

**S. 3742, THE DATA SECURITY
AND BREACH NOTIFICATION ACT OF 2010**

HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION,
PRODUCT SAFETY, AND INSURANCE

OF THE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION

UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

SEPTEMBER 22, 2010

Printed for the use of the Committee on Commerce, Science, and Transportation



U.S. GOVERNMENT PRINTING OFFICE

67-687 PDF

WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUE, Hawaii	KAY BAILEY HUTCHISON, Texas, <i>Ranking</i>
JOHN F. KERRY, Massachusetts	OLYMPIA J. SNOWE, Maine
BYRON L. DORGAN, North Dakota	JOHN ENSIGN, Nevada
BARBARA BOXER, California	JIM DEMINT, South Carolina
BILL NELSON, Florida	JOHN THUNE, South Dakota
MARIA CANTWELL, Washington	ROGER F. WICKER, Mississippi
FRANK R. LAUTENBERG, New Jersey	GEORGE S. LEMIEUX, Florida
MARK PRYOR, Arkansas	JOHNNY ISAKSON, Georgia
CLAIRE McCASKILL, Missouri	DAVID VITTER, Louisiana
AMY KLOBUCHAR, Minnesota	SAM BROWNBACK, Kansas
TOM UDALL, New Mexico	MIKE JOHANNNS, Nebraska
MARK WARNER, Virginia	
MARK BEGICH, Alaska	

ELLEN L. DONESKI, *Staff Director*

JAMES REID, *Deputy Staff Director*

BRUCE H. ANDREWS, *General Counsel*

ANN BEGEMAN, *Republican Staff Director*

BRIAN M. HENDRICKS, *Republican General Counsel*

NICK ROSSI, *Republican Chief Counsel*

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND
INSURANCE

MARK PRYOR, Arkansas, <i>Chairman</i>	ROGER F. WICKER, Mississippi, <i>Ranking</i>
BYRON L. DORGAN, North Dakota	OLYMPIA J. SNOWE, Maine
BARBARA BOXER, California	JIM DEMINT, South Carolina
BILL NELSON, Florida	JOHN THUNE, South Dakota
CLAIRE McCASKILL, Missouri	JOHNNY ISAKSON, Georgia
AMY KLOBUCHAR, Minnesota	DAVID VITTER, Louisiana
TOM UDALL, New Mexico	

CONTENTS

	Page
Hearing held on September 22, 2010	1
Statement of Senator Pryor	1
Statement of Senator Wicker	36
Statement of Senator Klobuchar	41

WITNESSES

Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection, Federal Trade Commission	3
Prepared statement	5
Mark Bregman, Chief Technology Officer, Symantec Corporation on Behalf of Symantec Corporation and TechAmerica	10
Prepared statement	12
Ioana Rusu, Policy Counsel, Consumers Union	21
Prepared statement	22
Stuart K. Pratt, President and CEO, Consumer Data Industry Association	24
Prepared statement	25
Melissa Bianchi, Hogan Lovells U.S. LLP, on Behalf of the American Hospital Association	32
Prepared statement	33

APPENDIX

Hon. John D. Rockefeller IV, prepared statement	51
Confidentiality Coalition, prepared statement	51
Response to written questions submitted by Hon. Mark Pryor to:	
Maneesha Mithal	55
Ioana Rusu	58
Stuart K. Pratt	59
Melissa Bianchi	61
Letter, dated December 7, 2010 to Senator Roger Wicker, from Stuart K. Pratt, Consumer Data Industry Association	63

**S. 3742, THE DATA SECURITY
AND BREACH NOTIFICATION ACT OF 2010**

WEDNESDAY, SEPTEMBER 22, 2010

U.S. SENATE,
SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT
SAFETY, AND INSURANCE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:33 p.m. in room SR-253, Russell Senate Office Building, Hon. Mark Pryor, presiding.

**OPENING STATEMENT OF HON. MARK PRYOR,
U.S. SENATOR FROM ARKANSAS**

Senator PRYOR. I'll go ahead and call us to order here. I want to thank everyone for being here today on this hearing on S. 3742, the Data Security and Breach Notification Act of 2010. I know we have a couple of Senators that are on the way, whether literally or figuratively, but they'll be here shortly. So I think what I will do is go ahead and do my opening statement, and if they want to make opening statements when they come that would be great, or we'll jump right into statements and questions.

But let me go ahead and start today, to say that the Privacy Rights Clearinghouse recently estimated that since 2005 a half billion sensitive records have been breached. So I think that is worth repeating: The Privacy Rights Clearinghouse recently estimated that since 2005 a half billion sensitive records have been breached.

The TJMaxx case is one of the more high profile cases, but the truth is, even though that one did involve 45 million names, credit cards, driver's license information, et cetera, there are a slew of other examples of entities large and small who've had these data breaches. In fact, just recently in Arkansas an employee of one of our State universities inadvertently released personal information on more than 2,000 university employees to a list of nearly 150 individuals.

So obviously this is an issue that touches all of us. Studies have shown the average victim of identity theft pays between \$400 and \$880 and devotes between 400 and 300 hours to remedy problems due to identity theft. Just think about someone spending 40 hours trying to fix this. That's an entire week's worth of work that they could be working, could be productive, could be with their families or whatever else they're doing, but they're fooling around with this thing because someone has stolen their identity.

This has become such a problem, and my sense is the current state of the law is not sufficient to handle it. I think we need to do more. As we all know, data security breaches can lead to identity theft and other types of fraud. They say each year—and I'm not quite sure how solid this statistic is, but they say each year approximately 9 million Americans have their identities stolen.

So if their information is compromised due to inadequate security measures or insufficient safeguards, those entities responsible should be held accountable and should notify customers when a breach has occurred. If a customer's personal information falls into the wrong hands, it's only fair that companies be expected to give quick warning to affected consumers.

So I've drafted a bill along with Senator Rockefeller that we filed on August 5 of this year. It's S. 3742, the Data Security and Breach Notification Act of 2010. It will require entities that own or possess data containing personal information to establish reasonable security policies and procedures to protect that data. If a security breach occurs, entities would have to notify each individual whose information was acquired or accessed as a result of the breach within 60 days.

Affected consumers would be entitled to receive consumer credit reports and credit monitoring services for 2 years, as well as instructions on how to request these services.

As a former attorney general, I'm very comfortable with allowing the State AGs to protect their residents from harm and so my bill grants the State attorneys general important powers enabling them to do just that.

Before I turn it over to our witnesses for their opening statements, I would like to thank the Chairman for his steadfast support of the bill. He and I have worked closely on this, and I look forward to continuing those conversations. I also want to thank Chairman Inouye, who graciously allowed me to pick up this issue and to carry it forward. Finally, I want to thank my friends on the House side, including Congressmen Rush and Stern, for their hard work on this issue. The House passed by voice vote last December a companion measure which we've used as some of our base text here, and I think that one of the good things about the Commerce Committee is we have a record of working across the aisle and down the hall with the House as well. So I just want to let my Republican colleagues know that I look forward to the dialogue and look forward to working on this and trying to get this to a fairly rapid conclusion. I'm certainly receptive to more input and suggestions.

Again, I want to thank the Chairman for this opportunity to take the lead on this very critical matter.

So what I thought we would do here is, when Senator Wicker comes we'll ask him if he wants to give an opening statement. I know he's in another committee tied up right now, but I think he's on his way at some point.

Also what I'd like to do is just go ahead and introduce our witnesses very quickly and try to introduce everybody. What I'd like to ask everyone to do is limit your opening statements to 5 minutes if possible, and we'll make your written statement part of the record and then we'll dive in and ask questions.

So I guess in the order—I guess you guys are lined up in the order that we have you listed here. So why don't we first go with Maneesha Mithal. She's the Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission.

Then we'll have: Mr. Mark Bregman, Chief Technology Officer of Symantec, and on behalf of TechAmerica; and then Ms. Ioana Rusu, Policy Counsel, Consumers Union; and then Mr. Stuart Pratt. He's President, Consumer Data Industry Association. And then Ms. Melissa Bianchi. Am I getting that right?

Ms. BIANCHI. Yes.

Senator PRYOR. American Hospital Association. And I guess you're with a law firm, Hogan Lovells; is that right?

Ms. BIANCHI. Yes.

Senator PRYOR. On behalf of the American Hospital Association.

So, Ms. Mithal, why don't we start with you, and we'll just try to do 5 minutes and then we'll just go from there. Go ahead. Thank you.

**STATEMENT OF MANEESHA MITHAL, ASSOCIATE DIRECTOR
OF THE DIVISION OF PRIVACY AND IDENTITY PROTECTION,
FEDERAL TRADE COMMISSION**

Ms. MITHAL. Thank you, Mr. Chairman. My name is Maneesha Mithal and I'm an Associate Director at the Federal Trade Commission, and I'm delighted to be here today to talk about our data security program and also to provide comments on S. 3742.

The FTC promotes data security through law enforcement, education, and policy initiatives. On the law enforcement front, we've brought 29 cases against businesses that failed to safeguard consumers' personal information. Let me give you a couple of recent examples.

First, we sued Rite-Aid because they disposed of sensitive health, financial, and employee information into open dumpsters. We alleged that they didn't implement reasonable security to dispose of this information.

Second, we sued the social media service Twitter for, among other things, failing to require its employees to use strong passwords. Because of its security failures, a hacker was able to use a simple automated password-guessing tool to access employee accounts and send fake tweets.

Third, we sued LifeLock for inadequate data security. LifeLock sold consumers an identity theft protection service. You may recall LifeLock's ads, which prominently displayed the CEO's real Social Security number to show how confident he was in LifeLock's service. As it turns out, the CEO later became a victim of identity theft. Despite the fact that LifeLock collected Social Security numbers from consumers, it didn't maintain reasonable security for them.

In each of these cases, the Commission's orders required the companies to maintain reasonable security and to get periodic independent audits of their security practices.

In addition to law enforcement, we've launched educational campaigns directed to consumers on how to avoid identity theft and what to do if they become victims. We've released general data security guidance for businesses and we've also created business edu-

cation materials on specific topics. For example, earlier this year, we sent letters notifying several entities that customer information from their computers had been made available through P2P file sharing networks. In the letter we included educational materials about the risks associated with P2P file sharing and companies' obligations to protect consumer and employee information from these risks.

Finally, we engage in policymaking efforts to promote data security and stay abreast of new issues in this area. For example, over the past several months, the FTC has hosted three privacy roundtables to explore consumer privacy issues. Panelists discussed the impact of new technologies, such as cloud computing and mobile services, on data security. The Commission staff expects to issue a report on the roundtables later this year.

Let me now turn to our legislative recommendations. We strongly support the goals of S. 3742. In particular, we support the general requirement to maintain reasonable security, the requirement to provide notice to consumers when their information is breached, and the grant of civil penalty authority to the FTC. We also support the provisions giving State attorneys general authority to sue companies for violations of the bill.

In addition, S. 3742 contains specific provisions governing data brokers, including provisions giving consumers the right to access data that data brokers have about them. The Commission believes these provisions can help to alleviate concerns raised at our privacy roundtables about the invisibility of practices of the data broker industry.

On a related note, just today, the Commission announced a case against a data broker named US Search. This company had a public-facing search engine that allowed consumers to search for information about other consumers. The company allowed consumers to opt out of having their information appear in search results for a fee of \$10. Although 4,000 consumers opted out of the service, their names still appeared in search results. The Commission's settlement with the company requires US Search to disclose limitations on its opt-out and to refund consumers who had previously opted out.

Although the Commission has used its authority under the FTC Act to sue data brokers, S. 3742's data broker provisions would give the Commission additional authority in this area.

Finally, let me provide some comments about the scope of the bill. We're pleased that it covers nonprofits, as many of the security breaches we've heard about in the past several years involve universities and other nonprofits. We believe the bill should also apply to telecom common carriers, many of which maintain significant quantities of personal information.

In addition, we'd like to see the bill's breach notification provisions apply to paper as well as electronic records. Many cases we've seen, including the Rite-Aid case I mentioned earlier, involved inadequate security for paper records, which could cause significant harm to consumers.

We look forward to working with this committee as the bill moves forward. I thank you, Mr. Chairman. I'd be happy to answer any questions.

[The prepared statement of Ms. Mithal follows:]

PREPARED STATEMENT OF MANEESHA MITHAL, ASSOCIATE DIRECTOR OF THE DIVISION OF PRIVACY AND IDENTITY PROTECTION, FEDERAL TRADE COMMISSION

I. Introduction

Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee, I am Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission (“FTC” or “Commission”). I appreciate the opportunity to present the Commission’s testimony on data security and to provide the Commission’s thoughts on legislation in this area.¹

As the Nation’s consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace. Accordingly, the Commission has undertaken substantial efforts to promote data security in the private sector through law enforcement, education, and policy initiatives. The Commission’s testimony begins by describing these initiatives. It also sets forth the Commission’s support of the proposed data security legislation introduced by Chairman Pryor and Chairman Rockefeller along with certain recommendations on the legislation.

II. The Commission’s Data Security Program

A. Law Enforcement

To promote data security through law enforcement, the Commission brings enforcement actions against businesses that fail to implement reasonable security measures to protect consumer data. The FTC enforces several laws and rules imposing data security requirements. The Commission’s Safeguards Rule under the Gramm-Leach-Bliley Act (“GLB Act”), for example, provides data security requirements for financial institutions.² The Fair Credit Reporting Act (“FCRA”) requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,³ and imposes safe disposal obligations on entities that maintain consumer report information.⁴ In addition, the Commission enforces the FTC Act’s proscription against unfair or deceptive acts or practices⁵ in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.

Since 2001, the Commission has used its authority under these laws to bring 29 cases against businesses that allegedly failed to protect consumers’ personal information appropriately.⁶ These cases illustrate several general principles.

¹ This written statement represents the views of the Federal Trade Commission. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

² 16 CFR Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, Secretary of the Treasury, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

³ 15 U.S.C. § 1681e.

⁴ *Id.* at § 1681w. The FTC’s implementing rule is at 16 CFR Part 682.

⁵ 15 U.S.C. § 45(a).

⁶ See *In re Rite Aid Corp.*, FTC File No. 072–3121 (July 27, 2010) (consent approved subject to public comment); *In re Twitter, Inc.*, FTC File No. 092–3093 (June 24, 2010) (consent approved subject to public comment); *Dave & Buster’s, Inc.*, FTC Docket No. C–4291 (May 20, 2010) (consent order); *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-NVW (D. Ariz. Mar. 15, 2010) (stipulated order); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC (N.D. Ga. Oct. 14, 2009) (stipulated order); *In re James B. Nutter & Company*, FTC Docket No. C–4258 (June 12, 2009) (consent order); *United States v. Rental Research Servs.*, No. 0:09-CV-00524 (D. Minn. Mar. 6, 2009) (stipulated order); *FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 29, 2009) (stipulated order); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008) (stipulated order); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007) (stipulated order); *In re CVS Caremark Corp.*, FTC Docket No. C–4259 (Jun. 18, 2009) (consent order); *In re Genica Corp.*, FTC Docket No. C–4252 (Mar. 16, 2009) (consent order); *In re Premier Capital Lending, Inc.*, FTC Docket No. C–4241 (Dec. 10, 2008) (consent order); *In re The TJX Cos.*, FTC Docket No. C–4227 (July 29, 2008) (consent order); *In re Reed Elsevier Inc.*, FTC Docket No. C–4226 (July 29, 2008) (consent order); *In re Life is good, Inc.*,

Continued

First, businesses that make claims about data security should be sure that they are accurate. The Commission has brought several cases against companies that allegedly misrepresented their own security procedures. A recent example is our action against LifeLock, in which the Commission challenged the company's claims that it took stringent security measures to protect consumer data and that it encrypted such data.⁷ The FTC charged that Lifelock's data was in fact not encrypted and that its data system was vulnerable and could have been exploited by identity thieves or others seeking access to customer information. Similarly, in actions against Microsoft,⁸ Petco,⁹ Tower Records,¹⁰ Life is good,¹¹ and Premier Capital Lending,¹² the FTC challenged claims on the companies' websites that each had strong security procedures in place to protect consumer information. In these cases the FTC alleged that, contrary to their claims, the companies did not employ many of the most basic security measures.

