Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers

House Subcommittee on Commerce, Manufacturing and Trade

July 18, 2013

Submitted by:

Dan Liutikas, Chief Legal Officer

On Behalf of

The Computing Technology Industry Association (CompTIA)
515 2nd Street, NE, Washington, DC 2002

Introduction

Good afternoon, Chairman Terry, Ranking Member Schakowsky and distinguished members of the House Subcommittee on Commerce, Manufacturing, and Trade. This testimony is submitted on behalf of the Computing Technology Industry Association (CompTIA).

My name is Dan Liutikas and I am the Chief Legal Officer of CompTIA. Prior to CompTIA, I was an attorney in private practice focusing on corporate, technology and intellectual property matters.

I am a native of Chicago, Illinois and was born to immigrant parents from Lithuania. My father learned how to fix televisions for a national retailer until eventually opening his own television repair shop and then later starting a construction business. My mother waited tables at restaurants and then started her own restaurants, delis and banquet halls. Both lived the American dream by being entrepreneurial and starting their own small businesses. From my own experience I submit that small business owners don't want handouts. They just want a fair shot at pursuing the American dream. In the context of today's hearing, that means eliminating unnecessary barriers to entry, such as redundant and burdensome regulations.

I am here today on behalf of the 2000 members of the Computing Technology Industry Association, many of whom are small business owners as well. CompTIA is a non-profit IT trade association. Our members are at the forefront of innovation and provide a critical backbone that supports broader commerce and job creation. Our membership includes computer hardware manufacturers, software developers, technology distributors, and IT specialists that help organizations integrate and use technology products and services. CompTIA is also the leading developer and provider of vendor-neutral IT workforce certifications, including A+, Security+ and Network+.

The Need for Data Breach Notification Reform

It is hard to believe that it has been 10 years since California became the first state in the country to enact a state data breach notification law. To provide some perspective, 10 years ago the majority of people accessed their digital data from desktop computers, and the mobile device industry was in its infancy. In 2002, Nokia introduced the world's first camera cell phone, and in 2003, Samsung developed the first cell phone with multiple screens. Back then the innovation was a screen on the outside of the phone to allow users to view incoming calls without having to open up their phones.[1]. Within a couple of years there will be more mobile devices than people and more people will access the

[1] http://www.hongkiat.com/blog/evolution-of-mobile-phones/.

Internet via a mobile device than desktop computers.[2].

Data breach notification standards are clearly a relevant concern for the millions of users sharing information through the Internet and for information being stored in various forms. Yet, with the increasingly mobile and decentralized nature of our economy and data storage and dissemination technologies, there is a growing and exceptionally strong case to be made for the creation of a national data breach notification framework that supersedes state data breach laws. Such an approach will bring clarity and certainty to consumers who may not be aware of the notice obligations of a particular state DBN law or even when such obligations may apply. For SMB's the issue of DBN reform is especially important because many of these firms do not have the requisite in-house expertise to thoroughly understand all 46 state DBN laws. Streamlining this process promotes robust compliance and serves as an incentive to SMB's to expand their businesses across jurisdictions.

Today, there are 46 states, not including the District of Columbia, Guam, Puerto Rico and the Virgin Islands, that have enacted data breach notifications laws. This patchwork of state DBN laws creates significant compliance obligations since no two state data breach laws are exactly the same. Moreover, many of these state DBN laws are in conflict with each other. State DBN laws vary as to when a data breach notice is triggered, the timeline within which notice must be provided, and rules that outline the information that must be contained in the actual notice.

Some state DBN laws require prima facie notice to the consumer when a company is made aware of a breach. Other state DBN laws require notice only if the breached data has the likelihood of resulting in harm to the consumer. State DBN laws also differ on the type of penalties and fines that can be imposed and whether a consumer can file a private right of action against a company that has suffered a breach of a consumer's personally identifiable information (PII).

For example, what happens when a Massachusetts resident traveling out of state shares, through use of his or her mobile device, personally identifying information with a local or regional business where they are visiting, and the business subsequently suffers a data breach. Under the Massachusetts state's DBN the consumer notice requirement applies to " a person or agency that maintains, stores, owns or licenses personal information about a resident of the Commonwealth."[3] As a result, any business across the United States that suffers a data breach containing PII belonging to a Massachusetts resident is in violation of the Massachusetts data breach law if it fails to comply with the notification requirement. This is true even if the business complies with its own state data breach notification requirement.

