TechAmerica

TechAmerica.org

TechAmerica
601 Pennsylvania Avenue, NW
Suite 600, North Building
Washington, DC 20004
P 202.682.9110

Prepared Testimony and
Statement for the Record of

Mark Bregman
Chief Technology Officer
Symantec Corporation

On Behalf of
Symantec Corporation
and
TechAmerica

Before the

U.S. Senate Committee on Commerce, Science and Transportation
Subcommittee on Consumer Protection, Product Safety and Insurance

Hearing on

S. 3742, The Data Security and Breach Notification Act of 2010

September 22, 2010
252 Russell Senate Office Building

INTRODUCTION

Chairman Pryor, Ranking Member Wicker, Members of the Committee, good afternoon. Thank you very much for the opportunity to testify here today. My name is Mark Bregman and I am the Chief Technology Officer at Symantec Corporation. I will be testifying here today on behalf of TechAmerica.

Symantec[1] is the world's Information security leader with over 25 years of experience in developing Internet security technology. Today we protect more people and businesses from more online threats than anyone in the world. Symantec's best-in-class Global Intelligence Network[2] allows us to capture worldwide security intelligence data that gives us an unparalleled view of emerging cyber attack trends. We utilize over 240,000 attack sensors in 200 countries to track malicious activity 24 hours a day, 365 days a year. In short, if there is a class of threat on the Internet, Symantec knows about it.

TechAmerica[3] is the leading voice for the U.S. technology industry, which is the driving force behind productivity, growth and job creation in the United States, as well as the foundation of the global innovation economy. Representing approximately 1,500 member companies of all sizes, along with their millions of employees from the public and commercial sectors, TechAmerica is the industry's largest advocacy organization.

Further, TechAmerica's CxO Council is the only advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. The Council is led by CEOs of the world's top security providers who offer the technical expertise, depth and focus needed to encourage a better understanding of security issues. A comprehensive approach to ensuring the security and resilience of information systems is fundamental to global protection, national security and economic stability.

THE RECENT PROLIFERATION OF DATA BREACHES

TechAmerica appreciates the opportunity to discuss the serious issue of data security. For organizations that have critical information assets such as customer data, intellectual property, trade secrets, and proprietary corporate data, the risk of a data breach is now higher than ever before. In fact, more electronic records were breached in 2008 than in the previous four years combined.[4]

[1] Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

[2] Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec Global Intelligence Network. This network captures worldwide security intelligence data that gives Symantec analysts unparalleled sources of data to identify, analyze, deliver protection and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. More than 240,000 sensors in 200+ countries monitor attack activity through a combination of Symantec products and services as well as additional third-party data sources.

[3] TechAmerica is the technology industry's only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). TechAmerica was formed by the merger of AeA (formerly the American Electronics Association), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics & Information Association (GEIA).

[4] Verizon Business Risk Team, 2009 Data Breach Investigations Report

Identity theft continues to be a high-profile security issue. In a recent survey, 65 percent of U.S.-based poll respondents said that they were either "very concerned" or "extremely concerned" about identity theft.[5] Furthermore, 100 percent of enterprise-level respondents surveyed for the Symantec *State of Enterprise Security Report 2010* experienced loss or theft of data.[6] The danger of data breaches is of particular importance for organizations that store and manage large amounts of personal information. Not only can compromises that result in the loss of personal data undermine customer and institutional confidence, result in costly damage to an organization's reputation, and result in identity theft that may be costly for individuals to recover from, they can also be financially debilitating to organizations.[7] In 2009, the average cost per incident of a data breach in the United States was $6.75 million, which is slightly higher than the average for 2008. Considering that the average cost per incident has also been rising in recent years (having risen from $4.5 million in 2005, for example), it is reasonable to assume that average costs will continue to rise in coming years. Reported costs of lost business ranged from $750,000 to $31 million.[8]

Over the past several years, the frequency and severity of significant database security breaches has increased dramatically as well as the costs of responding to such incidents. One recent survey found that nearly 80 to 90 percent of Fortune 500 companies and government agencies have experienced security breaches. The stakes are high for consumers and getting higher all the time. Hardly a week passes without a news story about the theft of personal data from a computer database of a major company or organization. According to the Privacy Rights Clearinghouse, since 2005, over 365 million records containing sensitive personal information have been exposed by database breaches at companies and organizations that keep such information.