Second, businesses should protect against well-known, common technology threats. In a number of cases, the Commission has alleged that companies failed to protect their customer information from a simple and well-known type of attack—an SQL injection—designed to install hacker tools on the companies' computer networks.¹³ Most recently, the Commission announced its first data security case against social networking company Twitter, alleging that it failed to implement simple measures to counteract basic technology threats. For example, the Commission alleged that the company failed to require strong administrative passwords and to suspend passwords after a reasonable number of log-in attempts, and further alleged that this failure resulted in a hacker being able to use a simple automated password-guessing tool to gain administrative control of Twitter.

Third, businesses must know with whom they are sharing customers' sensitive information. One of the Commission's most well-known security cases involved ChoicePoint, a data broker that sold 160,000 consumer files to identity thieves posing as clients. In its complaint, the Commission alleged that ChoicePoint lacked reasonable procedures to verify the legitimacy of its customers.¹⁴ In settling the case, ChoicePoint agreed to pay \$10 million in civil penalties for alleged violations of the FCRA and \$5 million in consumer redress for identity theft victims. The company also agreed to undertake substantial new data security measures. Last year, the Commission charged that the company violated the earlier court order and obtained a stipulated modified order under which ChoicePoint agreed to expand its data security obligations and pay penalties in the amount of \$275,000.¹⁵

Fourth, businesses should not retain sensitive consumer information that they do not need. In cases against BJ's Warehouse,¹⁶ DSW Shoe Warehouse,¹⁷ and CardSystems Solutions,¹⁸ for example, the Commission alleged that the companies stored unencrypted, full magnetic stripe information on payment cards¹⁹ unneces-

FTC Docket No. C-4218 (Apr. 16, 2008) (consent order); *In re Goal Fin., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008) (consent order); *In re Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007) (consent order); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006) (consent order); *In re Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006) (consent order); *In re DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006) (consent order); *In re Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005) (consent order); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005) (consent order); *In re Nationwide Mortgage Group, Inc.*, FTC Docket No. C-9319 (Apr. 12, 2005) (consent order); *In re Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order); *In re Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005) (consent order); *In re MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004) (consent order); *In re Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003) (consent order); *In re Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

⁷ *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-NVW (D. Ariz. Mar. 15, 2010) (stipulated order).

⁸ *In re Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

⁹ *In re Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order).

¹⁰ *In re MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004) (consent order).

¹¹ *In re Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (consent order).

¹² *In re Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008) (consent order).

¹³ See, e.g., *In re Genica Corp.*, FTC Docket No. C-4252 (Mar. 16, 2009) (consent order); *In re Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007) (consent order).

¹⁴ *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006) (stipulated order).

¹⁵ *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC (N.D. Oct. 14, 2009) (stipulated order).

¹⁶ *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sep. 20, 2005) (consent order).

¹⁷ *In re DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006) (consent order).

¹⁸ *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sep. 5, 2006) (consent order).

¹⁹ Magnetic stripe information is particularly sensitive because it can be used to create counterfeit credit and debit cards that appear genuine in the authorization process.

sarily—long after the time of the transaction, when the companies no longer had a business need for the information. The Commission further alleged that, as a result, when thieves gained access to the companies' systems, they were able to obtain hundreds of thousands—in some cases millions—of credit card numbers and security codes.

Finally, businesses should dispose of sensitive consumer information properly. The Commission's most recent data security case against Rite Aid illustrates this principle.²⁰ In that case, the Commission alleged that Rite Aid failed to implement reasonable and appropriate procedures for handling personal information about customers and job applicants, particularly with respect to its practices for disposing of such information. The FTC's action followed media reports that Rite Aid pharmacies across the country were throwing pharmacy labels and employment applications into open dumpsters. The FTC coordinated its investigation and settlement with the Department of Health and Human Services ("HHS"), which investigated Rite Aid's handling of health information under the Health Insurance Portability and Accountability Act. Under its settlement order with the FTC, Rite Aid agreed to establish a comprehensive information security program and obtain biennial audits of this program for the next 20 years. HHS announced a separate agreement with Rite Aid in which the company agreed to pay a \$1 million fine.²¹

Some of the Commission's data security actions described above involve unfair or deceptive practices under the FTC Act, while others involve the GLB Act and related Safeguards Rule or the FCRA. Although the Commission brings its cases under different laws, all of its cases stand for the principle that companies must maintain reasonable and appropriate measures to protect sensitive consumer information.²²

B. Education

The Commission also promotes better data security practices through extensive use of consumer and business education. On the consumer education front, the Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security.²³ OnGuard Online was developed in partnership with other government agencies and the technology sector. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Línea have attracted nearly 12 million unique visits.

In addition, the Commission has engaged in wide-ranging efforts to educate consumers about identity theft, one of the harms that could result if their data is not adequately protected. For example, the FTC's identity theft primer²⁴ and victim recovery guide²⁵ are widely available in print and online. Since 2000, the Commission has distributed more than 10 million copies of the two publications, and recorded over 5 million visits to the Web versions. In addition, in February 2008, the U.S. Postal Service—in cooperation with the FTC—sent copies of the Commission's identity theft consumer education materials to more than 146 million residences and businesses in the United States. Moreover, the Commission maintains a telephone hotline and dedicated website to assist identity theft victims and collect their complaints, through which approximately 20,000 consumers contact the FTC every week.

The Commission recognizes that its consumer education efforts can be even more effective if it partners with local businesses, community groups, and Members of Congress to educate their employees, communities, and constituencies. For example,

²⁰ See *In re Rite Aid Corp.*, FTC File No. 072-3121 (July 27, 2010) (consent approved subject to public comment).

²¹ The FTC brought a similar case against CVS Caremark alleging that the company failed to properly dispose of sensitive customer and employee information. See *In re CVS Caremark Corp.*, FTC Docket No. C-4259 (Jun. 18, 2009) (consent order). The FTC also has brought cases involving mortgage companies' alleged improper disposal of sensitive customer financial information. See *FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 29, 2009) (stipulated order); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007) (stipulated order).

²² The Commission recognizes that what is "reasonable" under these laws will depend on the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the information at issue. The principle recognizes that there cannot be "perfect" security, and that data breaches can occur even when a company maintains reasonable precautions to prevent them. At the same time, companies that put consumer data at risk can be liable even in the absence of a known breach.

²³ See www.onguardonline.gov.

²⁴ *Avoid ID Theft: Deter, Detect, Defend*, available at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth01.htm>.

²⁵ *Take Charge: Fighting Back Against Identity Theft*, available at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.htm>.

the Commission has launched a nationwide identity theft education program, “Avoid ID Theft: Deter, Detect, Defend,” which contains a consumer education kit that includes direct-to-consumer brochures, training materials, presentation slides, and videos for use by such groups. The Commission has developed a second consumer education toolkit with everything an organization needs to host a “Protect Your Identity Day.” Since the campaign launch in 2006, the FTC has distributed nearly 110,000 consumer education kits and over 100,000 Protect Your Identity Day kits.

The Commission directs its outreach to businesses as well. The FTC widely disseminates its business guide on data security, along with an online tutorial based on the guide.²⁶ These resources are designed to provide diverse businesses—and especially small businesses—with practical, concrete advice as they develop data security programs and plans for their companies.

The Commission also has released articles for businesses relating to basic data security issues for a non-legal audience,²⁷ which have been reprinted in newsletters for local Chambers of Commerce and other business organizations.

The FTC also creates business educational materials on specific topics, often to address emerging issues. For example, earlier this year, the Commission sent letters notifying several dozen public and private entities—including businesses, schools, and local governments—that customer information from their computers had been made available on peer-to-peer (“P2P”) file sharing networks. The purpose of this campaign was to educate businesses and other entities about the risks associated with P2P file sharing programs and their obligations to protect consumer and employee information from these risks. As part of this initiative, the Commission developed a new business education brochure—*Peer-to-Peer File Sharing: A Guide for Business*.²⁸

C. Policy

The Commission’s efforts to promote data security also include policy initiatives. Over the past several months, the FTC has convened three public roundtables to explore consumer privacy.²⁹ Panelists at the roundtables repeatedly noted the importance of data security in protecting privacy. Many participants stated that companies should incorporate data security into their everyday business practices, particularly in today’s technological age. For example, participants noted the increasing importance of data security in a world where cloud computing enables companies to collect and store vast amounts of data at little cost.³⁰ In addition, participants noted that the falling cost of data storage enables companies to retain data for long periods of time, again at little cost. Even if old data is not valuable to a particular company, it could be highly valuable to an identity thief. This is one of the reasons why businesses should promptly and securely dispose of data for which they no longer have a business need.³¹

The Commission staff expect to issue a report later this year seeking comment on these and other topics. Among other things, the report will encourage companies to incorporate sound data security and data retention practices into their business models in a reasonable and cost-effective way.

III. Legislative Recommendations

The Commission appreciates the opportunity to comment on the proposed legislation introduced by Chairman Pryor and Chairman Rockefeller. The Commission

²⁶ See www.ftc.gov/infosecurity.

²⁷ See <http://business.ftc.gov/privacy-and-security>.

²⁸ See <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm>.

²⁹ See generally FTC Exploring Privacy web page, www.ftc.gov/bcp/workshops/privacyroundtables.

³⁰ See, e.g., Privacy Roundtable, Transcript of January 28, 2010, at 182, Remarks of Harriet Pearson, IBM (noting the importance of data security as an issue for new computing models, including cloud computing).

³¹ See, e.g., Privacy Roundtable, Transcript of January 28, 2010, at 310, Remarks of Lee Tien, Electronic Frontier Foundation (“And having the opposite of data retention, data deletion as a policy, as a practice is something that, you know, really doesn’t require any fancy new tools. It is just something that people could do, would be very cheap, and would mitigate a lot of privacy problems.”); Privacy Roundtable, Transcript of March 17, 2010, at 216, Remarks of Pam Dixon (supporting clear and specific data retention and use guidelines). The Commission has long supported this principle in its data security cases. Indeed, at least three of the Commission’s data security cases—against DSW Shoe Warehouse, BJ’s Wholesale Club, and Card Systems—involved allegations that companies violated data security laws by retaining magnetic stripe information from customer credit cards much longer than they had a business need to do so. Moreover, in disposing of certain sensitive information, such as credit reports, companies must do so securely. See FTC Disposal of Consumer Report Information and Records Rule, 16 CFR § 682 (2005).

supports the goal of improving the security of consumer data. The proposed legislation contains several important components.

First, it would require a broad array of companies to implement reasonable security policies and procedures, including both commercial and nonprofit entities. Problems with data security and breaches affect businesses and nonprofit organizations alike. Requiring reasonable security policies and procedures of this broad array of entities is a goal that the Commission strongly supports, as illustrated by its robust data security enforcement program described above.

Second, it would require covered companies to notify consumers when there is a security breach. The Commission believes that notification in appropriate circumstances can be beneficial.³² Indeed, various states have already passed data breach notification laws which require companies to notify affected consumers in the event of a data breach. These laws have further increased public awareness of data security issues and related harms, as well as data security issues at specific companies.³³ Breach notification at the Federal level would extend notification nationwide and accomplish similar goals.

Third, the Commission learned from its privacy roundtables that data brokers often gather consumer data from a variety of sources, combine it, and use it for purposes that consumers may never have anticipated when it was collected. Given the invisibility of these practices, consumers are unaware of and thus unable to control them. If information from data brokers is inaccurate—for example, if a data broker provides inaccurate information to a business for purposes of verifying a job applicant's identity—consumers can be harmed by the lack of access to, and ability to correct, that information. The Commission believes that S. 3742's provisions on access can help to alleviate these concerns.

At the same time, the Commission acknowledges that providing access can be costly, and that the right to suppress data rather than correct it may be sufficient in certain circumstances—if the data is used, for example, to make marketing decisions. The proposed rulemaking authority for the Commission will allow it to scale the legislative provisions on access, weighing its costs and benefits in particular circumstances.

Finally, the Commission supports the legislation's robust enforcement provisions, which would: (1) give the FTC the authority to obtain civil penalties for violations³⁴ and (2) give state attorneys general concurrent enforcement authority.³⁵

The Commission has three main recommendations for the legislation at this time. First, it recommends that the provision requiring notification in the event of an information security breach not be limited to entities that possess data in electronic form, because the breach of sensitive data stored in paper format can be just as harmful to consumers.³⁶ Second, as the proposed legislation is currently drafted, its

³²This recommendation is consistent with prior Commission recommendations. See Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Science, and Transportation, 109th Cong. (Jun. 16, 2005), available at <http://www.ftc.gov/os/2005/06/050616databreaches.pdf>; Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Trade, and Consumer Protection, 111th Cong. (May 5, 2009), available at <http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf>.

³³See, e.g., Samuelson Law, Technology, & Public Policy Clinic, University of California-Berkeley School of Law, *Security Breach Notification Laws: Views from Chief Security Officers* (Dec. 2007), available at http://www.law.berkeley.edu/files/cso_study.pdf; Federal Trade Commission Report, *Security in Numbers: SSNs and ID Theft* (Dec. 2008), available at <http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf>.

³⁴See *supra* at n. 32.; see also Prepared Statement of the Federal Trade Commission Before the Subcomm. on Interstate Commerce, Trade, and Tourism of the S. Comm. on Commerce, Science, and Transportation Committee, 110th Cong. (Sep. 12, 2007) available at <http://www.ftc.gov/os/testimony/070912reauthorizationtestimony.pdf>; Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Science, and Transportation, 110th Cong. (Apr. 10, 2007), available at <http://www.ftc.gov/os/testimony/P040101FY2008BudgetandOngoingConsumerProtectionandCompetitionProgramsTestimonySenate04102007.pdf>. These recommendations also were made in an April 2007 report released by the President's Identity Theft Task Force, which was co-chaired by the Attorney General and the FTC Chairman, as well as in a report on Social Security numbers released in December 2008. See The President's Identity Theft Task Force Report, Sep. 2008, available at <http://idtheft.gov/reports/IDTReport2008.pdf>; FTC Report, "Recommendations on Social Security Number Use in the Private Sector." (Dec. 2008), available at <http://www.ftc.gov/opa/2008/12/ssnreport.shtm>.

³⁵See The President's Identity Theft Task Force, "Combating Identity Theft: A Strategic Plan," (Apr. 2007), available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

³⁶According to one survey, a significant number of breaches involve paper documents. See Ponemon Institute, *Security of Paper Documents in the Workplace* (Oct. 2008), available at <http://www.ponemon.org/data-security>. In addition, the Commission has brought several data security cases involving improper disposal of paper documents, including the Rite Aid case dis-

requirements do not apply to telecommunications common carriers, many of which maintain significant quantities of highly personal information. The Commission believes that the legislation should cover these entities and that the Commission should have authority to enforce the legislation as to them. Third, the bill requires the Commission to establish a process for small businesses to request a waiver from having to provide free credit reports or credit monitoring to consumers following a breach. The Commission believes that such a business-by-business waiver process would be resource intensive for both the Commission and small businesses. Instead, the Commission suggests that the bill grant it rulemaking authority to determine circumstances under which the provision of free credit reports or credit monitoring may not be warranted.³⁷ The Commission would be pleased to work with this Committee to address these issues.

IV. Conclusion

Thank you for the opportunity to provide the Commission's views on the topic of data security. We remain committed to promoting data security and look forward to continuing to work with you on this important issue.

Senator PRYOR. Mr. Bregman.

STATEMENT OF MARK BREGMAN, CHIEF TECHNOLOGY OFFICER, SYMANTEC CORPORATION ON BEHALF OF SYMANTEC CORPORATION AND TECHAMERICA

Mr. BREGMAN. Mr. Chairman, Ranking Member Wicker: I am Mark Bregman, Chief Technology Officer for Symantec Corporation. Thank you for inviting me to appear before you to discuss the Data Security and Breach Notification Act.

As a global information security leader, Symantec welcomes the opportunity to provide our insights on this important legislation. Today I will also be testifying on behalf of TechAmerica, which is the technology industry's largest advocacy organization, representing over 1,500 member companies.

