Prepared Testimony and

Statement for the Record of

Elizabeth Hyman

Executive Vice President, Public Advocacy

TechAmerica, the public sector and public policy department of CompTIA | CompTIA.org

Before the

U.S. House Energy and Commerce Committee

Subcommittee on Commerce, Manufacturing, and Trade

Hearing on

What Are the Elements of Sound Data Breach Legislation?

Tuesday, January 27, 2015

2123 Rayburn House Office Building

Summary

Compared to the current patchwork of state data breach notification laws, a single federal data breach notification standard will better protect consumers and allow companies to respond quickly and effectively following a breach. The key to any federal DBN law will be finding a single standard that maintains the strong consumer protections currently required by the states, but that does not overburden or impose inappropriate penalties on companies who should be focusing on notification and investigation in the wake of a breach. A federal standard should:

- Contain strong preemption language
- Avoid over-notification of consumers through
    - Requiring a significant risk of harm before notification
    - Allowing for adequate time for a risk assessment
    - A narrow definition of PII
- Avoid mandating specific technologies
- Encourage good security practices
- Forbid a private right of action

Introduction

Good morning Chairman Burgess, Ranking Member Schakowsky, and distinguished members of the Subcommittee on Commerce, Manufacturing, and Trade. Thank you for convening this hearing on the important issue of consumer data breach notification. TechAmerica appreciates the opportunity to provide our insights as the Subcommittee explores the effectiveness of current state data breach laws, and considers whether Congress should enact legislation establishing a national breach notification standard.

My name is Elizabeth Hyman, and I am the Executive Vice President of Public Advocacy for TechAmerica, the public sector and public policy department of The Computing Technology Industry Association (CompTIA). We represent over 2200 technology companies, a large number of which are small and medium-sized Information Technology companies, and are committed to expanding market opportunities and driving the competitiveness of the U.S. technology industry around the world.

We commend the Subcommittee for making consumer data breach notification a priority. This issue is a matter of great concern for both consumers and for our member companies that engage in global electronic commerce and provide much of the infrastructure to make e-commerce possible.

Technology companies take their obligations to protect consumers' information very seriously. Data is the life-blood of the Internet economy and protecting consumers' information is not only a responsibility of the industry, but also a crucial business practice. Failure to appropriately protect consumers' information will lead to a loss in customer faith and damage to a business' reputation.

Unfortunately, the reality of today's world is that criminals are constantly trying to hack into databases to steal valuable information, and despite the extensive efforts companies employ to stop such criminals, some are bound to succeed. Data breaches are sadly a part of doing business in 2015, and thus we need strong consumer protections in place to inform consumers when a harmful breach occurs, and provide the necessary information to enable consumers to take steps to protect themselves from those who may have already obtained their information.

The current state of data breach notification law, however, does not meet this goal. As you are all well aware, there currently is no federal standard for data breach notification. Instead, 47 different states (all except for Alabama, New Mexico and South Dakota), the District of Columbia, Puerto Rico, Guam and the Virgin Islands all have their own separate data breach notification laws and requirements.

With the increasingly mobile and decentralized nature of our economy and data storage and dissemination technologies, most companies are under the umbrella of multiple state laws at all times. This patchwork of state DBN laws creates significant

compliance costs since no two state data breach laws are exactly the same. Moreover, many of these state DBN laws are in conflict with each other. For example, laws may vary as to when a data breach notice is triggered, the timeline within which notice must be provided, and what must be contained in the actual notice. This complex and burdensome system is costly and inefficient, and is potentially harmful to the very consumers it seeks to protect. A federal DBN standard is thus necessary to protect consumers and ensure that companies can respond quickly and effectively after a breach.

Responding to a data breach for a company of any size is difficult. It requires a company to first ascertain if a breach has occurred, and if so, what type of data may have been compromised; whether the data contains personally identifiable information (PII); what the risk is for consumers, business partners and others; how was it compromised; has the hole been plugged; and what are next steps. Concurrently, they also have to determine if consumer data was accessed, whether the type of data that was accessed could trigger data breach notification provisions in any one of 47 states, and if so, whether they have any consumers that live in any of those states assuming they even have that information. If a company does determine that notification may be required in some states, they then need to figure out who to notify, how to notify, what information to include, and what the timelines for notification are.

Small and medium-sized businesses, which make up a large portion of our 2200 members, face particularly difficult compliance challenges. To address their obligations to resolve the breach, gather information, and notify the necessary parties, these companies often rely on cyber-insurance, help from law enforcement or payment processors, or outside counsel to help them put together and implement a data breach response plan; none of these options is cheap.

