



March 17, 2015

The Honorable Michael Burgess
Chairman, Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
2336 Rayburn House
Washington D.C. 20515

The Honorable Jan Schakowsky
Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
237 Cannon HOB
Washington, D.C. 20510

Re: Comments on Discussion Draft "Data Security and Breach Notification Act of 2015"

Dear Chairman Burgess and Ranking Member Schakowsky,

The Online Trust Alliance (OTA) submits this letter in advance of the March 18, hearing being held by the Commerce, Manufacturing, and Trade Subcommittee on the recent draft "Data Security and Breach Notification Act," authored by Representatives Blackburn and Welch.

We commend the Subcommittee for recognizing the need to develop meaningful legislation to help protect consumers from the onslaught of data breaches and negligent data protection practices, which risk considerable harm to consumers. Indeed, for the 15th consecutive year - identity theft is the top category of consumer complaints made to the Federal Trade Commission (the "Commission"), **underscoring the need for legislation requiring responsible data security practices along with timely and actionable notices of a data breach.**¹

OTA and our members have deep experience in this subject matter, and based upon our experiences, have identified several areas for enhancement and clarification of the draft bill. These comments follow OTA's letter dated March 3, 2015, to the House Committee on Commerce, Science, and Transportation, concerning draft data breach legislation. (Attached).

¹ <https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer-complaint-categories-again-2014>

We believe a single Federal law pre-empting the patchwork of 47 State laws will benefit consumers and business alike, by providing clarity and a single standard definition of privacy, notification requirements and reasonable security requirements. **However, any federal data breach notification law must be sufficiently robust, while not unduly burdening businesses committed to protecting consumers and their data.**

Consumers today are becoming jaded and risk being overwhelmed by the sheer volume of data breach notices. Often, these notices are unclear, not prescriptive nor timely. **It is critical that any federal data breach legislation recognize that for each day a consumer is not provided actionable notification, the risk of victimization grows.**

Below is a summary of key points which we believe are essential for an effective and balanced federal data breach notification law, to pre-empt existing state laws.

- 1. Covered Data** – As written, the scope of the Act only covers electronic data. However, an organization’s accidental loss or discarding of paper records containing personal information impacts consumers in the same fashion as an electronic breach. A paper data loss can result in “dumpster diving” and identity theft. In many cases, the paper data loss of consumer information can be more impactful, especially where tax returns, W-2s, bank statements, or other financial data are involved. With this in mind, we recommend that the bill be amended to include covered data in any form, whether electronic or paper.^{2,3}
- 2. Section 2 Requirements** – **OTA’s independent analysis shows that more than 90% of breaches that occurred in 2014 could have been prevented and contained by adoption of best practices.** OTA agrees with the concept in the draft bill that covered entities must maintain reasonable security measures to protect and secure personal information. While there is no perfect security, prevention is only one facet of data protection. As outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity, covered entities must also deploy processes to help detect a data loss incident, as well as formulate measures to contain and minimize the impact of a data breach incident.⁴ Equally as important, a covered entity must have an up-to-date data breach response plan. All too often we have witnessed organizations failing to have such a plan, delaying timely notices to the consumer. The draft bill should be amended to include these requirements and to afford “safe harbor” treatment from violations and fines for those entities who can demonstrate they have implemented said best practices in their respective areas.

² <http://recode.net/2015/03/10/dumpster-divers-could-be-the-next-sony-hackers/>

³ <http://www.click2houston.com/news/tax-documents-found-in-dumpster/30932828>

⁴ <http://www.nist.gov/cyberframework/index.cfm>

- 3. Notification** – There are three primary facets of notification that are required to maximize consumer protection and help defend our nation from cybercrime. These are: (1) regulatory authorities (the Commission), (2) law enforcement, and (3) consumers and other impacted parties (e.g. partners, investors, etc.). Section 3(a)(3) specifies a “covered entity shall as expeditiously as possible notify the Commission and the Secret Service or the Federal Bureau of Investigation.” Based on recent notifications that have lagged upwards to six months or greater, it is recommended that the draft bill specify notice to the Commission and Law Enforcement be within seventy-two hours (3 business days) after discovery of a breach or data loss incident involving personal information. It is recognized the full impact of the incident may not be known and the reporting entity will likely revise their findings, but delaying notification until an internal investigation is complete impedes the efforts of the law enforcement community and first responders.
- 4. Non-Profit Entities** - As written, the draft bill only addresses 501(c)(3) charitable organizations and reduces their notification requirement. OTA strongly believes all non-profit organizations should be classified as covered entities. We have witnessed trade organizations, religious organizations, and others experiencing data breaches resulting from insecure storage of personal information.^{5 6} All organizations that hold and collect personal information must be held to the same standards for both protecting covered data and providing notifications.
- 5. Method and Content of Notifications** – The draft bill in Section 3(d)(1)(ii)(III) recognizes that data breach notifications should be constructed so they do not become an attack vector, by not containing any hyperlinks. It is important to recognize there are other measures that must be in place as well to help prevent consumers from receiving dubious and look-a-like notices, as experienced in the recent Target breach. In the absence of rulemaking provisions for the Federal Trade Commission, it is recommended this section be expanded to include two critical requirements: 1) notices should only come from the recognizable domain and consumer facing brand of the covered entity; and 2) the covered entity must implement anti-spoofing and phishing standards to aid internet service providers and receiving networks to help detect and block phishing and malicious email.^{7, 8, 9}
- 6. Content of Notification** – Notifications that include detailed information are extremely important to aid consumers to be able to take action to protect themselves. Section 3(b) should add an additional provision requiring the notification to include the physical location of the breach, if known. For example in last summer’s Jimmy Johns breach, the precise location and date of the incident was made known to customers. Providing this information enabled Jimmy John’s customers to quickly determine if their credit card was compromised.