Mr. Chairman, TechAmerica commends you and Chairman Rockefeller for your thoughtful leadership in addressing the pervasive threat of data breaches through the introduction of the Data Security and Breach Notification Act. Over the past few years, the frequency and severity of significant data breaches has increased dramatically, along with the costs of responding to such incidents. One survey estimates that between 80 and 90 percent of Fortune 500 companies and government agencies have experienced security breaches.

Additionally, as the Chairman mentioned in his opening remarks, the Privacy Rights Clearinghouse disclosed that over 510 million records containing sensitive personal information have been exposed by data breaches since 2005.

For organizations that possess critical information assets, such as customer data, intellectual property, and trade secrets, the risk of a data breach is now higher than ever before, especially for those organizations that store and manage large amounts of personal information. Not only can compromises result in the loss of personal data, they also undermine customer and institutional confidence. Breaches often lead to damage that is financially debilitating to organizations, while leaving consumers open to identity theft.

cussed above. The facts of these cases illustrate how breaches of sensitive data stored in paper format may create a serious potential for consumer harm.

³⁷The Commission notes that, as drafted, S. 3742 would preempt state law. In light of this, the Commission encourages this Committee to closely examine relevant state law, such as state data breach notification laws, to ensure that any Federal legislation in this area continues to provide consumers with a high level of protection.

The root causes of a data breach are of three main types: well-meaning insiders, targeted attacks, and malicious insiders. In fact, 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.

Company employees who inadvertently violate data security policies represent the largest population of data breaches. Other breaches are as a result of targeted attacks by organized crime, which are increasingly aimed at stealing information for the purposes of identity theft. Such attacks are often automated by using malicious code that can penetrate into an organization undetected and export data to remote hacker sites.

TechAmerica believes that consumers should have the highest confidence that any personal information they share with government agencies or business entities will remain private and secure in a trusted environment. We have long advocated that Congress include three essential core elements in data security legislation. First of all, the scope should apply equally to government and private sector entities that collect, maintain, or sell significant numbers of records containing sensitive personal information. Second, implementing reasonable pre-breach security measures and risk assessments should be central to any legislation in order to minimize the likelihood of the breach. And third, encryption or other proven security measures that render data unreadable or unusable should be a key element to establish the risk-based threshold for notification.

TechAmerica strongly supports the Data Security and Breach Notification Act. We believe that it's a well-considered piece of legislation on a very complex topic. The bill would establish a much-needed national law for all holders of sensitive personal information, requiring organizations to safeguard data and establish uniform notification mechanisms when a security breach presents a real risk of harm.

In addition to protecting consumers, the bill provides a clear roadmap for compliance for nearly all businesses by requiring organizations to take common sense steps to protect personally identifiable information both at rest and in motion. This bill prudently promotes reasonable preventative security measures, practices, and policies in order to ensure that confidentiality and integrity of consumers' personally identifiable information is maintained.

We commend the inclusion of a provision in the bill that provides a rebuttable presumption that loss of data has been rendered unusable, unreadable, or undecipherable through the use of encryption or other acceptable means should not be subject to the breach disclosure requirements.

This is precisely the kind of roadmap to compliance that will reduce the burden on consumers and businesses while achieving the bill's goal of greater security.

Finally, it's important to note that, through effective preemption, this legislation will unify and simplify the existing 46 State data breach laws now in effect, making the current patchwork of compliance efforts less burdensome and costly.

In closing, TechAmerica urges Congress to act to enact a national data breach law this year.

Thank you for considering the views of Symantec and TechAmerica on this important measure. I'd be happy to answer any questions.

[The prepared statement of Mr. Bregman follows:]

PREPARED STATEMENT OF MARK BREGMAN, CHIEF TECHNOLOGY OFFICER,
SYMANTEC CORPORATION ON BEHALF OF SYMANTEC CORPORATION AND TECHAMERICA

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.

Symantec¹ 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 Network² 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.

TechAmerica³ 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 4 years combined.⁴

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 per-

¹Symantec 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.

²Symantec 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.

³TechAmerica 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).

⁴Verizon Business Risk Team, 2009 Data Breach Investigations Report.

⁵<http://arstechnica.com/security/news/2009/10/americans-fear-online-robberies-more-than-meatspace-muggings.ars>.

⁶http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf.

sonal 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 Team⁹ 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

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

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+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.

¹² *Ibid.*

¹³ Ponemon Institute, 2008 Annual Study: Cost of a Data Breach, February 2009.

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.
- *E-mail, web mail, and removable devices.* Risk assessments performed by Symantec for prospective customers show that on average approximately one in every 400 e-mail 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 e-mail 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 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.

¹⁴Verizon Business Risk Team, op. cit.

¹⁵Ponemon Institute, op. cit.

¹⁶Symantec Data Loss Prevention Risk Assessments.

¹⁷Verizon Business Risk Team, op. cit.

¹⁸*Ibid.*

¹⁹Symantec Internet Security Threat Report XIV.

²⁰Verizon Business Risk Team, op. cit.

²¹*Ibid.*

- *Improper credentials.* Passwords on Internet-facing systems such as e-mail, 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, e-mail 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 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 e-mail 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

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 obliga-

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.

tions 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 data bases 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 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 U.S. 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

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>.

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>.

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 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

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.lashdot.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.

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. Data bases 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.

Senator PRYOR. Thank you.
Ms. Rusu.

**STATEMENT OF IOANA RUSU, POLICY COUNSEL,
CONSUMERS UNION**

Ms. RUSU. Good afternoon, Chairman Pryor, Ranking Member Wicker, and distinguished members of the Subcommittee. My name is Ioana Rusu, Policy Counsel for Consumers Union, the nonprofit publisher of *Consumer Reports*. We appreciate this opportunity to share our perspective on the Data Security and Breach Notification Act of 2010.

In January of this year, over 600,000 Citigroup customers were shocked to discover that their Social Security numbers had been printed on the outside of envelopes containing annual tax statements. In July, a Lincoln National Life Insurance vendor made available on its public website a user name and password for agents and authorized brokers. The log-in information allowed access to anyone to medical records, Social Security numbers, addresses, policy numbers, and driver's license numbers of individuals seeking life insurance. Only last June, in one of the largest data security breaches recorded, malicious spyware compromised around 130 million credit card transactions processed by Heartland Payment Systems, a U.S. payments processing company.

These incidents are not unique or isolated. Almost every day new data breach incidents lead to identity theft, lost revenue, and decreased consumer confidence in the marketplace. Sometimes these incidents affect 10 or 20 consumers. At other times the private information of hundreds of millions of Americans is compromised.

The ubiquity of security breach incidents today renders the Data Security and Breach Notification Act of 2010 particularly timely and relevant. Consumers Union strongly supports the provisions of this bill. I would like to highlight a number of the bill's provisions which we believe will best promote consumer data privacy.

First of all, we are pleased that the bill covers not only business entities, but also nonprofit organizations, including private universities. Consumers face the same risks when their information is compromised whether or not the source of the compromise is a for-profit entity. As a result, we commend the bill's scope. This provision will provide more meaningful protection for consumer information.

In addition, we applaud the bill's notification provisions, which require covered entities to provide notice of security breach within 60 days. The sooner consumers are made aware of the breach, the quicker they can take remedial action such as closely monitoring their credit, checking their financial statements frequently, placing a Federal fraud alert on their credit files, and placing a security freeze on their consumer credit files. The instances in which a covered entity may exceed the 60-day deadline are appropriate and narrowly tailored.

We also support the bill's requirements that covered entities that provide at least 2 years of free credit reports or credit monitoring following a notice of breach. Consumers should not have to bear the cost of securing personal information when a data breach is caused by a company's inadequate data security practices.

The exemption in the bill allowing covered entities to avoid the bill's requirements only as long as there is no reasonable risk of identity theft, fraud, or other unlawful conduct is also narrowly tai-

lored. However, we do have some concern that under this bill all data breach incidents involving encrypted information, defined in the bill as information that has been rendered unusable, unreadable, or indecipherable, would automatically be presumed to present no reasonable risk of identity theft, fraud, or other unlawful conduct. While that may be true in most cases, data that has been initially rendered unusable or unreadable can sometimes be reconstructed. We encourage the bill's sponsors to address this issue by directing the Federal Trade Commission to clearly identify which technologies do indeed render consumer data indecipherable and unusable.

We are particularly pleased that the bill focuses on the activities of information brokers, defined as commercial entities whose business is to collect, assemble, or maintain personal information concerning individuals with the purpose of selling such information to unaffiliated third parties. We agree that information brokers should maximize the accuracy and accessibility of their records, as well as provide consumers with a process to dispute information. In addition, the provisions requiring information brokers to submit their security policies to the FTC, as well as to undergo potential FTC post-breach audits, will foster accountability and enforcement of this bill.

We strongly favor the provision that permits State attorneys general and other officials or agencies of the State to bring enforcement actions against any entity that engages in conduct violating this bill. High profile cases such as ChoicePoint and TJX have demonstrated that State attorneys general, in particular, have been at the forefront of notice of data breach issues and have played an invaluable role in addressing identity theft and data breach. This bill arms State officials with strong enforcement tools to ensure compliance with the law. Consumers' personal information will be better protected.

In closing, I want to thank you for the opportunity to speak before you today in support of the Data Security and Breach Notification Act of 2010. Consumers Union appreciates the Subcommittee's interest in addressing issues of data security and consumer privacy. We believe that the passage of this bill will give rise to responsible data security policies and will increase consumer confidence in the marketplace.

Thank you.

[The prepared statement of Ms. Rusu follows:]

PREPARED STATEMENT OF IOANA RUSU, POLICY COUNSEL, CONSUMERS UNION

Good afternoon Chairman Rockefeller, Ranking Member Hutchinson, and distinguished members of this Committee. My name is Ioana Rusu, Policy Counsel for Consumers Union, the non-profit publisher of *Consumer Reports*®. We appreciate the invitation by the Senate Committee on Commerce, Science, and Transportation to share our perspective on the Data Security and Breach Notification Act of 2010.

In January of this year, over 600,000 Citigroup customers were shocked to discover that their Social Security numbers had been printed on the outside of envelopes containing annual tax statements. In July, a Lincoln National Life Insurance vendor printed a user name and password for agents and authorized brokers in a brochure, which was made readily available on the agent's public website. The login information allowed access to a website containing the medical records, Social Security numbers, addresses, policy numbers, and driver's license numbers of individuals seeking life insurance. And only last year, in one of the largest data security

breaches recorded, malicious spyware compromised around 130 million credit card transactions processed by Heartland Payment Systems, a U.S. payments processing company.

These incidents are not unique or isolated. Almost every day, new data breach incidents lead to identity theft, lost revenue, and decreased consumer confidence in the way their personal information is handled in the marketplace. The incidents often occur through inadvertent disclosures, physical loss of stored paper or electronic records, data theft by company insiders, and data breach by third parties through hacking or malware. Sometimes, these incidents affect ten or twenty consumers. Other times, the private information of hundreds of millions of Americans is compromised.

The ubiquity of security breach incidents today renders the Data Security and Breach Notification Act of 2010 particularly timely and relevant. Consumers Union strongly supports the provisions of this bill. I would like to highlight a number of the bill's provisions, which we believe will best promote consumer data privacy.

First of all, we are pleased that the bill covers not only business entities, but also non-profit organizations, including private universities. Personal consumer data must be safeguarded by all those to whom it is entrusted, without regard to for-profit or non-profit status. Consumers face the same risks when their information is compromised, whether or not the source of the compromise is a for-profit entity. As a result, we commend the bill's scope. This provision will provide more meaningful protection for consumer information.

In addition, we applaud the bill's notification provisions, which require covered entities to provide notice of security breach within 60 days of the breach. The sooner consumers are made aware of the breach, the quicker they can take remedial action such as closely monitoring their credit, checking their financial statements frequently, placing a Federal fraud alert on their credit files, and placing a security freeze on their consumer credit files. The instances in which a covered entity may exceed the 60-day deadline are appropriate and narrowly tailored.

We also support the bill's requirements that covered entities provide at least 2 years of free credit reports or credit monitoring following a notice of breach. Consumers should not have to bear the costs of securing personal information when a data breach is caused by a company's inadequate data security practices.

The exemption in the bill, allowing covered entities to avoid the bill's requirements only as long as there is "no reasonable risk of identity theft, fraud, or other unlawful conduct," is also narrowly tailored.

However, we have some concern that, under this bill, all data breach incidents involving encrypted information, defined in the bill as information that has been rendered "unusable, unreadable, or indecipherable," would automatically be presumed to present "no reasonable risk of identity theft, fraud, or other unlawful conduct." While that may be true in most cases, data rendered "unusable or unreadable" can sometimes be reconstructed. We encourage the bill's sponsors to address this issue by directing the Federal Trade Commission to clearly identify which technologies do, indeed, render consumer data indecipherable and unusable.

We also support the bill's definition of "personally identifiable information," which includes not only an individual's name, in combination with one other listed data element, but also an individual's address or phone number, combined with one of the listed data elements. We believe including an individual's address and phone number is important due to the use of reverse search directories, which can reveal the person's name as long as an address or phone number is provided.

We are particularly pleased that the bill focuses on the activities of information brokers, defined as commercial entities whose business is to collect, assemble, or maintain personal information concerning individuals with the purpose of selling such information to unaffiliated third parties. We strongly support the provisions instructing information brokers to maximize the accuracy and accessibility of their records, as well as to provide consumers with a process to dispute information. In addition, the provisions requiring information brokers to submit their security policies to the FTC, as well to undergo potential FTC post-breach audits, will foster accountability and enforcement of this bill.

We strongly favor the provision that permits State Attorneys General and other officials or agencies of the state to bring enforcement actions against any entity that engages in conduct violating the bill. High-profile cases such as ChoicePoint and TJX have demonstrated that state attorneys general, in particular, have been at the forefront of notice of data breach issues, and have played an invaluable role in addressing identity theft and data breach. This bill arms state officials with strong enforcement tools to ensure compliance with the law. Consumers' personal information will be better protected.

In closing, I want to thank you for the opportunity to speak before you today in support of the Data Security and Breach Notification Act of 2010. Consumers Union appreciates this committee's interest in addressing issues of data security and consumer privacy. We believe that the passage of this bill will give rise to responsible data security policies and will increase consumer confidence in the marketplace.

Senator PRYOR. Thank you.
Mr. Pratt.

**STATEMENT OF STUART K. PRATT, PRESIDENT AND CEO,
CONSUMER DATA INDUSTRY ASSOCIATION**

Mr. PRATT. Chairman Pryor and Ranking Member Wicker: thank you for this opportunity to discuss S. 3742. Today my testimony will focus on the value of our members' products, the sufficiency of current laws which regulate them, and specific comments on the bill.

The use of our members' products protects consumers from criminal acts, such as identity theft, and ensure that they are treated fairly in the marketplace. Beneficial uses include preventing money laundering, making fair and sound underwriting decisions, researching fugitives, reducing government entitlement fraud, ensuring that pedophiles don't work in day care centers, and improving disaster assistance responses and services to victims.

With these uses in mind, let me turn to the relevant Federal laws which are on the books today. The U.S. is at the forefront of establishing sector-specific laws regulating the uses of personal information of many types. The list of laws is extensive, but let me focus on two of these in greater detail.

First, the Fair Credit Reporting Act regulates any use of personal information which is used to make decisions, such as approval of a credit application. Due to the fact that data regulated by the FCRA is used to make decisions, the law provides consumers with a full complement of rights, such as access, correction, as well as receiving notices regarding adverse action in risk-based decisions. Further, furnishers must provide accurate data to consumer reporting agencies and consumer reporting agencies must load that data accurately.

Data regulated under the Gramm-Leach-Bliley Act is not used to make a yes-or-no decision, but GLB does impose strict limitations on how nonpublic personal information can be used. Many of our members' fraud prevention systems are regulated by GLB and annually U.S. businesses conduct an average of 2.6 billion searches to check for fraud.