The Identity Theft Resource Center (ITRC) reports that the number of personal records --data such as Social Security numbers, medical records and credit card information tied to an individual--that hackers exposed has skyrocketed to 220 million records in 2009, compared with 35 million in 2008. That represents the largest collection of lost data on record. Symantec's *2010 Internet Security Threat Report* also found that 60 percent of the data records exposed were compromised as a result of hacking, up from 22 percent in 2008.

WHY DATA BREACHES HAPPEN

While the continuing onslaught of data breaches is well documented, what is far less understood is why data breaches happen and what can be done to prevent them. In order to prevent a data breach, it is essential to understand why they occur. Third-party research into the root causes of data breaches, gathered from the Verizon Business Risk Team[9] and the Open Security Foundation,[10] reveals three main types: well-meaning insiders, targeted attacks, and malicious insiders. In many cases, breaches are caused by a combination of these factors. For example, targeted attacks are often enabled inadvertently by well-meaning insiders who fail to comply with security policies, which can lead to a breach.[11]

[5] http://arstechnica.com/security/news/2009/10/americans-fear-online-robberies-more-than-meatspace-muggings.ars
[6] http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf
[7] http://www.wired.com/threatlevel/2009/11/pos?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+wired%2Findex+%28Wired%3A+Index+3+%28Top+Stories+2%29%29
[8] http://www.encryptionreports.com/download/Ponemon_COB_2009_US.pdf
[9] Ibid.
[10] http://datalossdb.org/
[11] Verizon Business Risk Team, op. cit.

WELL-MEANING INSIDERS

Company employees who inadvertently violate data security policies represent the largest population of data breaches. According to the Verizon report, 67 percent of breaches in 2008 were aided by "significant errors" on the part of well-meaning insiders.[12] In a 2008 survey of 43 organizations that had experienced a data breach, the Ponemon Institute found that over 88 percent of all cases involved incidents resulting from insider negligence.[13] An analysis of breaches caused by well-meaning insiders yields five main types:

- **Data exposed on servers and desktops.** Daily proliferation of sensitive information on unprotected servers, desktops, and laptops is the natural result of a highly productive workforce. Perhaps the most common type of data breach occurs when well-meaning insiders, unaware of corporate data security policies, store, send, or copy sensitive information unencrypted. In the event a hacker gains access to a network, confidential files stored or used without encryption are vulnerable and can be captured by hackers. As a result of data proliferation, most organizations today have no way of knowing how much sensitive data exists on their systems. Systems that held data the organization did not know was stored on them accounted for 38 percent of all breaches in 2008—and 67 percent of the records breached.[14]

- **Lost or stolen laptops.** The 2008 Ponemon Institute study found that lost laptops were the top cause of data breaches, representing 35 percent of organizations polled.[15] In a typical large enterprise, missing laptops are a weekly occurrence. Even when such cases do not result in identity theft, data breach disclosure laws make lost laptops a source of public embarrassment and considerable expense.

- **Email, web mail, and removable devices.** Risk assessments performed by Symantec for prospective customers show that on average approximately one in every 400 email messages contains unencrypted confidential data.[16] Such network transmissions create significant risk of data loss. In a typical scenario, an employee sends confidential data to a home email account or copies it to a memory stick or CD/DVD for weekend work. In this scenario, the data is exposed to attack both during transmission and on the potentially unprotected home system or removable media device.

