note that the *Data Security and Breach Notification Act of 2015* includes a number of these critical elements in that it: (a) preempts the patchwork of 51 breach notification regimes; (b) recognizes that consumers want clarity and certainty in their notices; (c) recognizes that notification can only take place once an organization determines the scope of any data breach and has remedied vulnerabilities; (d) allows for flexibility in notification, permitting companies to heed law enforcement requests to delay notification; (e) recognizes the importance of avoiding over notification; (f) recognizes how businesses communicate with their customers in today's economy and permits flexibility in how notification is provided; (g) recognizes that data may be rendered unusable by certain security tools; (h) recognizes the reality of third-party business relationships; and (i) avoids subjecting certain industries to duplicative regulation when they are subject to existing sector-specific regimes.

Certain aspects of the draft legislation would benefit from greater clarity and further consideration. In particular, the threshold of "reasonable risk" combined with the phrase "economic loss or economic harm" could lead to over-notification. Another area that would benefit from greater clarity is the timeline for notification by a covered entity if the data breach was suffered by a third-party entity. As written, it is unclear whether the covered entity's notification requirement commences only when the third-party entity has had the opportunity to restore the integrity of its system. We also note that the defined term "breach of security" in the draft bill is not clear in that it includes a reference to the compromise of "security" thus creating circularity within the definition. In addition, the use of the definition could have negative unintended consequences in foreign jurisdictions that are considering imposing problematic cybersecurity requirements on the tech sector. We further note that the penalties authorized in the draft legislation are elevated and thus unfairly punitive for an organization that is itself victim of a crime.

Information Technology Industry Council

Written Testimony of:
Yael Weinman
VP, Global Privacy Policy and General Counsel

Information Technology Industry Council (ITI)

Before the:
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House Committee on Energy & Commerce

Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015

March 18, 2015

Chairman Burgess, Ranking Member Schakowsky, and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Yael Weinman and I am the Vice President for Global Privacy Policy and the General Counsel at the Information Technology Industry Council, also known as ITI. Prior to joining ITI, I spent more than 10 years as an attorney at the Federal Trade Commission, most recently as an Attorney Advisor to Commissioner Julie Brill.

ITI is the global voice of the technology sector. The 60 companies ITI represents—the majority based in the United States—are leaders and innovators in the information and communications technology (ICT) sector, including in hardware, software, and services. Our companies are at the forefront of developing the technologies that protect our networks. When a data breach occurs, however, there needs to be a streamlined process that helps guide how consumers are informed in cases when there is a significant risk of identity theft or financial harm resulting from the breach of personally identifiable information.

While companies and financial institutions invest tremendous resources in defending their infrastructures and protecting their customers' information, it is an ongoing virtual arms race. Organizations race to keep up with hackers while the criminals scheme to stay one step ahead. Unfortunately, it is no longer a matter of *if,* but a matter of *when,* a criminal hacker will target an

organization. And when certain information about individuals is exposed, those consumers may be at a significant risk of identity theft or other financial fraud.

As a result of this troubling landscape, over the years legislatures across the country enacted data breach notification regimes. Currently, there are 51 such regimes—in 47 states and four U.S. territories.[1] Consumers across the country have received notifications pursuant to these laws. I have received more than one such notice myself, and I imagine some of you may have as well.

As a result of this patchwork, the current scope of legal obligations in the United States following a data breach is complex. Each of the 51 state and territory breach notification laws vary by some degree, and some directly conflict with one another. There are significant variances among these state and territory laws, including the timeline for notification, what circumstances give rise to a notification requirement, how a notification should be effectuated, and what information should be included in a notification. Federal data breach notification legislation offers the opportunity to streamline these requirements into a single, uniform standard.

Federal data breach notification legislation should achieve the important goals of reducing consumer confusion, enabling faster consumer notification, and avoiding over-notification and consumer desensitization. ITI developed principles containing the elements a data breach notification bill must include to achieve these goals. The principals are attached to this testimony as Exhibit A. The *Data Security and Breach Notification Act of 2015* reflects several of these principles and offers a certain level of regulatory clarity and certainty, which is critical for businesses—like ITI member companies—that devote tremendous resources to legal compliance:

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

- The draft bill preempts the patchwork of 51 breach notification regimes. Preemption is critical in order to streamline the data breach notification regime in place today. Without preemption, however, the bill would further muddy the unclear waters and add another layer of complexity to the data breach response process by adding a 52nd law to the existing patchwork. By creating a single breach notification regime, consumers will experience consistency across notices, thereby ensuring notices are more easily understood, and companies will save response time by not running through 51 different checklists before sending a notification.

- The bill recognizes that consumers want clarity and certainty in their notices, and that they expect a company who suffers a breach to attempt to mitigate further harm. The bill recognizes that notification can only take place once an organization determines the scope of any data breach and has remedied vulnerabilities. Providing notice of a breach while a system remains vulnerable risks further attacks, potentially making consumer information more vulnerable. The bill also allows for flexibility in notification, permitting companies to heed law enforcement requests to delay notification to investigate the incident or pursue bad actors engaged in criminal activities.