Our members' location services are also regulated by GLB. Annually, hundreds of millions of searches are conducted to enforce child support orders, and contracts to pay debts. Pension funds use them to locate beneficiaries. Blood donor organizations ensure sufficient and safe blood supplies, as well as organizations focused on missing and exploited children.

With both an understanding of our members' products and the laws that regulate them, let me now turn to S. 3742 and start by stating unequivocally that CDIA's members agree that sensitive personal information should be protected and that consumers should receive breach notices where there is a significant risk of them becoming a victim of identity theft. Though we support these

goals, we believe provisions of S. 3742 need improvement. Further, it is our view that the information broker provisions should be struck.

To expand on this last point, let me touch on just some of the problems with the information broker provisions. These provisions impose accuracy, access, and correction standards to anyone defined as an information broker. However, on what industry or product the information broker provisions are intended to focus is very unclear. For example, the definition does not expressly and completely exclude consumer reporting agencies under the Fair Credit Reporting Act or financial institutions under GLB. This lack of clarity of scope and overlap with other Federal laws creates problems.

For example, it creates a system of double jeopardy under FCRA. Rather than fully exempt consumer reporting agencies, the bill proposes an exception which establishes an "in compliance with" test. In essence, a consumer reporting agency under FCRA is also an information broker under this proposal where the consumer reporting agency is not in compliance with FCRA.

Further, applying accuracy, access, and correction standards to fraud prevention and location tools can erode the performance of the very tools which are most effective in protecting consumers. None of these are used to deny or approve an application and the application of these standards does not make sense.

Regarding the data security provisions of the bill, while CDIA supports the creation of a national standard, we believe that it is also critical that such a standard does not interfere with the regulation of products governed by other Federal laws. The bill currently stipulates that a company is exempt from the data security standard only when it is "in compliance with" a similar standard found in another law. As discussed above, this "in compliance with" approach imposes two sets of duties, two sets of costs, two sets of liabilities, on that company. We urge the Committee to adjust the exception so the company is exempt where it is subject to a similar standard in another law.

In closing, CDIA also applauds the intent of this bill to set a true uniform national standard for data security and breach notification. However, the exception to this preemption standard which attempts to preserve State laws swallows the rule. Congress should not enact a 51st law. A true national standard will benefit consumers because they will enjoy the benefits of this standard no matter where they live.

We thank you again for giving us the opportunity to testify, and I'm happy to answer any questions.

[The prepared statement of Mr. Pratt follows:]

PREPARED STATEMENT OF STUART K. PRATT, PRESIDENT AND CEO,
CONSUMER DATA INDUSTRY ASSOCIATION

Chairman Rockefeller, Ranking Member Hutchison and members of the Committee, thank you for this opportunity to appear before you today to discuss S. 3742, the Data Security and Breach Notification Act of 2010. For the record, my name is

Stuart K. Pratt and I am President and CEO of the Consumer Data Industry Association.¹ My testimony will focus on:

- The value and importance of the data systems and analytical tools our members produce.
- The sufficiency of current laws which regulate our members' products.
- Comments on S. 3742.

CDIA Members' Data and Technologies Help Both the Public and Private Sectors to Manage Risk and Protect Consumers

Whether it is counter terrorism efforts, locating a child who has been kidnapped, preventing a violent criminal from taking a job with access to children or the elderly or ensuring the safety and soundness of lending decisions our members' innovative data bases, software and analytical tools are critical to how we manage risk in this country, ensure fair treatment and most importantly, how we protect consumers from becoming victims of both violent and white-collar crimes of all types.

Following are examples of how our members' products, software and data bases bring material value to consumers and our country:

- Helping public and private sector investigators to prevent money laundering and terrorist financing.
- Ensuring lenders have best-in-class credit reports, credit scoring technologies, income verification tools and data on assets for purposes of making safe and sound underwriting decisions so that consumers are treated fairly and products make sense for them.
- Bringing transparency to the underlying value of collateralized debt obligations and in doing so ensuring our Nation's money supply is adequate which militates against the possibility and severity of economic crises.
- Enforcing child support orders through the use of sophisticated location tools so children of single parents have the resources they need.
- Assisting law enforcement and private agencies which locate missing and exploited children through location tools.
- Researching fugitives, assets held by individuals of interest through the use of investigative tools which allow law enforcement agencies tie together disparate data on given individuals and thus to most effectively target limited manpower resources.
- Witness location through use of location tools for all types of court proceedings.
- Reducing government expense through entitlement fraud prevention, eligibility determinations, and identity verification.
- Making available both local and nationwide background screening tools to ensure, for example, that pedophiles don't gain access to daycare centers or those convicted of driving while under the influence do not drive school buses or vans for elder care centers.
- Helping a local charity hospital to find individuals who have chosen to avoid paying bills when they have the ability to do so.
- Producing sophisticated background screening tools for security clearances, including those with national security implications.
- Improving disaster assistance responses through the use of cross-matched data bases that help first-responders to quickly aid those in need and prevent fraudsters from gaming these efforts for personal gain.

Not only do our members' technologies and innovation protect us and ensure that we are managing risk in this country, but they reduce costs and labor intensity. Risk management is not merely the domain of the largest government agencies or corporations in America, it is available to companies of all sizes thanks to our members' investments. Consider the following scenarios:

Scenario 1—Effective Use of Limited Resources

The following example was given during a Department of Homeland Security meeting on use of data by the department:

¹ CDIA, as we are commonly known, is the international trade association representing over 300 consumer data companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, systems for insurance underwriting, skip-tracing tools, law enforcement investigative systems and also collection services.

“One extremely well-known law enforcement intelligence example from immediately post-9/11 was when there was a now well-publicized threat . . . that there might be cells of terrorists training for scuba diving underwater bombing, similar to those that trained for 9/11 to fly—but not land—planes. How does the government best acquire that? The FBI applied the standard shoe-leather approach—spent millions of dollars sending out every agent in every office in the country to identify certified scuba training schools. The alternative could and should have been for the Federal Government to be able to buy that data for a couple of hundred dollars from a commercial provider, and to use that baseline and law enforcement resources, starting with the commercial baseline.”

Scenario 2—Lowering Costs/Expanding Access to Best-in-Class Tools

One commercial database provider charges just \$25 for an instant comprehensive search of multiple criminal record sources, including fugitive files, state and county criminal record repositories, proprietary criminal record information, and prison, parole and release files, representing more than 100 million criminal records across the United States. In contrast, an in-person, local search of one local courthouse for felony and misdemeanor records takes 3 business days and costs \$16 plus courthouse fees. An in-person search of every county courthouse would cost \$48,544 (3,034 county governments times \$16). Similarly, a state sexual offender search costs just \$9 and includes states that do not provide online registries of sexual offenders. An in-person search of sexual offender records in all 50 states would cost \$800.

Scenario 3—Preventing Identity Theft & Limiting Indebtedness

A national credit card issuer reports that they approve more than 19 million applications for credit every year. In fact they process more than 90,000 applications every day, with an approval rate of approximately sixty percent. This creditor reports that they identify one fraudulent account for every 1,613 applications approved. This means that the tools our members provided were preventing fraud in more than 99.9 percent of the transactions processed. These data also tell us that the lender is doing an effective job of approving consumers who truly qualify for credit and denying consumers who are overextended and should not increase their debt burdens.

Current Laws Regulating Our Members Are Robust

The United States is on the forefront of establishing sector-specific and enforceable laws regulating uses of personal information of many types. The list of laws is extensive and includes but is not limited to the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*), The Gramm-Leach-Bliley Act (Pub. L. 106–102, Title V), the Health Insurance Portability and Accountability Act (Pub. L. 104–191), and the Drivers Privacy Protection Act (18 U.S.C. 2721 *et seq.*).

Following are more probative descriptions of some of these laws, the rights of consumers and also the types of products that fall within the scope of the law.

Fair Credit Reporting Act

Key to understanding the role of the FCRA is the fact that it regulates any use of personal information (whether obtained from a public or private source) defined as a consumer report. A consumer report is defined as data which is gathered and shared with a third party for a determination of a consumer’s eligibility for enumerated permissible purposes. This concept of an eligibility test is a key to understanding how FCRA regulates an extraordinarily broad range of personal information uses. The United States has a law which makes clear that any third-party-supplied data that is used to accept or deny, for example, my application for a government entitlement, employment, credit (*e.g.*, student loans), insurance, and any other transaction initiated by the consumer where there is a legitimate business need. Again, this law applies equally to governmental uses and not merely to the private sector and provides us as consumers with a full complement of rights to protect and empower us. Consider the following:

- The right of access—consumers may request at any time a disclosure of all information in their file at the time of the request. This right is enhanced by requirements that the cost of such disclosure must be free under a variety of circumstances including once per year upon request, where there is suspected fraud, where a consumer is unemployed and seeking employment, when a consumer places a fraud alert on his or her file, or where a consumer is receiving public assistance and thus would not have the means to pay. Note that the right of access is absolute since the term file is defined in the FCRA and it includes the base information from which a consumer report is produced.

- The right of correction—a consumer may dispute any information in the file. The right of dispute is absolute and no fee may be charged.
- The right to know who has seen or reviewed information in the consumer's file—as part of the right of access, a consumer must see all “inquiries” made to the file and these inquiries include the trade name of the consumer and upon request, a disclosure of contact information, if available, for any inquirer to the consumer's file.
- The right to deny use of the file except for transactions initiated by the consumer—consumers have the right to opt out of non-initiated transactions, such as a mailed offer for a new credit card.
- The right to be notified when a consumer report has been used to take an adverse action. This right ensures that I can act on all of the other rights enumerated above.
- Beyond the rights discussed above, with every disclosure of a file, consumers receive a notice providing a complete listing all consumer rights.
- Finally, all such products are regulated for accuracy with a “reasonable procedures to ensure maximum possible accuracy” standard. Further all sources which provide data to consumer reporting agencies must also adhere to a standard of accuracy which, as a result of the FACT Act, now includes new rule-making powers for Federal agencies.

Gramm-Leach-Bliley Act

Not all consumer data products are used for eligibility determinations regulated by the FCRA. Congress has applied different standards of protection that are appropriate to the use and the sensitivity of the data. We refer to these tools as Reference, Verification and Information services or RVI services. RVI services are used not only to identify fraud, but also to locate and verify information for the public and private sectors.

Fraud prevention systems, for example, aren't regulated under FCRA because no decision to approve or deny is made using these data. Annually businesses conduct an average more than 2.6 billion searches to check for fraudulent transactions. As the fraud problem has grown, industry has been forced to increase the complexity and sophistication of the fraud detection tools they use. While fraud detection tools may differ, there are four key models used.

- *Fraud data bases*—check for possible suspicious elements of customer information. These data bases include past identities and records that have been used in known frauds, suspect phone numbers or addresses, and records of inconsistent issue dates of SSNs and the given birth years.
- *Identity verification products*—crosscheck for consistency in identifying information supplied by the consumer by utilizing other sources of known data about the consumer.

Identity thieves must change pieces of information in their victim's files to avoid alerting others of their presence. Inconsistencies in name, address, or SSN associated with a name raise suspicions of possible fraud.

- *Quantitative fraud prediction models*—calculate fraud scores that predict the likelihood an application or proposed transaction is fraudulent. The power of these models is their ability to assess the cumulative significance of small inconsistencies or problems that may appear insignificant in isolation.
- *Identity element approaches*—use the analysis of pooled applications and other data to detect anomalies in typical business activity to identify potential fraudulent activity. These tools generally use anonymous consumer information to create macro-models of applications or credit card usage that deviates from normal information or spending patterns, as well as a series of applications with a common work number or address but under different names, or even the identification and further attention to geographical areas where there are spikes in what may be fraudulent activity.

The largest users of fraud detection tools are financial businesses, accounting for approximately 78 percent of all users. However, there are many non-financial business uses for fraud detection tools. Users include:

- *Governmental agencies*—Fraud detection tools are used by the IRS to locate assets of tax evaders, state agencies to find individuals who owe child support, law enforcement to assist in investigations, and by various Federal and state agencies for employment background checks.

- *Private use*—Journalists use fraud detection services to locate sources, attorneys to find witnesses, and individuals use them to do background checks on childcare providers.

CDIA's members are also the leading location services providers in the United States. These products are also not regulated under FCRA since no decision is based on the data used. These services, which help users locate individuals, are a key business-to-business tool that creates great value for consumers and business alike. Locator services depend on a variety of matching elements. Consider the following examples of location service uses of a year's time:

- There were 5.5 million location searches conducted by child support enforcement agencies to enforce court orders. For example, the Financial Institution Data Match program required by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PL 104-193) led to the location of 700,000 delinquent individuals being linked to accounts worth nearly \$2.5 billion.
- There were 378 million location searches used to enforce contractual obligations to pay debts.
- Tens of millions of searches were conducted by pension funds (location of beneficiaries), lawyers (witness location), blood donors organizations (blood supply safety), as well as by organizations focused on missing and exploited children.
- There were 378 million location searches used to enforce contractual obligations to pay debts.
- Tens of millions of searches were conducted by pension funds (location of beneficiaries), lawyers (witness location), blood donors organizations, as well as by organizations focused on missing and exploited children.

Clearly RVI services bring great benefit to consumers, governmental agencies and to businesses of all sizes. Laws such as the Gramm-Leach-Bliley Act and Fair Credit Reporting Act are robust, protective of consumer rights, but also drafted to ensure that products used to protect consumers, prevent fraud and to locate individuals are allowed to operate for the good of consumers and business.

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

Now let me turn to S. 3742. CDIA is pleased to provide our comments on the bill as a whole and in particular on provisions which propose to regulate and entity called an "information broker."

Let me start by stating unequivocally that CDIA's members agree that sensitive personal information should be protected. CDIA agrees that consumers should receive breach notices when there is a significant risk of them becoming victims of identity theft. Our members agree with the Federal Trade Commission recommendation offered in multiple testimonies on the Hill and via their joint Task Force report issued along with the Department of Justice that if a Federal statute is to be enacted, it should be a true national standard and that it should focus on safeguarding sensitive personal information and notifying consumers when a breach has occurred which exposes the consumer to a significant risk of becoming a victim of identity theft. Though our members support these goals, we believe provisions of S. 3742 need improvement and it is also our view that the provisions which propose to regulate an entity defined as an "information broker" should be struck. Following are more detailed comments regarding the bill.

Information Broker

This section of the bill imposes accuracy, access and correction standards to a certain type of entity defined as an information broker. It is still unclear to us on what industry the information broker provisions are intended to focus. We believe the provision should be struck from the bill and encourage the focus of this bill to be on data security and breach notification. Following are concerns we have with this provision:

Double Jeopardy with FCRA: As discussed above, consumer reporting agencies which compile and maintain data for purposes of producing consumer reports which are used for eligibility determinations are regulated under the FCRA. These products are subject to accuracy, access and correction standards. The definition of "information broker" does not expressly exclude consumer reporting agencies (FCRA). Rather than fully exempt consumer reporting agencies, the bill proposes an exception which establishes an "in compliance with" test. In essence a consumer reporting agency is regulated as a consumer reporting agency under FCRA and also as an "information broker" under this proposal where the consumer reporting agency is not in compliance with FCRA. CDIA appreciates

the effort to exclude consumer reporting agencies via Section 2(b)(3)(C) but we oppose this approach to an exception. By contrast in Section 2(c) the bill unequivocally exempts certain service providers. Consumer reporting agencies as defined under FCRA should not be considered information brokers in any context.

Interference with Fraud Prevention, Identity Protection and Location Services— RVI products such as those designed for fraud prevention and location are produced under laws such as the Gramm-Leach-Bliley Act and Section 5 of the Federal Trade Commission Act. financial institutions (GLB). The definition of information broker does not exclude financial institutions regulated under GLB. Therefore products developed under the data-use limitations found in GLB Title V, Section 502(e) are adversely affected by the information broker provision.

Neither a product developed for fraud prevention nor location should be subject to accuracy, access and correction standards since neither product is used to deny or approve an application, etc. If they were designed for the purpose of making decisions about a consumer's eligibility, then they would already be regulated under the FCRA.