---

[2] http://www.businessinsider.com/more-mobile-devices-than-people-2013-2; http://www.computerworld.com/s/article/9219932/Most_will_access_Internet_via_mobile_devices_by_2015_IDC_says.

[3] Mass. Gen. Laws Ann. ch. 93H, §§ 1–6 (2007), Mass. Gen. Laws Ann. ch. 93A, § 4 (2007)

More specifically, if a Massachusetts resident happens to share their PII via a mobile device with a local business while traveling in Florida then the conflicting data breach rules become much more complicated. Under Florida's DBN law, a consumer data breach notice is not required "if, after an appropriate investigation or after consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed."[4] It should also be noted that these problems are also present when consumers access a website from their place of residence and the business is located out of state. The issue of conflicting state DBN laws still persist.

There are countless other examples that we can share that highlight the huge regulatory compliance burden imposed upon businesses due to the patchwork of conflicting state data breach notification requirements. Since each state has different notice obligations, the average consumer who becomes the victim of a PII breach faces a herculean task tracking down where the breach occurred and whether he or she should expect notice from a business with the details of the leak. Simply from a consumer protection standpoint, a federal standard would provide greater piece of mind with respect to one's PII.

These compliance obligations are particularly burdensome, however, for the small to medium size business. For example, many of CompTIA's members are comprised of just a couple of employees with very specific IT skills and core competencies.

To be clear, CompTIA fully supports the requirement that consumers receive notice when their PII has been breached. The real issue is that data breach notice obligations should not put SMB's at an economic and regulatory disadvantage as compared to larger and better-capitalized companies. The cost of complying with 46 state DBN conflicting laws places a disproportionate financial impact on SMB's.

An annual report by the Ponemon Institute (and sponsored by Symantec) found that the organizational cost for a data breach event is on average $5.4 million and the cost to an organization for a single breached record is on average $188.[5] Many of the costs associated with data breaches results from legal and regulatory liabilities.

SMB's must hire lawyers and expend other resources simply to track down the various compliance obligations. With our increasingly mobile economy the application of these laws are getting even more complicated to understand since it is not always clear about

[4] Fla. Stat. Ann. § 817.5681 (2005).
[5] http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-global-report-2013.en-us.pdf

the geographic boundaries of where a data breach may have actually occurred which can be different from where a consumer may actually reside.

Therefore, CompTIA believes that the creation of a national framework for data breach notification can go a long ways towards promoting effective consumer notice, reducing costs and eliminating barriers to entry for SMB firms. A national framework for data breach notification can serve as an incentive toward the expansion of IT services across state lines. For instance, when an IT firm considers expanding its business across state lines it must take into account the state regulatory and compliance obligations. A national framework for data breach notification would provide regulatory relief from that obligation.

Any national data breach notification framework should incorporate the following principles, which we also believe would receive broad industry support:

1. Preemption of State Legislation – There should be a single national federal standard for Data Breach policy. Businesses which conduct commerce over multiple states need the certainty and efficiency that a national standard would provide.

2. Technology-Neutral policy – Congress and the FTC should not mandate specific technology or methods for data security practices. The environment for data security is constantly evolving, so any regulation should focus on promoting validated industry standards for security, rather than a single quickly-outdated solution.

3. Exemption from notification requirement for entities that deploy technology/methods such as encryption and other technologies that render data "unusable or unreadable" by hackers as a harm-prevention measure.

4. No Private Right of Action for individuals seeking litigation. All enforcement and penalties for Data Breach law should be administrated by a central government agent instead of state Attorneys General, except in cases where the federal agent can or has not acted.[6]

5. Focus on gaps in coverage - Entities compliant with existing Data Breach legislation (Ex. Gramm-Leach-Bliley) should be exempt from new regulation. Do not reinvent the wheel, or create conflicting and overlapping regulations.

[6] CompTIA believes that the industry will not support criminal prosecution for "negligent" actions.

6. Avoid over-notification of consumers – Notification should occur on a "reasonable timeframe," which includes allowances for risk assessment and any necessary law enforcement procedures or investigation. Notification should be focused on events where there is a possibility of "actual harm." Possibility of including a minimum threshold of affected individuals.

Thank you again for the opportunity to share our perspective on the issue of data breach notification reform, and I would be happy to answer any questions.

Public Advocacy
515 2nd St NE
Washington, DC 20002
202-503-3624