- The bill recognizes the importance of avoiding over-notification; the definition of "personal information" in the draft bill is appropriately limited to data, which, if obtained by a criminal, could result in concrete financial harms.

- The bill recognizes how businesses communicate with their customers in today's economy and permits flexibility in how notices occur. If a consumer typically engages with a company via email or other electronic means, then those would be permitted methods of providing notification. This is highly important, as consumers may not expect a written letter containing such a notice if they have previously only communicated with such companies electronically. Consumers and companies should have the flexibility to choose how to send and receive important notifications.

- The bill recognizes that data may be rendered unusable by certain security tools. Our companies are at the forefront of developing and utilizing the technologies to protect our networks and data. If data is unusable or unreadable notification is unnecessary.

- The bill recognizes the reality of third-party business relationships. Many organizations contract with third parties to maintain or process personal information. Consumers may be unaware of these third-party relationships and requiring a notification from the unknown third party to the consumer may create unnecessary confusion.

- The bill recognizes existing statutory regulatory frameworks and avoids subjecting certain industries to duplicative regulation when they are subject to existing sector-specific regimes.

ITI recognizes that many of the principles it has developed on data breach notification are reflected in the draft bill. However, certain aspects of the draft bill raise concerns in that they do not provide sufficient clarity as to what is to be expected of organizations—and such lack of clarity could be detrimental to consumers. Without clarity and certainty of what is required by law, companies will err on the side of caution to avoid being on the wrong side of a Federal law, resulting in over-notification to consumers and the desensitization of consumers to these notices.

One area where greater clarity is necessary is the description of the risk threshold that triggers consumer notification. ITI appreciates that the bill ties the unauthorized acquisition of "personal information" to the risk trigger. However, we are concerned that the threshold of "reasonable risk,"—which is lower than the "significant risk" threshold recommended in ITI's data breach notification principles—combined with the term "economic loss or harm" will inevitably lead to over-notification. It is unclear what is meant by "economic loss or harm" and how that category is distinguished from the phrase "financial fraud." The purpose of the bill is to enable consumers to take steps to protect themselves from identity theft and financial harm that can be perpetrated

by criminals who have gained access to certain personal information. Accordingly, we believe that tying the level of risk to "identity theft and financial harm" captures the scope of activities that consumers need to protect themselves from following a data breach. Accordingly, we urge you to consider eliminating the phrase "economic loss or harm" from the bill.

Another area that would benefit from greater clarity is the timeline for consumer notification following a data breach suffered by a third-party entity. The bill requires third-party entities to promptly notify the "covered entity." It is then unclear when the covered entity is required to notify consumers. When the covered entity itself suffers a data breach, notification occurs once the covered entity determines the scope of the breach and restores the integrity of its systems. As currently drafted, it could be construed that a covered entity, upon notification by the third-party of a breach, would need to notify its customers prior to the point in time when the third-party has determined the scope of the breach and restored the integrity of its systems. Accordingly, we recommend the Committee amend subsection 3(b)(1)(B) to read:

> Upon receiving notification from a third-party entity under subparagraph (A), a covered entity shall, *after the third-party entity has taken the necessary measures to restore the reasonable integrity, security, and confidentiality of the data system*, provide notification as required under subsection (a), unless it is agreed in writing that the third-party entity will provide such notification on behalf of the covered entity subject to the requirements of subsection (d)(3).

We also urge the Committee to eliminate the definition of "breach of security." First, the definition is confusing in that the meaning of a key phrase within it—"compromise of the security"—is itself unclear. In addition, this broad definition of "breach of security" could have negative consequences on our advocacy in foreign markets. A number of foreign governments are contemplating imposing problematic cybersecurity requirements on the technology sector, sometimes not for legitimate security reasons but rather to promote their own domestic industries. For the Congress to enact a law with a broad definition could empower other

countries to adopt the same definition with troubling results. The critical elements of this bill are to notify consumers within an appropriate period of time after the unauthorized acquisition of certain personal information that will likely result in certain harms—we believe defining a "breach of security" is not critical to this functionality. Given the potential for harmful, unintended consequences globally, we urge the Committee to eliminate this unnecessary definition, and directly tie personal information to the specific harms within subsection 3(a)(1).

Finally, the bill permits civil penalties of up to $2.5 million for each violation of section 2 (*Requirements for Information Security)* and up to $2.5 million for all violations of section 3 (*Notification of Information Security Breach)* arising from a single incident. 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 civil penalties that are five times higher than previous Congressional proposals are seemingly punitive in nature and thus not appropriate to impose on an organization that has been victimized by criminal hackers.

As ITI continues to gather feedback on the *Data Security and Breach Notification Act of 2015* 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 am happy to answer any questions you may have.

Information Technology
Industry Council

Exhibit A

Information Technology Industry Council

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.

Information Technology Industry Council
1101 K St, NW Suite 610, Washington, D.C. 20005
T +1 (202) 737-8888, www.itic.org

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.