Consider the effect of the information broker duties on fraud tools. While Section 2(b)(3)(A)(ii) provides a limited exception for fraud data bases consisting of inaccurate information, the exception is not sufficient, though we do applaud the effort to try and address the problem of imposing an accuracy standard on fraud tools. Fraud prevention tools are built based on data about consumers, data about confirmed fraud attempts, data about combinations of accurate and inaccurate data used for fraud attempts and more. Fraud tools are designed to identify transactions or applications that are likely to be fraudulent in order to allow the user to take additional steps to prevent the crime and still process legitimate transactions. The current exception does not appear to address all types of fraud prevention tools used today and further the limitations of the exception impose statutory rigidity that will prevent the design of new tools as the strategies of the criminals change. It is our view that applying an accuracy standard to any aspect of a fraud prevention system that is not used to stop a transaction or used to make a yes-or-no decision does not make sense.

Similarly it is wrong to subject fraud prevention tools to be subject to an access and correction regime. While Section 2(b)(3)(iv) attempts to exclude fraud prevention tools from the duty to disclose (and therefore any right to dispute data), the exception is tied to a variety of tests such as where the use of the tool would be "compromised by such access." It is our view that fraud tools, because they are not used to make decisions, should be absolutely excluded from duties to disclose. If details of a fraud tool are disclosed it is akin to disclosing the recipe for fraud prevention. The fact that the exception to disclosure is not absolute leaves open the risk that a tool will have to be disclosed which simply reduces the value of fraud prevention tools which are protecting consumers. This result works against the premise of the bill which is to protect consumer's from crime, particularly identity theft.

As discussed in this testimony, location services are materially important to how risk is managed. These tools are not designed to be used for decisionmaking and thus are not regulated under the FCRA, which already regulates all data used for eligibility decisions (including the imposition of accuracy, access and correction rights). Location services cannot have an accuracy standard applied to them as this bill would propose. The tools are about helping local law enforcement investigate crimes, attorneys to locate witnesses, and Federal agencies to cross match data in the pursuit of kidnappers, etc., nonprofit hospitals to collect debts from patients who have the ability to pay but refuse to do so and in the enforcement of child support orders. These systems are designed to, for example, help a user identify possible connections between disparate records and ultimately possible locations for the subject of the search. Measuring the quality of the possible connections is not akin to an accuracy standard, nor should an accuracy standard be applied to "possible matches." Further, providing access to a database for purposes of error correction could affect the quality of the systems since matches are sometimes based on combinations of accurate and inaccurate data. Ultimately, the data is not used to deny a consumer access to goods or services and thus CDIA opposes the application of accuracy, access and correction duties to these fraud prevention systems or RVI services.

Information Brokers and Audit Logs

Section 2(b)(4) establishes a duty for information brokers to maintain an audit logs for accessed or transmitted information. Such a duty is appropriate to a database used for eligibility and thus is appropriate under the FCRA. CDIA urges the

Committee to reject the application of such a concept to data systems which are not used to determine eligibility. Audit systems impose costs on business both small and large. Based on even the current limited exceptions to information broker duties to ensure accuracy and provide access and correction, it appears that an audit log must be maintained.

Harmonizing Data Security Standards

While CDIA's members support the creation of a national standard for data security, we believe that it is also critical that such a standard not interfere with the operation of other Federal laws which already exist. To accomplish this, additional work must be done to fine-tune the exception in the current bill. Allowing a company to be exempt from a data security standard only when it is "in compliance with" a similar standard found in another law imposes two sets of duties, two sets of costs and two sets of liability on that company. For CDIA's largest and smallest businesses this is an unnecessary burden. For our smallest businesses this duty likely increases the costs of the Errors and Omissions insurance policies which have to cover this dual liability risk. We urge the Committee to adjust the exception so that is not an "in compliance with" test and to instead use a "subject to" test.

FTC Website for Publishing Breaches

The bill requires covered entities to report any breach to the Federal Trade Commission and further it requires the FTC to publish the fact of these breaches on a website. The fact that the bill has a breach notification standard ensures that all affected consumers are notified when there's a risk of being harmed by the breach. CDIA agrees that notices to consumers who are at significant risk of becoming a victim of identity theft makes sense. However, publishing the names of companies does not. A company could have deployed best-in-class technologies and procedures and still have been affected by the criminal actions of rogue employees or new technologies used by an organized gang. The business or governmental agency which suffered the breach due to criminal actions is a victim of a crime. The publication of the names of those who have suffered a breach would imply that the business did not work hard, did not care about their customers and by these implications, the publication of names imposes a guilty verdict on their good names, no matter how hard the business had worked to protect the data and no matter how responsible they were in working to protect their customers following a breach. We urge the Committee to strike this provision.

Preemption

CDIA applauds the intent of this bill to set uniform national standards for data security and breach notification. However, the exception to this preemptive standard, which attempts to preserve state laws, swallows the rule. Congress should not enact a fifty-first law. A true national standard will benefit consumers because they will enjoy the benefits of this standard no matter where they live.

Enforcement

CDIA believes that the preservation of uniform national standards for data security and breach notification are best achieved by limiting the enforcement of the law to a single Federal agency, in this case the Federal Trade Commission. By extending the enforcement powers to state attorneys general, which in turn can designate any other "official or agency of the state" to bring enforcement actions, as well will not increase a company's desire to comply but will lead to experimental litigation that may simply diminish the true national standard the bill sets out to establish. Further, the same issues and same facts of a given incident should not be open for multiple lawsuits. CDIA operates an errors and omissions insurance program for its small-business members and it is our experience that policy costs will rise where there is additional exposure. Even larger members who self-insure simply have to set aside more money for litigation rather than investing it in research and development. We urge the Committee to limit enforcement to the FTC.

Conclusion

We thank you again for giving us this opportunity to testify. It is only through such dialogue that good laws are enacted. We welcome continued dialogue on S. 3742 and I'm happy to answer any questions.

Senator PRYOR. Ms. Bianchi.

**STATEMENT OF MELISSA BIANCHI, HOGAN LOVELLS U.S. LLP,
ON BEHALF OF THE AMERICAN HOSPITAL ASSOCIATION**

Ms. BIANCHI. Good afternoon, Chairman Pryor and Ranking Member Wicker. My name is Melissa Bianchi and I'm here today to testify on behalf of the American Hospital Association. Thank you for the opportunity to share the AHA's views today.

The AHA represents nearly 5,000 member hospitals, health systems, and other health care organizations, as well as 38,000 individual members. Our member hospitals are dedicated to safeguarding the privacy of their patients' personal information and are experienced in protecting this data.

As I'll discuss today, hospitals are deeply familiar with the type of obligations that are proposed in this legislation and indeed already are subject to a very similar regulatory framework. In the past, Congress has recognized this by exempting hospitals from duplicate regulatory requirements and we believe that a similar approach make sense here.

The Department of Health and Human Services has established detailed requirements under HIPAA for how hospitals must protect the privacy and security of the patient information they maintain. In 2009, Congress strengthened the HIPAA privacy and security requirements, as well as established new security breach requirement for HIPAA-covered entities. Under the HITECH Act, part of ARRA, HIPAA now contains stronger enforcement mechanisms and higher penalties for noncompliance. State attorneys general now have the power to bring enforcement actions under HIPAA and patients have more rights with respect to their own information. Also under HITECH, the HIPAA rules apply now not only to HIPAA-covered entities, but also directly apply to their subcontractors, known as business associates.

The protections proposed under this legislation duplicate those already in place under HIPAA. For hospitals and other HIPAA-covered entities, this act would require a whole new set of compliance activities that largely mirror HIPAA. This act also may subject hospitals to two parallel sets of enforcement activities. Penalties could apply under each set of requirements. Requiring HIPAA-covered entities to establish compliance standards for two different regulatory systems will be costly.

Because hospitals already must meet HIPAA's stringent data security standards, these additional compliance costs will not afford consumers any greater protection. Indeed, if hospitals are required to send both an HHS and an FTC notice to consumers in the event of a security breach, it will be confusing. In order for a consumer notice of a security breach to be meaningful, it is important that consumers not receive multiple notices of a single data breach.

The HIPAA rules apply to protected health information. Basically, this is health information that is held by a HIPAA-covered entity. Protected health information includes demographic information like a person's name and address. It includes payment information, such as credit card information or checking account information that a patient uses to pay for care. Generally, all identifiable information about a patient that is held by a hospital is protected by HIPAA.

HIPAA contains detailed requirements for maintaining the security and privacy of health information, and that includes electronic health information. Covered entities must put safeguards in place to protect the confidentiality, the integrity, and the security of this information, and these requirements cover virtually every circumstance in which patient information is stored or transmitted in the health care setting.

HIPAA regulations include new rules for responding to security breaches as the result of HITECH. A HIPAA-covered entity is required to notify each individual whose information is breached and also must notify HHS. For larger breaches, a hospital must also notify the media. HHS posts a list of breaches on its website.

The HITECH Act also establishes security breach requirements for a different kind of information, personal health records. These are records that any one of us can set up on a publicly available website to store our own health information ourselves. This information is not protected by HIPAA because it's not maintained by a HIPAA-covered entity. Instead, the information is maintained by the vendor of the website. In this case, the FTC regulates these entities.

These two sets of security breach rules do not overlap. This is because Congress recognized in HITECH that there is an existing privacy framework for HIPAA-covered entities, and we believe that this same approach makes sense going forward. HIPAA-covered entities and their business associates are fully and vigorously regulated by HHS. They are obligated to comply with detailed requirements designed to protect the security of patient information in both paper and electronic form. Where those systems fail, they must notify patients. Requiring HIPAA-covered entities and their business associates to develop two parallel compliance programs, set up by two different Federal agencies, will be cumbersome and costly for both hospitals and for patients, but it will not increase the security of patient information.

We appreciate the Subcommittee's interest in these issues and we thank you for the opportunity to testify.

[The prepared statement of Ms. Bianchi follows:]

PREPARED STATEMENT OF THE AMERICAN HOSPITAL ASSOCIATION

The American Hospital Association (AHA), on behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our 38,000 individual members, appreciates the opportunity to share its views on the Data Security and Breach Notification Act of 2010. This proposed legislation would require the Federal Trade Commission (FTC) to establish regulations requiring a broad range of entities, including many hospitals, to implement security practices to protect personal information and to provide for notification in the event of any security breaches of that information.

Hospitals already are regulated in this area. In the past, Congress has recognized this by exempting hospitals from duplicate regulatory requirements. We believe that a similar approach makes sense here.

My testimony will focus on the following:

- The scope and requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and how HIPAA protections for patient information recently have been strengthened.
- How the FTC and the Department of Health and Human Services (HHS) currently operate parallel and separate rules for security breaches.
- Why this approach—exempting HIPAA covered entities from the FTC rules—makes sense.

America's hospitals are dedicated to safeguarding the privacy of their patients' medical information. The AHA and its members have supported efforts by the Department of Health and Human Services (HHS) to implement HIPAA. Under HIPAA, HHS has established detailed requirements for how HIPAA covered entities must protect the privacy and security of the patient information they maintain. These include rules for notifying patients in the event of a security breach. Hospitals are deeply familiar with the type of obligations proposed in this legislation, and indeed already are subject to a very similar regulatory framework.

HIPAA was first enacted in 1996. In 2009, Congress strengthened the HIPAA privacy and security requirements as well as created a Federal framework for data breach notification for HIPAA covered entities. Under the HITECH Act—part of the American Recovery and Reinvestment Act of 2009—HIPAA now contains stronger enforcement mechanisms and higher penalties for noncompliance. State attorneys general now have the power to bring enforcement actions under HIPAA, in addition to HHS. The HITECH Act also gave more rights to patients. Patients now have an even greater ability to control how their information is used and to whom it is disclosed. Perhaps the most significant change under the HITECH Act is that the HIPAA rules now apply not only to HIPAA covered entities, but also directly apply to their subcontractors, known as business associates.

The protections proposed under the Data Security and Breach Notification Act duplicate those already in place under HIPAA. For hospitals and other HIPAA covered entities this Act would require a whole new set of compliance activities that largely mirror HIPAA. This Act may also subject hospitals to two parallel sets of enforcement activities; penalties could apply under each set of requirements. Requiring HIPAA covered entities to establish compliance standards for two different regulatory regimes will cost hospitals money. Because hospitals already must meet HIPAA's stringent data security standards, these additional compliance costs will not afford consumers any greater protection.

Information Protected by HIPAA

The HIPAA privacy and security rules apply to "protected health information." Basically, this is health information that is held by a HIPAA covered entity. It is information that either directly identifies an individual or for which there is a reasonable basis to believe that an individual could be identified. Protected health information includes demographic information, like a person's name and address. It includes payment information—such as credit card information or checking account information—that a patient uses to pay for care. Generally, all identifiable information about a patient that is held by a hospital is protected health information and is governed by HIPAA.

For almost a decade, HIPAA has provided a comprehensive framework for protecting the privacy and security of this patient information. The AHA's members are experienced in taking the steps necessary—and required by HIPAA—to protect patient information. The HIPAA regulations include a number of components—most importantly, baseline privacy regulations as well as security regulations that apply specifically to electronic information. The privacy regulations under HIPAA impose detailed rules about how a hospital may use patient information and when and to whom a hospital may disclose that information to another party.

For example, a hospital is allowed to use all of the information in a patient's medical record to treat a patient. Not all information, however, can be sent to a health plan to obtain payment for that care. The privacy regulations contain rules for almost every circumstance. There are rules about when a hospital can disclose patient information to a subcontractor—or business associate. There are rules establishing when a hospital must seek special permission from a patient before using that patient's information, such as to conduct research. There are rules for when and how patient information may be disclosed pursuant to a subpoena. And there are rules about how the information on minors and on deceased patients can be used. Hospitals simply do not and cannot do anything with patient information without referring to the HIPAA requirements.

HIPAA also contains security requirements. These are detailed requirements for maintaining the security of electronic information. HIPAA covered entities must put in place safeguards to protect the confidentiality, integrity, and security of electronic protected health information. As with the privacy requirements, these security requirements cover virtually every circumstance under which patient information is stored or transmitted electronically in the hospital setting. For example, a hospital must have a process in place for identifying and assessing reasonably foreseeable vulnerabilities in its information systems. Corrective actions are required to address any vulnerabilities identified.

HIPAA requires its covered entities to take a number of steps to comply with the privacy and security regulations. Hospitals are required to have detailed HIPAA policies and procedures and to train their employees on those practices. They also must appoint a privacy official and a security official responsible for managing the privacy and security practices.

HIPAA Requirements for Security Breaches

In addition to detailed privacy and security regulations, the HIPAA regulations include new rules for responding to security breaches. This is a result of the HITECH Act. A HIPAA covered entity, such as a hospital, is required to notify each individual whose information is breached. For larger breaches—those involving the health information of 500 or more individuals—a hospital also must notify the media. The Secretary of HHS also must be notified of all breaches, big and small. HHS posts a list of breaches on its website.

The HIPAA breach regulations include specific requirements for how individuals must be notified. These reflect the requirements Congress established under the HITECH Act. For example, individuals must be notified of a breach without unreasonable delay, and no later than 60 days after the breach is discovered. The notice must be in writing; it must describe the type of information breached and the steps individuals should take to protect themselves from potential harm resulting from the breach. HIPAA covered entities already are obligated to carry out the kinds of security breach activities that this proposed legislation requires.

Separate Rules for HIPAA and Non-HIPAA Entities

The HITECH Act established two parallel sets of rules for security breaches. One is under HIPAA, governed by HHS. Another set of rules covers a different kind of information—personal health records. These are records that any one of us can set up on a publicly available website to store our health information ourselves. They can contain personal, sensitive information. But the information isn't protected by HIPAA, because it is not maintained by a hospital or other HIPAA covered entity. Instead, the information is maintained by the vendor of the website and by the consumer. For these kinds of records, the Federal Trade Commission has authority to set the rules.

These two sets of security breach rules don't overlap. This is because, in the HITECH Act, Congress recognized that there is an existing privacy framework for HIPAA covered entities. Congress established a separate set of breach requirements under HIPAA and excluded HIPAA covered entities from the new FTC requirements. The AHA believes that this same approach makes sense going forward. Hospitals already follow a strict set of requirements for protecting patient information and for addressing security breaches.