- **Third-party data loss incidents.** Business relationships with third-party business partners and vendors often require the exchange of confidential information such as with a 401(k) plan, outsourced payment processing, supply chain order management, and many other types of operational data. When data sharing is overly extensive or when partners fail to enforce data security policies, the risk of data breaches increases. The Verizon report implicated business partners in 32 percent of all data breaches.[17]

- **Automated business processes.** One reason for proliferation of confidential data is that inappropriate or out-of-date business processes automatically distribute such data to unauthorized individuals or unprotected systems, where it can be easily captured by hackers or stolen by malicious insiders. Onsite

[12] Ibid.
[13] Ponemon Institute, 2008 Annual Study: Cost of a Data Breach, February 2009
[14] Verizon Business Risk Team, op.cit.
[15] Ponemon Institute, op.cit.
[16] Symantec Data Loss Prevention Risk Assessments
[17] Verizon Business Risk Team, op. cit.

risk assessments by Symantec find that in nearly half of these cases, outdated or unauthorized business processes are to blame for exposing sensitive data on a routine basis.

TARGETED ATTACKS

In today's connected world—where data is everywhere and the perimeter can be anywhere—protecting information assets from sophisticated hacking techniques is an extremely tough challenge. Driven by the rising tide of organized cyber-crime, targeted attacks are increasingly aimed at stealing information for the purpose of identity theft. More than 90 percent of records breached in 2008 involved groups identified by law enforcement as organized crime.[18] Such attacks are often automated by using malicious code that can penetrate into an organization undetected and export data to remote hacker sites.

What makes large scale data breaches so dangerous is that modern organized crime has developed efficient mechanisms for the sale and wide spread distribution of large quantities of identities and personal financial information. In 2008, Symantec created more than 1.6 million new malicious code signatures—more than in the previous 17 years combined—and blocked on average 245 million attempted malicious code attacks worldwide per month.[19] Measured by records compromised, by far the most frequent types of hacker attacks in 2008 were unauthorized access using default or shared credentials, improperly constrained access control lists (ACLs), and Structured Query Language (SQL) injection attacks.[20] In addition, 90 percent of lost records were attributed to the deployment of malware.[21] The first phase of the attack, the initial incursion, is typically perpetrated in one of four ways:

- **System vulnerabilities.** Many times laptops, desktops and servers do not have the latest security patches deployed, which creates a gap in an overall security posture. Gaps or system vulnerabilities can also be created by improper computer or security configurations. Cybercriminals search for and exploit these weaknesses in order to gain access to the corporate network and confidential information.

- **Improper credentials.** Passwords on Internet-facing systems such as email, Web, or FTP servers are often left on factory default settings, which are easily obtained by hackers. Under-constrained or outdated ACLs provide further opportunities for both hackers and malicious insiders.

- **Structured Query Language (SQL) injection.** By analyzing the URL syntax of targeted websites, hackers are able to embed instructions to upload spyware that gives them remote access to the target servers.

- **Targeted malware.** Hackers use spam, email and instant message communications often disguised as being from known entities to direct users to websites that are compromised with malware. Once a user visits a compromised website, malware can be downloaded with or without the user's knowledge. Gimmicks such as *free software* often deceive users into downloading spyware that can be used to monitor user activity on the web and capture frequently used credentials such as corporate logins and passwords. Remote access tools (RATs) are an example of spyware that is automatically downloaded to

[18] Ibid
[19] Symantec Internet Security Threat Report XIV
[20] Verizon Business Risk Team, op. cit.
[21] Ibid

a user's machine without their knowledge, silently providing the hacker control of the user's computer and access to corporate information from a remote location.

THE MALICIOUS INSIDER

Malicious insiders constitute drivers for a growing segment of data breaches, and a proportionately greater segment of the cost to business associated with those breaches. The Ponemon study found that data breaches involving negligence cost $199 per record, whereas those caused by malicious acts cost $225 per record.[22] Breaches caused by insiders with intent to steal information fall into four groups:

- **White collar crime.** The employee who knowingly steals data as part of an identity theft ring has become a highly notorious figure in the current annals of white collar crime. Such operations are perpetrated by company insiders who abuse their privileged access to information for the purpose of personal gain.

