TechAmerica

Prepared Testimony and
Statement for the Record of

Kevin M. Richards
Senior Vice President
Federal Government Affairs
TechAmerica

Before the

U.S. House Energy and Commerce Committee
Subcommittee on Commerce, Manufacturing and Trade

Hearing on

"Reporting Data Breaches:
Is Federal Legislation Needed to Protect Consumers?"

Thursday, July 18, 2013
2123 Rayburn House Office Building

INTRODUCTION

Mr. Chairman, Ranking Member Schakowsky and distinguished members of the subcommittee, thank you for convening this hearing and for bringing focus on the current state of consumer data breach notification in today's digital age. TechAmerica appreciates the opportunity to provide our insights as the Subcommittee on Commerce Manufacturing and Trade explores the effectiveness of current state data breach laws, and considers whether Congress should enact a national breach notification standard.

My name is Kevin Richards. I am the Senior Vice President for Federal Government Affairs of TechAmerica, an association representing the world's leading premiere technology companies of all sizes. TechAmerica[1] is the leading voice for the U.S. technology industry – the driving force behind productivity growth and job creation in the United States and the foundation of the global innovation economy.

We commend the subcommittee for making data breach notification a priority. This issue is a matter of great concern for our member companies that engage in global electronic commerce and provide much of the infrastructure to make e-commerce possible. Unauthorized disclosure and use of personal information erodes public confidence in the online world, and consumer notification when a breach has occurred gives consumers the knowledge and tools to protect them from possible harm.

TechAmerica and its member companies strongly support requiring entities that disclose sensitive personal information about consumers to notify consumers in appropriate circumstances, notably when there is a significant risk of harm. The question the committee is addressing today, whether federal legislation is necessary to protect consumers, is the right question to ask. State laws often vary needlessly and in some cases don't make sense. Therefore, we do believe that federal legislation is, in fact,

[1] TechAmerica is the leading voice for the U.S. technology industry – the driving force behind productivity growth and job creation in the United States and the foundation of the global innovation economy. Representing premiere technology companies of all sizes, we are the industry's only trade association dedicated to advocating for the ICT sector before decision makers at the state, federal and international levels of government. With offices in Washington, D.C., Silicon Valley, Brussels and Beijing, as well as regional offices around the U.S., we deliver our members top tier business intelligence and networking opportunities on a global scale. We are committed to expanding market opportunities and driving the competitiveness of the U.S. technology industry around the world.

necessary. However, some technology companies are not experiencing difficulties in complying with the various state data breach notification laws and for these firms a law that codifies one federal set of regulations and pre-empts state laws would be helpful, but not vital. Therefore, we believe that it is important that if Congress is going to address this issue, legislation needs to be done correctly and strike the right balance.

DATA BREACHES: ASSOCIATED BUSINESS RISKS

The rapid growth of the collection of information in electronic form has provided consumers, businesses and governments with tremendous opportunities, from revolutionizing the way medical care is provided, to enhancing government services to enabling a free internet, with more opportunities appearing daily. As Congress explores possible legislative responses to this issue, it is important to avoid any unintended consequences that legislation could have in this sensitive area.

However, this collection of data has also resulted in a concomitant exposure of companies to risks and liabilities arising from the collection, use, storage and transmission of information, particularly sensitive information about individuals.

There is a growing body of law directed at protecting personal information in the U.S. at both the state and federal levels, and in other countries, and notifying and empowering consumers with information about data breaches and the steps they can and should take to protect themselves in the event of a data breach. Many of these laws focus on the types of personal information that is often the subject of data breaches. This has likely mitigated the potential harm to consumers that may occur as a result of a data breach.

TechAmerica has been a leader in calling for a coherent, pre-emptive and meaningful national breach notification law. It is our desire in this hearing to share our experience with existing “breach notification” regimes, with the goal of providing “lessons learned” that will assist the committee in its examination of this important issue.

In the simplest terms, breach notification is one tool to respond to breaches when they occur. Breach notification requirements should also be focused on providing consumers appropriate notice about potential harm.

Any federal framework should provide for breach notification when there is, in fact, only a significant risk that identity theft has or is likely to occur. Without establishing a meaningful threshold and relevant requirements for notification, there is a very real likelihood of unintended, negative consequences for consumers, business entities and public authorities.

LESSONS LEARNED: TECHAMERICA'S POSITION ON A FEDERAL DATA BREACH LAW

TechAmerica believes that breach notifications should be required in those instances where there is a substantial risk of harm to a consumer. Federal legislation that promotes notification to consumers when their data has been compromised is needed and can effectively help restore consumers' online trust and confidence.

The first objective of federal data breach notification legislation should be to establish a uniform national standard and provide pre-emption of state laws. If a company does business in different states, they will usually notify in every state, even if their customers were not affected there and even if the state in question does not have an explicit breach notification requirement.

We urge the subcommittee to consider legislation which would provide a national data breach notification standard that creates a national standard and pre-empts the patchwork of existing state laws, while providing for safe harbor for those entities that take steps to protect their systems from breaches and render data unreadable, undecipherable, and unusable in order to protect individuals from harm.