Subjecting HIPAA covered entities and their business associates to the Data Security and Breach Notification Act would require hospitals to establish two parallel compliance programs, set up by two different Federal agencies. One to meet the long-standing HIPAA requirements, and another to comply with the FTC regulations that would be developed under this legislation. Inevitably, this will increase a hospital's compliance costs, but without increasing the security of patient information. Hospitals already are responsible for protecting patient information. Increased compliance costs have the effect of increasing health care costs, a result none of us wants.

There also is the potential that hospitals would be subject to two sets of penalties—one from HHS and one from the FTC—for the same security incident. We understand that under the Act the FTC would have the discretion to determine that HIPAA covered entities and their business associates are deemed in compliance with the Act by virtue of their HIPAA obligations. But even if the FTC takes this step, it is possible that, where a HIPAA covered entity failed to comply with HIPAA, it would be subject not only to the new and enhanced HIPAA penalties, but also to the FTC's penalties.

We believe it also is in the best interest of consumers for HIPAA covered entities and their business associates to be expressly exempted from the Act. If a hospital is required to comply with both the FTC and the HHS rules regarding security breaches, the hospital could be required to send two letters to the same patient for the same security incident. That simply doesn't make sense for patients, and it doesn't increase the protection of their information. In order for consumer notice of security breaches to be meaningful, it is important that consumers not receive multiple notices of a single data breach. It will be confusing for individuals to receive multiple letters about the same breach. If there are too many notices, at some point, letters about security breaches will become just more white noise. Consumers may end up disregarding important information and fail to take steps to protect against

future harm or misuse of their information. Consumers should receive a single notice for a single breach.

HIPAA covered entities and their business associates are fully and vigorously regulated by HHS. They already are obligated to comply with detailed requirements designed to protect the security of patient information. Where those systems fail, they must notify patients of a security breach, as HHS requires. An additional set of rules will be cumbersome and costly, both for hospitals and for patients.

We appreciate the Subcommittee's interest in these issues and thank you for the opportunity to testify.

Senator PRYOR. Thank you.

I'll call on Senator Wicker for his opening statement.

**STATEMENT OF HON. ROGER F. WICKER,
U.S. SENATOR FROM MISSISSIPPI**

Senator WICKER. Thank you very much, Mr. Chairman, and thank you to the witnesses. I was a little late because I was in your seat in another hearing room in another building. But I want to thank the Chair for holding this hearing and for his dedication to this important issue of protecting sensitive personal information. Data breaches over the last decade highlight the need to examine the way businesses and nonprofits currently protect consumer information. We should ensure that strong security features are in place and that consumers receive appropriate notification when a breach of their information occurs, exposing them to identity theft and similar threats.

Congress has been monitoring this issue for several years and I appreciate your efforts, Mr. Chairman, in seeking a comprehensive solution. Let me commit to you today, Mr. Chairman, that I want to work with you before the end of this Congress to co-sponsor a bill and to move it as far as we can toward passage during this calendar year.

The collection of personal information about consumers began as a commercial practice many years ago. Nevertheless, advancements in technology, particularly the continuing development of online commerce and the proliferation of electronic data, increase the amount of personal information that can be collected and maintained by companies and nonprofit organizations. These advancements greatly enhance the convenience for consumers in doing business all over the country. But they also increase the possibility for personal information to be unlawfully acquired and misused.

Data breaches can happen in many ways, ranging from complicated computer schemes created by sophisticated hackers to business records carelessly discarded in a dumpster, for example, behind a store. No matter how the unlawful acquisition of personal information occurs, it can present a real threat to an individual's credit, finances, and peace of mind.

The legislation before us today represents a comprehensive approach that would create a uniform standard throughout the country. Currently, no single Federal standard exists for guarding many types of consumer information.

I want to explore one aspect of the bill further with our witnesses—the interaction between this legislation and data security laws that are already in place. Many entities covered by this bill already act under existing standards, such as the security or notifi-

cation procedures required in the Gramm-Leach-Bliley Act and the HIPAA Act, as we've already received testimony about.

I'm interested to hear from those entities represented here today and from the FTC, who would be enforcing the new regulations, how would the interplay between these laws work and how can we ensure that we do not unintentionally create unnecessary, dual, or even conflicting standards.

Another provision in this bill would impose additional requirements on entities that are considered data brokers. These entities possess large amounts of personal information about consumers. Not surprisingly, as availability of personal data has increased so has the market for businesses to gather and utilize that data. It is important for us to learn more today about how those specific provisions would affect data brokers and their ability to keep data secure and take appropriate measures when that data is breached.

So thank you to all of our witnesses for sharing your time with us. I look forward to the questions and I want to work with each of you to achieve a goal that I know we all share, to ensure that sensitive personal information is protected.

Thank you.

Senator PRYOR. Thank you.

Let me go ahead and start with you, Ms. Mithal, if I may. You talked a little bit about the Rite-Aid case in your opening statement. As I understand it, you worked with the Department of Health and Human Services on that matter. Do you currently under existing Federal law, do you have the authority to file suit and did you do that in that case?

Ms. MITHAL. Yes, we did, Mr. Chairman. One of the things that we were very mindful of in that case is that we wanted to leverage our authority and HHS's authority to get the broadest possible relief for consumers without creating overlapping or duplicative requirements. So for example, HHS was able to get a civil penalty against the company under HIPAA. In our order provisions we didn't get a civil penalty. But our order provisions were much broader in the sense that they covered employee information, and they also covered certain electronic information that was not covered by the HHS order. So I think we worked together to leverage our authority and make sure we got the best result for consumers, without creating duplicative requirements for businesses.

Senator PRYOR. Can you tell us a little bit about the ChoicePoint case? This has come up a couple times. If you could just tell the Subcommittee what that is?

Ms. MITHAL. Certainly. I think it was widely reported that certain people were posing as others in order to get information from ChoicePoint. ChoicePoint was covered by the Fair Credit Reporting Act in that case, which requires an entity to maintain reasonable procedures before providing sensitive consumer report information to others. We alleged that ChoicePoint did not maintain such reasonable procedures and, because we were proceeding under the FCRA, we were able to get civil penalties.

So we can get civil penalties if we sue a company under FCRA, but we can't get civil penalties for our other data security cases, such as in the Rite-Aid case.

Senator PRYOR. You said in your opening statement that you support the goals of this legislation. Are there areas in the bill that you think we need to work on?

Ms. MITHAL. Let me just mention one, Mr. Chairman. I think with respect to the scope of the bill—and I think the Rite-Aid case is a good example of this—the breach notification provisions would only cover a breach of electronic information. So for example, if a consumer’s paper information were breached there would be no breach notification required under the bill.

We would like to see the breach notification provisions extended to paper as well as electronic records. As I mentioned, in the Rite-Aid case they had just disposed of information into open dumpsters, and we think that consumers have a right to be informed in that case.

Senator PRYOR. You said that you like the provisions in the bill that allow the State attorneys general to I guess bring actions. Tell the Subcommittee why you like that and why you think that’s important.

Ms. MITHAL. Well, I think it’s a model that has certainly worked well in other areas of FTC enforcement. Under the Fair Credit Reporting Act, we have concurrent enforcement authority with the States. I believe that model has worked well. I mentioned in my opening statement our case against LifeLock. This was a case we brought together with 36 State attorneys general, and we were able to get a broad set of relief and we were able to get media publicity in both local markets as well as nationally arising from that action.

Senator PRYOR. Ms. Rusu, let me ask you about the State attorneys general. I think in your statement you said that you like the provision about the State attorneys general.

Ms. RUSU. Correct.

Senator PRYOR. Could you elaborate on that?

Ms. RUSU. Sure. As far as we’ve seen, the State attorneys general really have been at the forefront of the battle against data breaches and identity theft. I think it may have to do with the fact that they’re a lot more plugged into what is going on at the ground level. They’re more likely to hear about these issues, and a lot of times perhaps more able to meet with the people and see what’s happening right down at the ground level.

So from past experience, from what we’ve seen, the State attorneys general have really been the ones that have brought these issues to public and national consciousness. We like this model and we’d like it to continue.

Senator PRYOR. Ms. Bianchi, did you say in your statement whether you like the State attorneys general provision or not? I don’t recall you mentioning that.

Ms. BIANCHI. The HIPAA rules do include, as a result of the HITECH Act, enforcement power for State attorneys general. So that’s a new provision in the last year or so, and I understand the Department of Health and Human Services is currently working with the attorneys general to train them on HIPAA and on how to identify and proceed with cases, and they’re required to coordinate with the Department in doing so.

Senator PRYOR. Mr. Pratt, did you have any comment on the State AG provision?

Mr. PRATT. Thank you, Mr. Chairman. I think the only point we would make is we would like to continue some discussion around the question of not simply the attorneys general's powers, but the ability to name an official or agency of the State, so it expands it. It seems to expand it beyond the borders of just the attorney general him or herself, and I think that's probably where we'd like to see a little more discussion. I think we'd like to see that more limited. That can otherwise invite maybe second-tier or third-tier litigation that would probably confuse rather than help with a true enforcement action.

Senator PRYOR. Senator Wicker.

Senator WICKER. Do any of you want to talk about the possibility of too much notification? The bill requires notification of a covered breach to be provided unless there's no reasonable risk of identity theft, fraud, or other unlawful conduct. Some have expressed the concern that this will result in notifications when there's little or no evidence that unlawful conduct is likely to occur, but it's not technically unreasonable to think it could.

Is there such a thing as too much notification? Do any of you believe this is a legitimate concern? Raise your hands.

[A show of hands.]

Senator WICKER. Ms. Rusu, would you like to go first?

Ms. RUSU. First of all, the first point I'd like to make is that we really do believe that consumers should be the ones to decide what is important and what is not. The reason that we are concerned about this is that if a company is the one that gets to decide in every situation whether or not something is relevant, whether it's not, then a lot of times we're worried that they'll decide in their own best interests. Of course, notification entails some costs, it entails negative public image in the media.

So first of all, we think that consumers should be able to decide whether this is something they want to act on, whether this is something that they want to do in order to protect themselves.

Second, however, we believe that these notifications should really decrease as a result of this law. The real purpose behind this seems to me to be providing incentives for companies to put in place much better, much more responsible data security practices, and if these data security practices are implemented correctly we should see a much decreased number of security breaches in general, and as a result we will require a lot less notifications.

Senator WICKER. Ms. Mithal?

Ms. MITHAL. I would certainly agree that overnotification could be a concern. So for example, we wouldn't want consumers to receive so many notifications that they become numb to them. I don't think this bill is there. I think that certainly if there is a breach and every time there is a breach a consumer received a notification, it would be a problem. But I think this bill sets a high enough threshold that overnotification would not be a problem.

Senator WICKER. Mr. Pratt?

Mr. PRATT. I'm not sure there's a perfect science around what words you choose for the trigger to send a notice. So I would agree—

Senator WICKER. I was afraid of that.

Mr. PRATT. If I hire three lawyers, I get at least four answers, I can assure you, and I'm billed for all of them.

We have seen other standards in other bills, for example "significant risk of identity theft." I think it's a worthwhile question because it is important to ensure that we don't end up with over-notification. It means that the consumers begin to simply file those notices in the same way that they sometimes file GLB privacy notices, because they're not really readable.

So yes, I think it's a good question. I'm not sure I have a crystal ball to tell you perfectly what that answer is. I can tell you that "any other unlawful conduct," for example, could mean a lot of different things, and so that alone expands this trigger somewhat beyond the borders of other statutes that we've seen in other States. We'd be happy after the hearing to see if we couldn't bring together some better experience from any of our members in terms of how different State statutes have affected the trigger of the notice.

Senator WICKER. I think we would appreciate that.

Anyone else want to comment on that question? Yes, sir, Mr. Bregman?

Mr. BREGMAN. I think it's important that the bill includes provisions for the exclusion of data that has been rendered unusable through encryption and careful key management from notification. Without that, there could be significant overnotification where there really is no risk. The technologies will proceed to evolve and so it's important that we use best state-of-the-art technologies and that could be best determined probably by regulatory agencies and the industry as technologies advance.

Senator WICKER. Mr. Pratt, you want to add?

Mr. PRATT. Senator, if I could just echo support for that. That is a terribly important component of the bill. We compliment you, Senator Pryor, for having included that in the bill.

I'm not sure we feel that the best motivation for data security is the low threshold of the trigger for a notice. It is a clear roadmap for us to find a means of compliance, and knowing that we have an ability to render data in a wide variety of ways, not just simply using an encryption technology, but using a wide variety of tools, is probably the best motivator for us to find a way to simply not ever have to send a notice because we are never breaching the kind of data that would put a consumer at risk or a customer at risk in the first place.

Senator WICKER. What about the risk of false notices? Could the plethora of notifications make it easier for ne'er-do-wells to submit false notices and then ask for information from consumers? Does anybody worry about that?

Mr. PRATT. I can just tell you, in certain experiences in certain States over the many decades I've worked in the industry, we've seen false notices as a means of obtaining sensitive personal information for purposes of perpetrating ID theft. I think the TechAmerica testimony tells you that, of course, there are the low-tech approaches, but there are also the very, very high-tech approaches that pose different risks, that are probably found on my laptop rather than in my mailbox. But both forms of risk exist, and they exist today because there are many State breach laws today in many States.

Senator WICKER. Well, the Chair's been very generous with his time. Let me ask Mr. Pratt one other question. You believe the bill's information broker provisions would actually harm the industry's ability to use data for fraud prevention. Could you elaborate on this? What services do you provide consumers that might be negatively impacted by the inclusion of the brokers in this legislation?

Mr. PRATT. Thank you, Senator. Fraud prevention and location services are two types of tools that our members make available in the marketplace, and I think our testimony, the full testimony, tries to explain in a little more—with a little more granularity what the problem is. The monolithic application of accuracy standards or a standard for access and correction would be wrong, and of course, Senator Pryor, your bill doesn't attempt monolithic application. You do have some exceptions. We feel that they're probably too rigid. It's hard for us to be sufficiently omniscient to know what the next product is and whether the current exception embraces our ability to innovate and build that next product.

We would rather see—ultimately the question is who is the information broker that we're trying to get to? Consumer reporting agencies are regulated under the FCRA. Financial institutions would be governed under GLB. A fraud prevention tool—by the way, we wouldn't want to be compelled to disclose a fraud prevention tool's data because you're disclosing the recipe by which we prevent fraud. Senator Pryor, I know full well that that's not what you want either, so we understand. Your staff has been wonderful about allowing us to have a chance to talk about that.

With a locator tool, it's really fairly irrelevant. Neither fraud tools nor location tools are used to make a decision about me. They are tools that are used to investigate. They are tools used to prevent crime. We see at least in those two cases where an information broker provision and the way it's structured would potentially impinge on the operation of those tools, on future innovation, and actually we still think overlap potentially with current laws that are in place today.

Senator WICKER. Thank you.

Senator PRYOR. Senator Klobuchar, are you ready?

**STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA**

Senator KLOBUCHAR. I certainly am.

Senator PRYOR. All right. You're up.

Senator KLOBUCHAR. Thank you very much.

Thank you, everyone. I'm sorry, I was over at a Judiciary Committee hearing, actually on this same, somewhat in the same subject, on fraud enforcement and some of the difficulties with prosecuting complicated cases. And certainly data security is a growing problem, with no easy solution.

I personally have heard from a number of Minnesota businesses. Actually, Senator Thune and I have a bill on peer-to-peer file sharing software and the issues with that, and I came across a number of victims in our State. I was actually quite surprised at the stories, including one involving a home garden center, where this woman actually just went home to work at home on her shared

payroll documents. She didn't know her kids had installed one of these programs, and the next thing she knew her employees, a number of them were victims of identity theft because all of their personnel data was on the computer, the kids' program took it.

I think there are an estimated 10 million Americans per year whose identities are stolen. So I am excited about the work we're doing here. I think it's very important.