- **Terminated employees.** Given the current economic crisis—where layoffs are a daily occurrence—data breaches caused by disgruntled former employees have become commonplace. Often, the employee is notified of his or her termination before entitlements such as Active Directory and Exchange access have been turned off, leaving a window of opportunity for the employee to access confidential data and email it to a private account or copy it to removable media. A recent study of the effects of employee terminations on data security revealed that 59 percent of ex-employees took company data, including customer lists and employee records.[23]

- **Career building with company data.** It is common for an employee to store company data on a home system in order to build a library of work samples for future career opportunities. While the motives for such actions may not be considered malicious on the order of identity theft, the effect can be just as harmful. If the employee's home system is hacked and the data stolen, the same damage to the company and its customers can ensue.

- **Industrial espionage.** The final type of malicious insider is the unhappy or underperforming employee who plans to defect to the competition and sends examples of his or her work to a competing company as part of the application and review process. Product details, marketing plans, customer lists, and financial data are all liable to be used in this way.

DATA BREACHES THAT COULD LEAD TO IDENTITY THEFT, BY SECTOR

Using publicly available data, Symantec was able to determine the sectors that were most often affected by breaches and the most common causes of data loss.[24] Using the same data, we also explored the severity of each breach in question by measuring the total number of identities exposed to attackers.[25]

[22] Ponemon Institute, op. cit.

[23] Ponemon Institute, "Data Loss Risks During Downsizing: As Employees Exit, So Does Corporate Data," 2008

[24] Open Security Foundation (OSF) Dataloss DB, see http://datalossdb.org

[25] An identity is considered to be exposed if personal or financial data related to the identity is made available through the data breach.

It should be noted that some sectors might need to comply with more stringent reporting requirements for data breaches than others. For instance, government organizations are more likely to report data breaches, either due to regulatory obligations or in conjunction with publicly accessible audits and performance reports.[26] Conversely, organizations that rely on consumer confidence may be less inclined to report such breaches for fear of negative consumer, industry, or market reaction. As a result, sectors that are not required or encouraged to report data breaches are consistently under-represented.

The education sector accounted for the highest number of known data breaches that could lead to identity theft, accounting for 20 percent of the total. This was a decrease from 27 percent in 2008, when the education sector also ranked first. Institutions in the education sector often store a wide range of personal information belonging to students, faculty, and staff. This information may include government-issued identification numbers, names, or addresses that could be used for identity theft. Finance departments in these institutions also store bank account information for payroll purposes and may hold credit card information for people who use this method to pay for tuition and fees.

Educational institutions are faced with the difficult task of standardizing and enforcing security across dispersed locations, as well as educating everyone with access to the data on the security policies. This may increase the opportunities for an attacker to gain unauthorized access to data because there are multiple points of potential security weakness or failure.

Although the education sector accounted for the largest percentage of data breaches in 2009, those breaches accounted for less than 1 percent of all identities exposed during the reporting period and ranked fourth. This is similar to 2008, when a significant percentage of breaches affected the education sector, but only accounted for 4 percent of all identities exposed that year. This is mainly attributed to the relatively small size of databases at educational institutions compared to those in the financial or government sectors. Each year, even the largest universities in the United States only account for students and faculty numbering in the tens of thousands, whereas financial and government institutions store information on millions of people.[27] As such, data breaches in those sectors can result in much larger numbers of exposed identities.

In 2009, the health care sector ranked second, accounting for 15 percent of data breaches that could lead to identity theft. In 2008, this sector also accounted for 15 percent, but ranked third. This rise in rank is most likely due to the decreased percentage of breaches that could lead to identity theft in the government sector. The health care sector accounted for less than 1 percent of exposed identities in 2009—a decrease from 5 percent in 2008. Like the education sector, health care institutions store data for a relatively small number of patients and staff compared to some organizations in the financial and government sectors.