⁵ <http://www.komonews.com/news/local/Victims-of-IRS-tax-fraud-continues-to-grow-250407271.html>

⁶ <http://www.net-security.org/secworld.php?id=13669>

⁷ <http://mainsleaze.spambouncer.org/target-spams-email-appended-list-with-data-breach-notice/>

⁸ Email Authentication Best Practices <https://otalliance.org/eauth>

⁹ <https://otalliance.org/EmailAudit>

The draft bill should be amended to state when known, the physical location(s) should be included and disclosed to the consumer in the notification.¹⁰

- 7. Notice Requirement of Service Providers** - Timely notification by service providers to covered entities is critical. As businesses are becoming more reliant on service providers, this risk is increasing, yet there is no such standard notification timetable for service providers. **Service providers often do not know the types of data they are holding, have access to the data and/or may be contractually prohibited to know what data they may be holding.** In the absence of this knowledge, they do not know if they need to notify the customer unless it has been contractually stipulated. For this reason, it is recommended service providers be required to notify the covered entity within forty-eight hours of the detection of a breach, data loss or possible incident impacting the service they are providing to a covered entity.
- 8. Covered Data** – The draft bill in Section 5(A)(iii) does not appear to include in the definition of personal information unique identifiers related to email, social networking accounts, dating, and other online services. The breach of these kinds of accounts can be drivers of identity theft and phishing. To maximize consumer protection, it is recommended the section be clarified to include any log-in credentials including a unique account identifier and associated security code, access code, password, or biometric data unique to an individual. Highlighting the importance of this clarification is the use of federated ID mechanisms outlined by the National Strategy for Trusted Identities in Cyberspace (NSTIC)¹¹ and federated sites using Facebook login credentials.¹² As defined in the draft bill, it is unclear if these account identifiers and security codes would be covered. To maximize consumer protection and harmonize with existing state breach laws, such accounts and credentials must be covered.
- 9. Sharing of investigative Data with Law Enforcement** - The draft bill does not provide any safe harbor for covered entities that share investigative reports or forensic data with law enforcement. The lack of a safe harbor from federal or state laws risk can impede the sharing of this critical information and threat intelligence. When such sharing is used exclusively for law enforcement investigative purposes it should not constitute a violation of federal or state law as well as a covered entity’s privacy policy. Sharing forensic data as soon as possible can be invaluable to aiding law enforcement to help protect others and ultimately bring criminals to justice. Thus, the sharing of such data, including investigative reports and forensic data, should be encouraged through appropriate protections in breach legislation.

¹⁰ <https://www.jimmyjohns.com/datasecurityincident/>

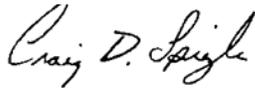
¹¹ <http://www.nist.gov/nstic/>

¹² <https://developers.facebook.com/docs/facebook-login/v2.2>

10. Maximum Total Liability – The draft bill in Section 4 imposes an unreasonably low penalty amount for violations which could not be reasonably expected to deter misconduct or redress tangible harms to consumers. We recommend that covered entities who fail to comply with Section 2 and are unable to demonstrate they have implemented reasonable security to help prevent, detect and contain an incident, should have a maximum civil penalty for each violation not to exceed \$20,000,000. This would be consistent with recent breach related settlements with multiple State Attorneys General.¹³

In summary, OTA applauds the Subcommittee in taking leadership in this critical area. We look forward to working with members in developing effective legislation that maximizes consumer protection, promotes innovation and aids in fighting cybercrime.