My first question would be of you, Ms. Mithal, and that is about these companies that are smaller. I think it's even harder for them to deal with it. While they may not be the major targets, but roughly a third of all data breaches happen at companies of less than 100 people. These companies, as I said, don't have that technical know-how. Will this legislation allow the FTC to tailor their regulations so they don't apply the same requirements to a company of 10 versus a company of 10,000? And should the size of the company matter?

Ms. MITHAL. Thank you, Senator. I agree with your comment. I think the size of the company should matter, and I think the bill imposes a reasonable security requirement on companies. The reasonableness in that requirement would include such things as the sensitivity of the data at issue, the cost of fixing a problem, and the cost—and the size of the business. So I think costs are definitely included in the calculus in the bill.

Senator KLOBUCHAR. OK.

Ms. Rusu, most consumers don't have the ability to evaluate a company's claim to good data security, because I know I've seen things that say that and you don't know, should I get on this website or not. How will establishing minimum data security requirements level the playing field for consumers and companies?

Ms. RUSU. I think first of all what we need to work on is, like you mentioned, providing notices that are readable to the average consumer. I think today the disclosures that are provided by companies are perhaps readable to someone who's graduated law school. So simplifying those notices is crucial, it is extremely important.

I think it's also important for notifications of breach to provide language that is very, very, simple, and clear. I think that a lot of times there's a tendency to provide too much information and this is where we get to the overnotification problem. When there's a long list of paragraphs that the consumer can barely get through, that's going to hinder their ability to take action. So simplifying language and helping consumers, regular day to day consumers, understand what these policies are will be a first big step.

Senator KLOBUCHAR. Very good.

Mr. Pratt, I think using a national standard here when so many of these issues, problems, easily cross State borders, makes sense to me. Do your members often have to comply with numerous State regulations and would establishing a national standard help?

Mr. PRATT. The easy answer is yes. A national standard does two things. Larger companies, of course, go out and hire a major law firm and ask those lawyers in that firm to set up a grid so they understand all the different State laws, and then they design their notification strategy around I guess the highest threshold that each

State statute might require for those States where consumers are the subject of the breach.

Yes, a single national standard would make that easier. Most importantly, though, when I get calls from my smaller corporate members they have a much harder time complying with those breach notification requirements because, of course, they have to ask me, what law firm should I hire in order to get a chart, in order to understand how to do it? So that's really important.

I would like to step back and also say that the scalability, so, Mr. Chairman, the scalability of the standards for security I think is an excellent component of the proposal, because it is important to acknowledge a smaller business with a lower threshold of risk should design a strategy that's appropriate for the risk. The FTC has done a good job of producing small business guidance in that regard as well. It's been beneficial for our members.

Senator KLOBUCHAR. Very good.

Ms. Bianchi, I know he turned to you about a large law firm. I used to work at one, so don't worry about it.

Just from the Hospital Association, Minnesota, as you know, is a mecca of health care, and Mayo has done some amazing things with sharing data, actually, within the Mayo system as a way of establishing costs and other things, that is actually one of the hallmarks of how they've been able to keep costs down and quality up. It's actually a model we want to use nationally. We had some issues with legislation and fights at midnight at one point, not health care, believe it or not, before that, about sharing information.

Do you want to talk a little bit about this—this will be my last question—from a hospital perspective and if you think this would be helpful, to have a national standard?

Ms. BIANCHI. Hospitals certainly really already have at least a national standard in place with respect to HIPAA. HIPAA establishes a floor. There are more restrictive State laws, but I think we certainly support a Federal standard. I think our concern really is that we're already subject to one.

Senator KLOBUCHAR. Right. You're concerned about another one.

Ms. BIANCHI. Right. So it's a concern about a second set of standards that would really in many ways duplicate the standards that hospitals have been operating under for several years, and hospitals certainly take these issues very seriously. We're just concerned about their compliance costs associated with parallel regulations.

Senator KLOBUCHAR. The other thing, just to get back to my point that I was making, was there are always issues where we want to be able to share data, not only for patients, so that one doctor in an emergency room will be able to access that data. I found that to be a huge issue and a problem. Then the second, again, would be what I was talking about, was sharing underlying medical information so you can figure out, how are we ever going to know how cost-effective a certain surgery is or a certain treatment is if we're not able to compile that data and figure that out as we look at how we reduce costs in health care.

Do you want to comment about that?

Ms. BIANCHI. Sure. I think that's obviously a critical issue coming out of health reform and out of ARRA and HITECH. The Department of Health and Human Services, as the result of Congress's action in those laws, is enormously invested in developing a national network of health information. Health information does have some special issues associated with it. One of the things that components of HHS have spent a lot of time on is worrying about the privacy and security of information in the context of developing this national network.

So I think it's important for those two sides of HHS to be able to work together to make health information available to improve quality and bring down costs, but at the same time not jeopardize the privacy and security of individual information. That is a challenge and HHS really has the expertise to do this in the health care context.

Senator KLOBUCHAR. Very good.

Anyone else want to enter into the fray?

[No response.]

Senator KLOBUCHAR. Thank you very much.

Senator PRYOR. All right, thank you.

Let me, Ms. Bianchi, sort of pick up with you in a little bit of a follow-up on a previous answer that you gave. You talked about HIPAA and HITECH and other laws. Is it your position that the existing Federal laws, whatever they may be, really cover every instance of data breach or data security for the hospitals?

Ms. BIANCHI. For HIPAA-covered entities, HIPAA provides a very comprehensive set of security requirements, privacy requirements. They're very detailed. They are scalable, so that a rural single provider office, single doctor's office, doesn't have to do the same things that a large hospital network would need to do.

But it is a very comprehensive system. It really is, I think, the best standard that we have now for data security and, particularly as the result of HITECH, a model for—many of the components of this bill really track the HIPAA standard. So yes, I do think it provides a very comprehensive system framework.

Senator PRYOR. Mr. Pratt, let me ask you. We've talked a little about having a national standard for information security, etcetera. In your opening statement you talked a little bit about this idea of double jeopardy, how your folks might be subject to two different laws or more and have to maybe send out multiple notices.

Could you talk a little bit more with the Subcommittee about that? You talked about the term "in compliance with" and you also talked about this idea of "where subject to." Could you tell us a little bit more about that?

Mr. PRATT. Thank you, Mr. Chairman. In several places it's encouraging, the structure and the approach that you've taken, and it appears that the goal would be in fact to achieve some alignment between the requirements of this statute, to fill in the gap where there is no statute in place. So if there's no HIPAA in place, this kind of fills in the gap.

In our view, if there's no FCRA in place this statute would fill in the gap, or similarly under the Gramm-Leach-Bliley Act, two statutes that we tend to live and work with every day. If the test, however, of determining whether or not I'm exempt is that I'm in

compliance with another statute—and of course, every company works to be in compliance, but every company may find from time to time that they are not. You can simply go to the FTC website and you'll see an investigation of some company for not having been in compliance.

That's the whole purpose of that law. Where you're not in compliance, there are penalties and consequences for that statute. So our only point would be to replace the phrasing "in compliance with" with the phrasing "subject to." In other words, I am subject to a standard of law that is similar to the one that you have outlined here, as opposed to I'm in compliance with.

Of course I'm going to be in compliance with it. If I'm a consumer reporting agency under FCRA, I'd better be complying, and that is true under the Gramm-Leach-Bliley Act. And by the way, that would be true to the extent that our member would run a business that would now have to comply with the requirements of this statute as well.

And we're happy to comply with all three of those statutes and to protect data relative to the sensitive personal information in all three cases. We just want to know that we don't end up with the tripwire being because you fell out of compliance you now are supposed to be in compliance over here as well. And there might be some differences in compliance requirements, so now it's almost an *ex post facto* application of duties that I was not first subject to, but I'm only subject to because I failed in some way relative to the duty that I had over here with this statute that is the primary statute that governs me, FCRA, GLB.

So we just simply are urging the Committee to adjust the approach to the exception so that they make it clear that if you're subject to the Fair Credit Reporting Act we would simply make the argument FCRA would require similar standards, therefore we are in compliance with and exempt from. And if we are subject to the Gramm-Leach-Bliley Act and the safeguards rule in the Gramm-Leach-Bliley Act, we have a substantially similar set of requirements and therefore we're exempt from this, but we're of course not exempt from GLB.

In no case are we asking to be somehow exempt from something that would allow us to therefore be sloppy with sensitive personal information.

Senator PRYOR. I understand the distinction you're trying to make.

Ms. Bianchi, let me ask you. On HIPAA, as I understand HIPAA—and I know HIPAA's fairly comprehensive—I don't think it covers employee data, does it?

Ms. BIANCHI. It covers—it can in some cases, but mostly no, it does not, it does not cover employee data.

Senator PRYOR. Do you think the hospital should be subject to this law we're proposing for employee data purposes?

Ms. BIANCHI. I think to the extent that hospitals have information that is not part of their covered entity and is not subject to the requirements of HIPAA, that certainly hospitals support robust security standards. I think the importance would be for the exemption to be with respect to all protected health information, and

where that does include employee information that that also would be covered under that.

It's really a concern about not being subject to two different sets of rules for the same set of information.

Senator PRYOR. Right. I appreciate that.

Mr. Bregman, I'm not going to let you off the hook. Maybe you thought I wasn't going to ask you any questions and you were going to slip the noose. But I have a few for you.

Senator KLOBUCHAR. "Slip the noose"?

Senator PRYOR. Let me ask about your view of whether we should extend a law like this to nonprofits. I don't know if you mentioned that in your opening statement, but to schools and nonprofits, et cetera; is that in your view good policy?

Mr. BREGMAN. I think it is good policy. If you look at the data, a large amount of data breach occurs from the nonprofit sector, where they do have sensitive data. And I don't think this legislation would impose an undue burden on them.

Senator PRYOR. I think in your statement you talked about personally identifiable information and the definition of that. Would this definition effectively capture the trigger for breach notification to the affected consumers where appropriate?

Mr. BREGMAN. I think the intent is that personally identifiable information would be subject to this to the extent that it's not rendered unusable through technical means, such as encryption or other alternative accepted technologies.

Senator PRYOR. Do you like the way we've tried to set the trigger in our legislation, or could you improve on that? Or do you know enough about the bill to comment on that?

Mr. BREGMAN. Well, to the extent I understand the bill, I think it's reasonably set at this point.

Senator PRYOR. Ms. Rusu, in your statement you talked about "unusable" and "unreadable" data. You mentioned that data can sometimes be reconstructed in some way. I think I know what you mean by that, but tell me what you mean by that and what a viable solution there might be?

Ms. RUSU. A lot of times data can initially appear encrypted, it can initially appear unusable or unreadable, but subsequently by using certain technologies that data could be reconstructed and actually re-attributed to the person to whom it belongs and then used for identity theft.

So really our recommendation is that, together with the FTC, we work toward identifying those types of methods of encryption that really do render the data unusable and unreadable to the extent that it cannot be reconstructed.

Senator PRYOR. I asked Mr. Bregman a few minutes ago about extending the law to nonprofits and I assume that—I understand that Consumers Union is for that. But does Consumers Union think that there should be any exceptions to that? Is there anybody you think ought to be exempted or excepted?

Ms. RUSU. Exempted from the nonprofit requirement?

Senator PRYOR. Right.

Ms. RUSU. I would be happy to get back to you in writing on that, if possible.

[The information referred to follows:]

Consumers Union believes that it is important to require both non-profit and private sector entities to protect the security of the personal consumer data they maintain and to provide breach notice. Consumers face the same risks, whether their data is compromised by for-profit or non-profit entities. While we are certainly cognizant of the fact that many non-profits may not have the resources to provide notification or credit monitoring, we believe that the bill's provisions exempting such action due to excessive cost are sufficient.

Senator PRYOR. Did you have any questions?

Senator KLOBUCHAR. Just one more follow-up with Mr. Bregman. I know that the Verizon business risk team, working with the United States Secret Service, recently released their 2010 report on security breaches, and I think one of the most surprising findings of the report was that 96 percent of breaches were avoidable through simple or intermediate data security controls. Is this consistent with your experience and would provisions in the Data Security and Breach Notification Act that require companies to implement basic data security practices address many of these problems?

Mr. BREGMAN. Absolutely. The vast majority of data breaches are avoidable through good practices, good data hygiene, and good IT practices. I think this legislation would put organizations on notice that, in the absence of that, they're going to have to make breach notification and they may be subject to other sanctions.

I think the important point is that as we look at the methodologies to avoid data loss and data breach, those methods and techniques will change over time. So it's important not to try to define specific technologies in the legislation, but rather to assure that Federal regulators, in consultation with industry, will regularly update the best practices and make those the metrics for whether a company is in compliance.

Senator KLOBUCHAR. Ms. Rusu?

Ms. RUSU. I'd also like to add that I think the strong point of this bill is not only to get companies to employ those best practices, but also to expand their practices toward data minimization and data retention limits. I think a lot of times maybe companies will realize that, if we're amassing this huge amount of data and we're keeping it in perpetuity, we may be subject to a lot more requirements. There is a much higher risk of losing it through data breach. So perhaps part of those best practices will be setting data retention limits or minimizing the amount of data the companies collect.

Senator KLOBUCHAR. The Cyber Protection Informed Users Act I mentioned that I have introduced with Senator Thune, focuses on some of the file sharing software and allows for users to be clearly notified that it's on their computer, so that they have a chance to opt out. Do you see this file sharing as a growing data security problem, Mr. Bregman, if you want to answer?

Mr. BREGMAN. I think it is. I think it's really an example of a broader issue of particularly consumers taking advantage of technologies without having a deep understanding. You mentioned in an earlier question that, how do we help consumers understand whether the techniques being used by companies are adequate, and I think that's an example where we would hope that consumers could look to Federal regulators to evaluate and essentially apply that stamp of approval that this set of technologies has been tested and meets those needs. And those technologies will change rapidly in the marketplace.

Senator KLOBUCHAR. I just think people would be surprised that their kid can put something on their computer that—I speak as a mother of a 15-year-old—that their kid can just put something on the computer that will allow all the stuff they put on there to be shared with a bunch of people. I think it’s pretty shocking and that we have to get that information out there to them.

All right, thank you very much.

Thank you, Chairman.

Senator PRYOR. Thank you, Senator Klobuchar. It’s always good to have you here.

Let me ask really just a couple of last questions. First, for Mr. Pratt. Do you think that consumers should have the ability to have access to their information, to go in and clean it up? And I guess, how would that work?

Mr. PRATT. OK, fair enough. Let’s start with what we definitely know, and that is, where data is used to make a decision about me I should always have access. I should have access before the data is used, any time I wish to see it. Of course, that occurs here in the U.S. primarily because the data is being used in the context of the Fair Credit Reporting Act. So any type of decision for eligibility is likely an FCRA transaction of some sort. So I have the right of access today.

If you’re talking about a fraud prevention tool, as I discussed earlier, I think that would be different. Yes, some of my information might be in a database that includes confirmed fraudulent applications that have been pooled together by a variety of large insurance and financial institutions who are trying to stop future fraud. That kind of information doesn’t really—we don’t want to clean up that information. We actually want to know about the combinations of data that were used to attempt to prevent the fraud. We don’t want to disclose that we have all of that data and that we have certain pattern analyses that we then deploy at the point of the next application.

So the answer to that would be no. But remember, the fraud prevention tool doesn’t stop the transaction. The fraud prevention tool just raises a yellow flag and says to the end user: You should take additional steps to verify the consumer. That’s what we want. We want the additional steps to be taken so the identity theft is stopped at the point of sale.

A location service is yet again different. That’s about possibilities. I am a law enforcement agency in a small town in the U.S., but I’m trying to investigate a crime and I’m looking at—I’m trying to locate possible witnesses, or I am trying to locate somebody who has skipped on a parole, and I use the tool to locate relatives, locate friends, see previous addresses at which the individual lived, and these are part of my investigative tools.

But we wouldn’t want somebody to be able to sever, quote unquote, “clean that up,” so that the noncustodial parent who’s not paying child support can figure out a way to uncouple themselves from their responsibility.

So a locator service is again, not a tool that stops a transaction or affects how I, as the real person, get to do business. But they are used in different ways.