Additionally, health care organizations often store information that may be more sensitive than that stored by organizations in other sectors and this may be a factor in the implementation of certain regulatory measures. For instance, as of 2010, greater responsibility for data breaches will be enforced for health care organizations in

[26] Please see http://www.privacyrights.org/fs/fs6a-facta.htm and http://www.cms.hhs.gov/HealthPlansGenInfo/12_HIPAA.asp
[27] http://www.osu.edu/osutoday/stuinfo.php

United States because of regulations introduced by the Health Information Technology for Economic and Clinical Health Act (HITECH).[28]

The government sector accounted for 13 percent of breaches that could lead to identity theft in 2009 and ranked third. This is a decrease from 20 percent in 2008, when the government sector ranked second. Although the percentage of these breaches has decreased in recent years, they account for a larger percentage of exposed identities. In 2009, data breaches in the government sector exposed 35 percent of reported identities exposures, an increase from 17 percent in 2008.

The increase in percentage of identity exposures in the government sector is primarily due to a breach attributed to insecure policy from the National Archives and Records Administration in the United States.[29] A faulty hard drive containing unencrypted personal information on 76 million military veterans was sent to a third-party electronics recycler without first removing the data. This was the largest ever exposure of personal information by the United States government. Earlier in 2009, another hard drive belonging to the National Archives and Records Administration was either lost or stolen; it is believed to have contained highly sensitive information about White House and Secret Service operating procedures, as well as data on more than 100,000 officials from the Clinton administration.[30]

The financial sector was subject to one of the most notable data breaches reported in 2009. This sector ranked fifth for breaches with 10 percent of the total, but accounted for the largest number of identities exposed with 60 percent. The majority of this percentage was the result of a successful hacking attack on a single credit card payment processor.[31] The attackers gained access to the company's payment processing network using an SQL-injection attack. They then installed malicious code designed to gather sensitive information from the network on the compromised computers, which also allowed them to easily access the network at their convenience. The attack resulted in the theft of approximately 130 million credit card numbers. An investigation began when the company began receiving reports of fraudulent activity on credit cards that the company itself had processed. The attackers were eventually tracked down and charged by federal authorities.

Notably, one of the hackers was Albert "Segvec" Gonzalez, who had been previously convicted of other attacks. He plead guilty to 19 counts of conspiracy, wire fraud and aggravated identity theft charges in March 2010 and was sentenced to serve up to 25 years in prison. He had also worked as an FBI informant at one point, providing information about the underground economy.[32] These attacks and the events surrounding them are referenced in the Symantec *Report on the Underground Economy*.[33]

This attack is evidence of the significant role that malicious code can play in data breaches. Although data breaches occur due to a number of causes, the covert nature of malicious code is an efficient and enticing means for attackers to remotely acquire sensitive information. Furthermore, the frequency of malicious code

[28] http://findarticles.com/p/articles/mi_hb4365/is_21_42/ai_n47569144/
[29] http://www.wired.com/threatlevel/2009/10/probe-targets-archives-handling-of-data-on-70-million-vets/
[30] http://fcw.com/Articles/2009/05/20/Web-NARA-missing-hard-drive.aspx
[31] http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html
[32] See http://www.wired.com/threatlevel/2009/12/gonzalez-heartland-plea/ and http://yro.slashdot.org/article.pl?sid=10/03/26/124256
[33] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

threats that expose confidential information, underscores the significance of identity theft to attackers who author and deploy malicious code.

PRACTICAL SECURITY CONSIDERATIONS TO AVOID A SECURITY BREACH

While a company's information security system may be unique to its situation, there are recognized basic components of a comprehensive, multi-layered program to protect personal information from unauthorized access. At the outset, companies should review their privacy and security policies and inventory records systems, critical computing systems, and storage media to identify those containing personal information.