The issue of data breach notification and when it should be provided to consumers first burst on to the scene in 2005, when ChoicePoint announced that it had compromised the records of 163,000 people and paid a record fine to the Federal Trade Commission (FTC). Since then, while Congress, the FTC and other federal

agencies have addressed various concerns about data breach notifications in fits and starts, the states and the market have taken the lead in addressing this problem.

Today, there are forty-eight different state jurisdictions in the United States[2] that have implemented data breach notification laws, and the U.S. Federal Trade Commission (FTC) is bringing actions under its existing authority[3] for failure to maintain or disclose security practices. The following recommendations are a result of the lessons learned from the implementation of these regimes and serve as a good benchmark for the drafting of potential federal legislation to ensure appropriate consumer protections:

1) **Legislation must establish a single, uniform, preemptive standard.** Any federal standard must be uniform and pre-emptive. Adding a fifty-first standard and/or layering on additional federal requirements on top of current state requirements would only add confusion, cost and risk to the system. The current patchwork quilt of current state data breach notification laws is a burdensome compliance challenge which is confusing for both businesses and consumers. One strong, uniform federal system that promotes predictability and certainty for consumers, consumer protection authorities and businesses, and reduces duplication, compliance costs and inconsistencies, is much preferable.

2) **Establish a meaningful threshold for notification.** To ensure that notification is part of a coherent approach to combating the pernicious effects of identity theft, a legal regime should require notification to consumers when the security of sensitive personal information has been breached in a manner that creates a significant risk of identity theft. The establishment of a meaningful threshold is essential as there may be direct and harmful unintended consequences that may be associated with broad notification. For example, the experiences with notification regimes to date have demonstrated that consumers have been subjected to fraud scams

[2] A generally reliable, publicly available resource that summarizes the state data breach laws has been prepared by the Perkins Coie (Law Firm), "Security Breach Notification Chart":[Link: http://www.perkinscoie.com/files/upload/PS_12_04SecurityBreachNotificationLawChart.pdf].

[3] E.g., primarily Section 5 of the FTC Act for deceptive and unfair trade practices. See, also, Children's Online Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA).

and "phishing" attacks when bad actors hear through the media about notifications, and a meaningful threshold predicated on a "significant risk" standard is essential to avoid over-notification of consumers, and minimizes the risk of fraud and identity theft that could result from consumer confusion. As former FTC Chairman Deborah Majoris has suggested, over-notification will cause "consumers [to] become numb if they are continuously notified of every breach."

3) **Define carefully the kind of personally identifiable information that is covered by notification requirements.** Central to an effective framework is a meaningful definition of "sensitive personal information" that is relevant to combating the pernicious effects of identity theft. It is essential that a careful circumscribed set of "sensitive personal information" be the basis for determining whether any notification should occur. It should not include elements that are widely used in commerce to facilitate transactions. It also makes no sense to require companies to impose additional security requirements on or notify consumers of security breaches on information that is already widely available and in the public domain.

4) **Avoid mandating specific technologies, while encouraging the adoption of good practices.** As part of the inquiry into whether "sensitive personal information" has been released in a way that may be harmful to consumers, TechAmerica urges the Committee to take into account whether the information that may have been accessed or released is usable. For example, a number of security methods and practices are available to businesses and government, including encryption, truncation, access controls, anonymization and redaction that would render any data that is breached unusable. In those instances, the requirement to notify consumers is unnecessary. To single out one method to secure data in legislation, such as encryption, suggests, if not outright mandates a de facto exclusive means to avoid notification, and creates a false sense of security. Singling out one methodology would not be in the overall best interests of the security marketplace, since it may reduce the development and use of diverse and innovative security tools.

5) **Where third parties manage data, and notification is required, avoid consumer confusion.** In cases where a 3rd party manages "sensitive personal information" of consumers for entities that own or possess sensitive personal information, notification requirements should be constructed to avoid consumer confusion. The best way to achieve this end is to obligate the third party to notify the entity that owns or licenses the data – i.e., the entity that has the relationship with the person whose sensitive personal information may have been breached. The entity that owns or licenses the sensitive personal information should, in turn, notify the end user or consumer. Otherwise, individuals are unlikely to recognize the source of the notice and thus unlikely to act in a manner to protect them, which is the object of notification regimes.

6) **A federal law should do more than the patchwork of state laws to protect consumers.** While TechAmerica believes that a uniform, national standard that protects consumers is more desirable than the current patchwork, Congress needs to be careful to ensure that any federal law that is enacted is careful to build on the experience of the states, not undermine the significant protections that consumers currently have at the state level.

CONCLUSION

In conclusion, TechAmerica believes that the "patchwork quilt" of state laws and existing requirements needs to be overhauled by a uniform, pre-emptive standard based on the risk of harm. This would be an effective addition to the significant protection that consumers receive today. Please find attached a copy of TechAmerica's National Data Breach Legislative Principles which we'd like to submit to the Record for today's hearing proceedings.

Mr. Chairman and members of the subcommittee, TechAmerica greatly appreciates the opportunity to testify today. We share the goal of the House Energy and Commerce Committee to help protect consumers and mitigate the potential harm posed by data breaches. We are happy to work with you as the legislative process moves forward.

Thank you for allowing me the privilege to appear here today in order to share TechAmerica's views on the important issue of data breach notification. I'd be happy to answer any questions that the committee may have at this time.