Thus, the key to any federal DBN law will be finding a single standard that maintains the strong consumer protections currently required by the states, but that does not overburden or impose inappropriate penalties on companies who should be focusing on notification and investigation in the wake of a breach.

Strong Preemption Language

Any federal data breach notification law must preempt state laws and requirements. Without strong preemption language, the entire basis for enacting a federal DBN standard disappears.

In addition to the compliance challenges already discussed, states are regularly changing and updating their DBN laws, adding yet another layer of complexity in trying to keep up with the changes. Last year, 23 different state DBN bills were introduced across the country, and this year we've already seen 17 bills introduced in 7 states in the first two weeks of the state sessions.

A federal standard needs to be *the* standard for all companies to comply with; it cannot simply become a 48th standard that states can add their own requirements atop. Overlaying more regulations on top of the existing patchwork of laws adds to the problem and does not help our companies protect consumers.

We do, however, believe that state attorneys general should be able to enforce the federal standard, as more cops on the beat helps protect consumers. But any federal standard should clearly state that companies cannot be penalized on both the state and federal levels for the same violation.

Avoid Over-notification of Consumers

It is essential that consumers only receive notification about a breach when their information has actually been accessed, and even then only when that information is likely to be used in a harmful manner. As former FTC Chairman Deborah Majoris has noted, over-notification will cause "consumers [to] become numb if they are continuously notified of every breach." Additionally, the experiences with notification regimes to date have demonstrated that consumers have been subjected to fraud scams and “phishing” attacks when bad actors hear through the media about notifications. Over-notification increases these risks.

To minimize the risk of fraud and identity theft that could result from consumer confusion due to over-notification, a federal DBN standard should contain three things: 1) Any federal framework should require consumer breach notification only when there is a *significant risk* that harm has or is likely to occur; 2) adequate time

for risk assessment; and 3) a careful definition of personally identifiable information.

Significant Risk of Harm

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. 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 sensitive personal information has been accessed in a manner that creates a significant risk of harm.

Adequate Time for Risk Assessment

When a breach is discovered, one of the first things that a company must do is to conduct a risk assessment to determine the type of data that has been accessed and the risk that potential fraudulent use of the data could entail. This risk assessment is a vital component to a company's data breach response, and, depending upon the seriousness of the breach, may take some time to complete. We therefore ask that a federal standard "starts the clock" on a notification requirement only after the risk assessment has been completed.

Short-changing the risk assessment is dangerous to the company and consumers. If a company does not have adequate time to complete a risk assessment, there is a chance that the company may not have time to adequately assess the scope of the breach or the damage caused by the breach.

If a company has inadequate time to conduct a risk assessment, it may report that credit card data or other PII may have been accessed, only to find out later that none of that data was actually accessed. This type of over-notification could lead consumers to cancel their credit cards, often at significant expense to credit unions and other credit card issuers, as well as possible inconvenience to consumers, even though it turns out that such a reaction was unnecessary.

Alternatively a company may initially inform consumers that PII was not accessed, only to find out later that it was. This could lull consumers into ignoring the later, and more important, notice, potentially subjecting themselves to risk as a result of the initial under-notification.

Instead, we believe that getting the notification right could be more beneficial to consumers than rushing to notify with potentially erroneous information.

Definition of PII

Central to an effective framework is a meaningful definition of "sensitive personally identifiable information" that is relevant to combating the pernicious effects of identity theft. It is essential that a careful circumscribed set of "sensitive personally identifiable information" be the basis for determining whether any notification should occur. For example, such a definition should not include publicly available information.

Avoid Mandating Specific Technologies and Encourage Good Practices

As part of the inquiry into whether the "sensitive personally identifiable information" obtained could be harmful to consumers, TechAmerica urges the Committee to consider whether the information accessed has been rendered unusable. 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 should be unnecessary.

Further, the legislation should exempt companies from notification requirements where data is rendered unusable.

No private rights of action

Data breaches are criminal activity, as the President's proposal to impose criminal penalties on entities that export data out of the U.S. implicitly acknowledges. Companies should not be punished for the criminal acts of others, and therefore any legislation in this space should explicitly ban private rights of action regarding data breaches and breach notification.

Conclusion

In closing, I would like to, again, thank the Subcommittee for working on the issue of data breach, which continues to put consumers at risk. Unfortunately, the patchwork of state laws, while well-intentioned, has created such a burdensome and complex compliance regime that it is now contributing to the problem; not helping to solve it. A strong, single standard that applies throughout the country will ensure

that consumers are safer and will help ensure that companies are aware of how to respond to the growing threat of data breaches.

Security and economic growth are not mutually exclusive and I would respectfully request that the solutions you draft through this Subcommittee address both through a national data breach notification standard.