It is important to categorize personal information in records systems according to sensitivity. Based on those classifications, physical and technological security safeguards must be established to protect personal information, particularly higher-risk information such as Social Security numbers, driver's license numbers, financial account numbers, and any associated passwords and PIN numbers, as well as health information. This involves establishing policies that provide employees with access to only the specific categories of personal information their job responsibilities require, use technological means to restrict access to specific categories of personal information, monitor employee access to higher-risk personal information, and remove access privileges of former employees and contractors immediately.

Companies should promote awareness of security and privacy policies through ongoing employee training and communications. They should also require third-party service providers and business partners that handle personal information on behalf of the company to follow specified security procedures. This can be accomplished by making privacy and security obligations of third parties enforceable by contract. Internally, companies must employ the use of intrusion-detection technology to ensure rapid detection of unauthorized access to higher-risk personal information and, wherever feasible, must use data encryption, in combination with host protection and access control, to protect sensitive information. Data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard. Companies should also dispose of records and equipment containing personal information in a secure manner, such as shredding paper records and using a program to "wipe" and overwrite the data on hard drives.

TECHAMERICA'S FEDERAL DATA SECURITY LEGISLATIVE PRINCIPLES

TechAmerica believes that consumers should have confidence that any personal information they provide to government agencies or business entities will remain private and secure, and we consider privacy and security to be key components of business operations for the public and private sectors. We have advocated for three essential elements to any data security and breach notification bill:

1. **Data security legislation should apply equally to all.** The scope of the legislation should include all entities that collect, maintain, or sell significant numbers of records containing sensitive personal information. Requirements should impact government and the private sector equally, and should include educational institutions and charitable organizations as well.

2. **Implementing pre-breach security measures should be central to any legislation.** An ounce of prevention is worth a pound of cure. New legislation should not simply require notification of consumers in case of a data breach. It should also require reasonable security measures to ensure

the confidentiality and integrity of sensitive personal information in order to minimize the likelihood of a breach. New legislation should not direct the creation of new standards, but draw upon existing standards set out under Gramm-Leach-Bliley, the Fair Credit Reporting Act, and industry-developed standards such as the Payment Card Data Security Standard and ISO 27001. Directing the creation of new standards could unnecessarily create conflicting or duplicative standards, increasing the burden on business and increasing confusion for consumers.

3. **The use of encryption or other security measures that render data unreadable and unusable should be a key element in establishing the threshold for the need for notification.** Any notification scheme should minimize "false positives." A clear reference to the "usability" of information should be considered when determining whether notification is required in case of a breach. Consistent with the position of consumer and financial groups, TechAmerica believes a provision similar to California's SB 1386 promoting the voluntary use of encryption as a best practice without a mandate would significantly reduce the number of "false positives," reducing the burden on consumers and business.

ADDITIONAL FEDERAL DATA BREACH PUBLIC POLICY ISSUES

TechAmerica recognizes that there are a number of other critical issues to the data security debate. These are issues on which we may be called to give an opinion, but are not issues that are TechAmerica’s top priorities. They may, however, be critical to whether a bill gets enacted, and are therefore important to TechAmerica.

1. **Enforcement.** Enforcement should be by the Federal functional regulators. TechAmerica would acknowledge that the State Attorneys General could enforce data notification requirements on entities that do not have a Federal functional regulator. Entities already covered by a Federal law such as the Health Insurance Portability and Accountability Act, Fair Credit Reporting Act, or the Gramm-Leach-Bliley Act, would not need to be additionally covered by a new law.

2. **Pre-emption.** New legislation should preempt relevant State and local laws and regulation. In the absence of such a provision, multiple conflicting standards for security and notification will emerge, unnecessarily increasing the burden on business and confusing consumers.