Sincerely,



Craig D. Spiegle
Executive Director and President
Online Trust Alliance
Craigs@otalliance.org
+1 425-455-7400

cc: House Commerce, Manufacturing and Trade Committee Members

¹³ http://www.dispatch.com/content/stories/business/2009/06/23/tjmax_settlement.html



March 3, 2015

Chairman Fred Upton
U.S. House of Representatives Energy & Commerce Committee
2183 Rayburn House
Washington D.C. 20515

Ranking Member Frank Pallone, Jr.
U.S. House of Representatives
237 Cannon HOB
Washington, D.C. 20510

Re: Proposed Data Breach Notification Legislation

Dear Chairman Upton and Ranking Member Pallone:

The Online Trust Alliance (OTA), a 501c3 non-profit with the mission to enhance online trust and promote innovation, submits the following in response to the recently announced Personal Data Notification & Protection Act and several related draft legislative proposals.

OTA represents over 100 organizations committed to the development and advancement of best practices, meaningful self-regulation, data stewardship and balanced legislation. Last month, OTA released its 2015 Data Protection & Breach Readiness Guide developed through feedback from over 100 security and privacy professionals, and held four town halls around the United States where over 500 attendees provided input concerning the various data breach notification proposals. America's leadership is being threatened and data breaches are a challenge to national security, the economic prosperity of our nation, and most importantly, to the privacy and financial protection of our citizens.

Below is a summary of six key points and provisions which we believe are important considerations for an effective and balanced federal data breach notification law.

First, any federal data breach notification law must preempt the existing 47 state laws imposing a myriad of data breach notification obligations. State breach laws are a complex web of varied timing and notification requirements, and are a difficult mish-mash for an inter-state business to navigate during the challenge of responding to a data breach incident. Similar to the single data breach notification requirement in the EU, a single federal law will provide

businesses, consumers and regulators with clarity and simplicity concerning data breach notification obligations and provide a level playing field for all consumers – no matter their state of residence. However, any federal data breach notification law must be robust and not provide lesser protections than under existing state laws while not unduly burdening businesses.

Second, any federal data breach notification law must contain a safe harbor from regulator penalties for those businesses or organizations that can demonstrate a commitment to the adoption of best security and privacy practices. While it is important to recognize there is no perfect security, OTA's analysis of data shows that more than 90% of breaches that occurred in 2014 could have been prevented by adoption of best practices. A safe harbor from penalties for self-certified adoption of best practices would strongly encourage businesses to adopt best practices when they are most needed - in advance of a breach.

Third, any federal data breach notification law must contain a State right of enforcement. Similar to the Children's Online Privacy Protection Act (COPPA) and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), a state right of enforcement not only permits a state to protect its own citizens, but also allows states to complement the overburdened federal regulators by pursuing those companies and organizations that fail to live up to their data breach obligations. States have a strong interest in protecting their own citizens and a federal data breach notification law with a State right of enforcement would recognize and embrace this interest.

Fourth, any federal data breach notification law must contain an appropriate coverage of personal information triggering notification obligations. This is critical to ensure consumers are notified in a timely manner and for those breaches they need to know about, and are not over notified. If notifications become commonplace, consumers will get lost in the noise and likely not take appropriate action. Thus, the definition of what data is covered must be balanced and appropriate, must include paper records, and due to the common reuse of passwords by consumers across their numerous accounts – must include coverage for email/username address and passwords. A user's email address and password are essentially the keys to their online kingdom, permitting access to social and financial websites, either directly or through a master account password reset.

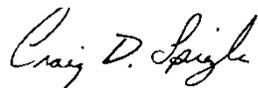
Fifth, timely notice is critical to not only consumers, but also to regulatory authorities and law enforcement agencies. Businesses should be required to notify the FTC, FCC or other primary regulatory within seventy-two hours after discovering a breach involving covered data. Since the window of consumer victimization begins within days of a breach, it is critical that businesses notify consumers as soon as possible - but no later than 30 days after a breach. While breach investigations are complex and take time, they often identify additionally impacted consumers weeks later. With this in mind, any data breach legislation must provide for a rolling period of notification not to exceed 30 days after discovery that a consumer's personal information has been breached.

Sixth, any data breach legislation must permit businesses to share investigative forensics reports and related data with any law enforcement agencies investigating a breach. This sharing should not constitute a breach under the legislation nor impact any privilege or protections belonging to a business. Sharing forensic reports and data as soon as possible concerning a breach and attempted breach can be invaluable to help protect others and bring attackers to justice, or should be encouraged through appropriate protections in any data breach legislation.

OTA applauds Congress and the President for taking leadership in this critical area. As an individual's online worlds grows and expands, as our next generations spend more and more time socializing, communicating, gaming, shopping, banking, and researching online, so must the protections afforded to them.

We look forward to working with your staff and colleagues in the developing effective legislation which maximizes consumer protection and promotes innovation and fight the threats which our undermining the interest and our economy.

Sincerely,



Craig D. Spiegle
Executive Director and President
Online Trust Alliance
Craigs@otalliance.org
+1 425-455-7400