3. **Information Broker.** Special provisions for information brokers have emerged in data breach legislation over the last few Congresses. This was in large part a response to the scandal involving ChoicePoint a number of years ago. Any special Information Broker provisions should be carefully targeted to those engaged in the data broker business, which have otherwise slipped through the cracks of laws such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act. Where there is a gap in regulation, it should be filled; but overlapping requirements are counter-productive. Particular care must be taken not to inadvertently sweep in companies collecting information in the normal course of business, such as businesses monitoring their own websites. In general, we believe information broker provisions are not core to an effective data security and breach notice bill, and therefore should be dropped, as they have become a complication and impediment to the enactment of a bill. We think this provision certainly merits further analysis and may warrant legislation as a separate bill.

4. **Public Records.** A breach notice should not be required for a breach involving only information that is already publicly available. This is a related issue to the issue of the "threshold" for notice.

THE DATA SECURITY AND BREACH NOTIFICATION ACT OF 2010

Mr. Chairman, I commend you and Chairman Rockefeller for your leadership in addressing the pervasive threat of data breaches through the introduction of the Data Security and Breach Notification Act (S.3742). TechAmerica strongly supports this legislation which, if enacted, would establish a much-needed national law for all holders of sensitive personal information requiring organizations to safeguard data and establish uniform notification requirements when a security breach presents a risk of harm. We urge the Committee to expedite passage of this important legislation in order to create a strong, uniform national data breach notification law.

The Data Security and Breach Notification Act is a well-considered piece of legislation on a complex topic. The bill not only protects consumers in that it requires nearly all businesses to take steps to protect personally identifiable information at rest and in motion. The legislation prudently promotes reasonable, preventative security measures, practices and policies to ensure the confidentiality and integrity of consumers' personal identifiable information.

Besides providing extensive consumer protection, the Data Security and Breach Notification Act also provides businesses a reasonable "rebuttable presumption" by declaring loss of data that is "unusable, unreadable, or indecipherable" by the use of encryption or other technology, not subject to the breach disclosure requirements. This bill also, of course, will unify the existing 47 state data breach bills now in effect. TechAmerica believes that the Data Security and Breach Notification Act effectively addresses several key areas necessary to secure consumer sensitive personal information, specifically:

1. **Federal Pre-emption**. S. 3742 would preempt relevant State or local laws or regulation. In the absence of such a provision, multiple conflicting standards for notification will emerge, unnecessarily increasing the burden on business and confusing consumers. Without Federal pre-emption, businesses will continue to face a web of potentially conflicting breach notification requirements in forty-six states. TechAmerica believes that your bill takes the appropriate approach to pre-emption.

2. **Scope.** A breach notification requirement should apply to any agency or person, as defined in Title V of the U.S. Code, who owns or licenses computerized data containing the sensitive personal information of others and should not be limited to "data brokers." Legislation should address "gaps" in existing laws related to the security of personal information, not add another layer on those already bound by an existing Federal law. Security breaches have been confirmed in a variety of organizations, ranging from data brokers, to banks, hospitals, educational institutions and other large employers. TechAmerica believes that S. 3742 is generally applicable to the correct scope of persons and organizations. Some clarification may be necessary on the carve-out for those bound by another Federal law.

3. **Reasonable Security Practices**. S. 3742 goes beyond simple notification requirements to consumers in case of data breach; it importantly also requires reasonable security measures to ensure the confidentiality and integrity of sensitive personal information. For data breach legislation to be effective in safeguarding consumers' sensitive information, all business entities operating in the U.S., as well as

federal and state agencies, should follow a consistent set of security standards. We note that some Federal laws already exist that require private entities to establish security programs for protecting the privacy and security of consumer information. Legislation should not duplicate or impose conflicting obligations for private entities that already are bound by these federal data security requirements.

4. **Threshold for Notification.** TechAmerica believes that the Data Security and Breach Notification Act's notification requirement will minimize "false positives." The bill's language contains a clear understanding that the "usability" of information should be considered when determining whether notification is required in case of a breach. Consistent with the position of consumer groups and the financial services sector, TechAmerica believes a provision similar to CA's SB 1386 promoting the voluntary use of encryption as a best practice without specifically mandating it would significantly reduce the number of "false positives," reducing the burden on consumers and business. TechAmerica applauds the inclusion of section 3(f), which creates a presumption that, when used properly, encryption can provide a strong tool to prevent the misuse of personal information. S. 3742 also prudently recognizes the use of redaction, truncation or other methods of rendering data unreadable or unusable as a best practice without creating a technology mandate.

5. **Global Harmonization.** The passage of S. 3742 will also have important implications internationally as it is likely to form the basis upon which the Federal Trade Commission will commence negotiations to create consistency in breach regulations with the European Union. The European Union continues to lead the way in enforcing some of the most stringent privacy regulations on the Internet. With regulators in Europe moving ahead on their plans to provide even more privacy safeguards for their citizens, it's critical that U.S. regulators finalize the data breach requirements so they can focus on some of the more current issues.

CONCLUSIONS

TechAmerica urges Congress to enact a national data breach bill this year for several key reasons:

- **Identity Theft Tops the Federal Trade Commission's List of U.S. Consumers Complaints:** The increasing number of data breaches is a major threat to privacy, consumers' identities and our nation's economic stability. Databases of sensitive personal information are prime targets of hackers, identity thieves and rogue employees as well as organized criminal operations. According to the Better Business Bureau identity theft affects an estimated 10 million U.S. victims per year. For the ninth year in a row, identity theft tops the list of complaints that consumers filed with the Federal Trade Commission.

- **Massive Data Leakage Will Continue Unless the Public and Private Sectors are Required by Congress to Implement Strong Security Measures to Prevent Breaches:** According to the non-partisan *Privacy Rights Clearinghouse, a* staggering 365 million records containing sensitive personal information have been breached since 2005. Congressional action is urgently needed to ensure the security and resilience of information systems fundamental to consumer confidence, homeland security, e-commerce and economic growth.

- **Data Breaches Continue to Undermine Consumer Confidence in the Internet for E-Commerce:** Consumers are beginning to rethink doing business online - and with good reason. In the wake of massive data breaches at businesses, educational institutions and medical facilities, consumers are modifying their purchasing behavior, including online buying, out of concern for the security of their personal information. The 2007 Consumer Survey on Data Security from Vontu and the Ponemon Institute found that 62 percent of respondents have been notified that their confidential data has been lost. 84 percent of those respondents reported increased concern or anxiety due to data loss events. These data breaches have had a direct impact on consumer buying behavior, including reluctance to use their credit or debit card to make a purchase with a Web merchant they don't know, and unwillingness to provide their Social Security number online. Congress needs to act to stop the erosion of public trust in the Internet.

- **The Increasingly Expensive Financial Impact of Data Breaches on Business and Government:** In 2008, the average cost per incident of a data breach in the United States was $6.7 million, an increase of 5 percent from 2007, and lost business amounted to an average of $4.6 million.

- **A Pre-emptive, National Data Security Law Makes Compliance Less Burdensome:** Currently, businesses with nation-wide operations face a challenging patchwork quilt of state data breach laws regarding both steps required to safeguard personal data as well as steps to be taken in the event of a breach. With regard specifically to post-breach notifications, 46 states, the District of Columbia, Puerto Rico and the Virgin Islands all have enacted their own data breach laws requiring notification of security breaches involving personal information. Therefore, for large enterprises, which are also subject to complex federal rules such as HIPAA, data security planning can be a daunting undertaking making compliance a difficult and burdensome.

In conclusion, TechAmerica believes that the United States urgently needs to pass a national data breach law. We urge the Committee to expeditiously approve S. 3742, The Data Security and Breach Notification Act.

TechAmerica appreciates the opportunity to testify today. Thank you for considering TechAmerica’s views on this important measure. I’d be happy to answer any questions the Committee may have at this time.