So, I guess those are just good examples of how the fair information practice of access is appropriate to some types of data uses and it's inappropriate to others. I think that's pretty consistent globally, that fair information practices are not applied monolithically to the nature of the data, but to some extent to the use of the data.

Senator PRYOR. Ms. Mithal, did you have any comments on behalf of the FTC about consumers cleaning up their data?

Ms. MITHAL. Yes. I would absolutely agree with Mr. Pratt that consumers should have access to data when it's used to deny them benefits or used for eligibility purposes. We do note that we had these three public roundtables and one of the things we learned is that consumers may be denied benefits that don't fall within the Fair Credit Reporting Act. So I think there are certain holes in the Swiss cheese that we want to fill with, potentially with an access provision similar to what you have in the legislation.

So for example, I'm Maneesha Mithal. I don't have a criminal record, but if somebody denies me a benefit based on the fact that their database shows that I had a criminal record, I might want access to that and the ability to correct it. Even if it's not used for credit or employment purposes, I might just not want that to be out there. So that's why we think the access and correction provisions you have in the legislation could alleviate that concern.

Senator PRYOR. Yes, sir, Mr. Pratt?

Mr. PRATT. So I guess just to add to that. The reason that we're asking for this provision to be struck is not because we want to just stick our head in the sand and ignore the kind of question that Ms. Mithal has just raised, but that it's an idea that deserves a good deal more scrutiny. What we try to put forward in our testimony is that we just don't know who is that type of entity that we're trying to target. And the way the definition is structured and the way the language of the section is structured, I don't think we're close yet to knowing how to apply that, who is that entity and what kind of entity are we trying to track down, on-line, off-line, and so on.

It's a worthwhile dialogue. We're not afraid to have that dialogue. We're happy to have that dialogue. We just think that it's one that—this is a less matured, less fully understood provision than data security and security breach notice, where we have a very clear understanding and a plethora of hearings and an understanding of what it is and why it's important to get that part of the job done.

Senator PRYOR. Listen, I want to thank all of you for being here today and all your preparation and your time involved in getting here and testifying today. We really appreciate it.

What we're going to do is we're going to leave the record open for a week. We actually, may actually try to mark up this bill next week, so we're going to encourage our Senators to get any follow-up questions that they may have to you ASAP and encourage you to get those back ASAP if at all possible. So we continue to work on this and, as Senator Wicker said a few moments ago, he wants to continue to work on this with us. We hope this is very much a bipartisan group effort as we go through the process.

So I want to thank you all for being here and thank you for coming before the Subcommittee today. With that, we will adjourn.

[Whereupon, at 3:48 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. JOHN D. ROCKEFELLER IV

Thank you, Senator Pryor, for holding this hearing, and I want to commend you for your continued, excellent stewardship of the Consumer Protection Subcommittee.

In today's economy, a vast array of businesses and organizations maintain information about consumers. When a person buys a book online, the company asks for the name, address and credit card information from the individual. When a student pays his or her tuition, a college may collect that student's debit card information. Employers gather information about their employees, including background data, and their bank account number for direct deposit. All these entities store consumers' personal information in databases—some of which are well protected and some of which are not. Every day, consumers run the risk that the entities holding their information will suffer a data breach, and their information will be compromised by no fault of their own.

Data breaches plague businesses and organizations, putting millions of consumers at risk. According to the Privacy Rights Clearinghouse, over half a billion data records have been compromised by unauthorized access to consumer databases since 2005. In 2009 alone, there were 498 data breaches involving 222 million sensitive records.

The consequences of these breaches are grave: identity theft, depleted savings accounts, a ruined credit score, and trouble getting loans for cars, homes and kids are just some of the effects.

To minimize data breaches, deter identity theft and protect consumers, Senator Pryor and I introduced *S. 3742, the Data Security and Breach Notification Act of 2010*. The legislation establishes needed protections for consumers, while at the same time providing regulatory certainty to businesses.

In *S. 3742*, Senator Pryor and I address the dangers of data breaches and identity theft by imposing two key mandates on businesses and nonprofit organizations that maintain large consumer databases. First, the bill requires these businesses and organizations to adopt security protocols to reasonably protect their databases from unauthorized access. Second, the bill requires breached entities to notify all affected consumers of data breaches in a timely manner—unless there is no reasonable risk of identity theft or harm to consumers.

The bill also imposes new requirements on information brokers—the companies that amass, organize, and sell vast amounts of American consumers' information to third party buyers for a profit. Specifically, the *Data Security and Breach Notification Act of 2010* gives consumers the right to know what data information brokers are collecting on them; and the right to correct any inaccuracies they may find.

It is important to note that our bill represents a carefully crafted compromise between consumer groups and the business community. On the one hand, consumers get strong protections and aggressive enforcement by states' attorneys general. On the other hand, the bill creates national standards that facilitate interstate commerce; and the Federal Trade Commission is provided with regulatory flexibility to accommodate technical complexities and small business concerns.

The Commerce Committee has twice reported data security legislation out of Committee. Both times the Senate has failed to take it up on the floor. I fully intend to report this bill out of the Commerce Committee in next week's markup, and it is my sincere hope that this time—the third time—is the charm. The House has passed data security legislation on voice vote. I hope we can achieve a similar result in the Senate.

PREPARED STATEMENT OF THE CONFIDENTIALITY COALITION

The Confidentiality Coalition thanks the Senate Commerce, Science and Technology Committee for the opportunity to submit a statement for the record on the "Data Security and Breach Notification Act of 2010" (S. 3742). The Confidentiality

Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health produce distributors, pharmacy benefit managers, pharmacies, health information and research organizations, patient groups, and others¹ founded to advance effective patient confidentiality protections.

The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new life-saving and life-enhancing medical interventions. The Confidentiality Coalition is committed to ensuring that consumers and thought leaders are aware of the privacy protections that are currently in place. And, as healthcare providers make the transition to a nationwide, interoperable system of electronic health information, the Confidentiality Coalition members believe it is essential to replace the current mosaic of sometimes conflicting state privacy laws, rules, and guidelines with a strong, comprehensive national confidentiality standard.

As such, the Confidentiality Coalition believes that the privacy of patients' health information is of the utmost importance. Nothing is more important to engendering trust in the healthcare system than a comprehensive set of privacy protections for personal health information. That said, we have concerns that S. 3742 would result in health information being governed needlessly by two entities—the Federal Trade Commission (FTC) under the current Senate bill and the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA).

The Data Security and Breach Notification Act of 2010 would require the Federal Trade Commission (FTC) to establish regulations requiring a broad range of entities, including healthcare organizations, to implement security practices to protect personal information and to provide for notification in the event of any security breaches of that information. The protections proposed by S. 3742 unnecessarily duplicate the protections already in place under HIPAA, and would likely have disruptive effects on the normal business activities of healthcare organizations by altering current and accepted practices across the industry. In other words, the legislation would create a parallel and inconsistent enforcement mechanism for the healthcare industry, which is already subject to comprehensive and effective privacy and security regulation at both the Federal and state levels.

Accordingly, we encourage a clear statement in this legislation that exempts healthcare companies that are HIPAA "covered entities"² and their "business associates"³ from the reach of this new legislation. This clarification would preserve the careful lines drawn by the HIPAA privacy and security rules and would permit the healthcare industry to continue to provide services to members and patients without the need to dramatically alter its current (and already heavily regulated) arrangements. We view this exemption as appropriate to avoid substantial disruption of the important work conducted by healthcare organizations on behalf of patients and consumers.

Discussion

The Confidentiality Coalition applauds Congress' effort to require entities holding sensitive consumer information to develop a comprehensive data compliance protection plan and adhere to strict breach reporting requirements. While we understand and support these goals in connection with currently unregulated arenas, these goals—and the consumer risks they are designed to address—have already been addressed for the healthcare industry. The healthcare industry is heavily regulated in

¹ A list of the Confidentiality Coalition members is attached to this letter.

² 45 CFR 160.103 Covered entity means: (1) A health plan; (2) A health care clearinghouse; (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

³ 45 CFR 160.103 Business associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity.

its privacy and security obligations. These obligations have been in place since 2003 under HIPAA, and recently have been revised and expanded through the Health Information Technology for Economic and Clinical Health (HITECH) Act of the American Recovery and Reinvestment Act (P.L. 111-5).

The HIPAA privacy and security rules apply to “protected health information”—health information that is held by a HIPAA covered entity. It is information that either directly identifies an individual or for which there is a reasonable basis to believe that an individual could be identified. Protected health information includes demographic information, such as a person’s name and address. It includes payment information—such as credit card information or checking account information—that a patient uses to pay for care. Generally, all identifiable information about a patient that is held by a HIPAA covered entity is protected health information and, therefore, governed by HIPAA.

The HIPAA regulations include a number of components—most importantly, baseline privacy regulations as well as security regulations that apply specifically to electronic information. These HIPAA/HITECH provisions impose specific requirements on covered entities to provide notice to patients and members of all uses and disclosures of personal information obtained in the course of providing services to these individuals. In addition to the detailed privacy notice, the HIPAA/HITECH rules impose specific consent obligations, with certain areas where consent is assumed (primarily, the core healthcare purposes of treatment, payment, and healthcare operations), certain areas where use and disclosure is permitted without the need for consent (such as certain public health disclosures or disclosures in connection with litigation), and other areas—essentially, all other disclosures—where a specific, detailed individual “authorization” is required.

“Marketing” in connection with the healthcare industry also is heavily regulated and limited—both through the original HIPAA rules and through new, stricter, provisions in the HITECH Act. These rules address the specific operations of healthcare companies and under these rules, most marketing activities require a specific patient authorization. The only marketing activities that are permitted without authorization are those that the Department of Health and Human Services (HHS) has deemed to be useful and appropriate for consumers in the healthcare industry. The HHS Office of Civil Rights has jurisdiction to enforce these provisions (including expanded new penalties created by the HITECH Act). In addition, the HITECH Act authorizes state Attorneys General to enforce the HIPAA rules.

As evidenced above, the HIPAA privacy and security rules provide a comprehensive privacy and security framework for HIPAA covered entities. Initially, “business associates” under HIPAA—those companies that provide services to HIPAA covered entities—were regulated through contracts with these covered entities. Now, as a result of the HITECH law, these business associates also are directly subject to privacy and security requirements, subject to primary enforcement by HHS, and face the same penalties as covered entities for non-compliance. Thus, all organizations handling protected health information are subject to the same stringent requirements and penalties for violations or breaches of this information.

Accordingly, while HIPAA does not apply to all entities that might collect, use, or disclose health-related information,⁴ HIPAA does create a comprehensive set of standards and an overall enforcement protocol for those entities—both covered entities and business associates—who are regulated directly under the HIPAA rules. Moreover, as a result of the HITECH law, both covered entities and business associates face significantly increased exposure for violations of these rules, as well as the ongoing possibility of criminal penalties.

Therefore, for these covered entities and business associates, regulation under HIPAA/HITECH is both comprehensive and substantial. HIPAA/HITECH incorporates a wide range of standards for the use and disclosure of health information, creating specific rules for all aspects of the operations of the covered entities and their business associates. Moreover, the HIPAA Security Rule imposes perhaps the most significant set of security-related requirements imposed by law under any standard.

In addition to detailed privacy and security regulations, the HITECH Act includes new rules for responding to security breaches. HIPAA covered entities and their business associates are required to notify each individual whose information is breached. For larger breaches—those involving the health information of 500 or more individuals—these organizations also must notify the media. The Secretary of

⁴The Coalition supports efforts by Congress and the Federal Trade Commission to evaluate appropriate privacy and security obligations for these unregulated healthcare entities or for uses and disclosures of sensitive healthcare information that are outside the scope of HIPAA.

HHS also must be notified of all breaches, large and small. HHS posts a list of breaches on its website.

The HIPAA breach regulations include specific requirements for how individuals must be notified. These reflect the requirements Congress established under the HITECH Act. For example, individuals must be notified of a breach without unreasonable delay, and no later than 60 days after the breach is discovered. The notice must be in writing; it must describe the type of information breached and the steps individuals should take to protect themselves from potential harm resulting from the breach. Thus, HIPAA covered entities already are obligated to carry out the kinds of security breach activities that S. 3742 requires.

With these standards in place, we have significant concerns about the risks and burdens of creating unnecessary additional obligations related to breach notices for healthcare entities. S. 3742 would create a new and inconsistent set of obligations on both notice and consent for the healthcare industry. We recognize that there is language addressing entities in “compliance with any other Federal law that requires such covered entity to maintain standards and safeguards for information security and protection of personal information in the legislation (in the section entitled “Treatment of Entities Governed by Other Law”), but the effect of this language as drafted is unclear. Therefore, to the extent that this legislation applies to healthcare entities and their business associates, we believe strongly that these provisions would require fundamental changes in the healthcare industry without any identified need or specific rationale.

The HIPAA rules—particularly with the additional obligations imposed by the HITECH Act—create a challenging set of standards for any affected healthcare entity. To apply different or additional standards to this information would create significant additional cost and unneeded complexity.

Also, there is no need for an additional regulator to oversee these obligations. The Department of Health and Human Services has primary authority under these rules, with a significant new set of enforcement tools in its arsenal. There is no need for FTC to enter this arena to provide additional (and potentially inconsistent) regulatory oversight. To the extent that Congress wants FTC to have any involvement at all in the regulation of health information, it should limit this involvement (if any) to those entities that are outside the HIPAA/HITECH structure. Congress should not permit the FTC to regulate those companies—whether a covered entity or a business associate—who already face regulation by HHS and the Attorneys General around the country.

Therefore, we encourage Congress to amend S. 3742 by crafting a clear and explicit exemption for personal information held by covered entities and their business associates that is already protected and regulated by HIPAA. Specifically, Congress should ensure that there is an explicit statement in the legislation that entities covered by HIPAA and their business associates are exempt to the extent that the information they hold is protected and regulated by HIPAA. This specific language should recognize that the privacy and security practices of the healthcare industry already are heavily regulated, with principles designed to facilitate the appropriate use and disclosure of healthcare information for appropriate purposes. Any change to these rules in legislation that is focused on the activities of the healthcare industry would be duplicative at best and disruptive and damaging for patients at worst.

We look forward to working with you as this bill moves through the legislative process and hope you can address the concerns we have raised. The Confidentiality Coalition appreciates the opportunity to continue our discussion with you on this legislation. If you have any questions or would like further information, please contact Tina Olson Grande, Sr. Vice President for Policy, at the Healthcare Leadership Council and Executive Director of the Confidentiality Coalition (tgrande@hlc.org).

2010 Steering Committee Membership

Aetna	Healthcare Leadership Council
American Hospital Association	IMS Health
America’s Health Insurance Plans	Marshfield Clinic
Association of Clinical Research Organizations	McKesson Corporation
Blue Cross Blue Shield Association	Medco
CVS Caremark	National Association of Chain Drug Stores
Federation of American Hospitals	Pharmaceutical Care Management Association
Greenway Medical Technologies	Pharmaceutical Research and Manufacturers of America
Gundersen Lutheran Health Dialog	

Premier, Inc.
Prime Therapeutics
Texas Health Resources

VHA
Walgreens
Wellpoint

General Membership

ACA International
Adheris
American Academy of Nurse
Practitioners
American Benefits Council
American Clinical Laboratory
Association
American Electronics Association
American Managed Behavioral
Healthcare Association
Amerinet
AstraZeneca
American Pharmacists Association
Ascension Health
Association of American Medical
Colleges
Baxter Healthcare
BlueCross BlueShield of Tennessee
Catalina Health Resource
CIGNA Corporation
Cleveland Clinic
College of American Pathologists
DMAA: The Care Continuum Alliance
Eli Lilly
ERISA Industry Committee
Food Marketing Institute
Fresenius Medical Care
Genentech, Inc.
Genetic Alliance
Genzyme Corporation
Health Care Service Corporation

Humana, Inc.
Intermountain Healthcare
Johnson & Johnson
Kaiser Permanente
Mayo Clinic
Medical Banking Project
Medtronic
Merck
MetLife
National Association of Health
Underwriters
National Association of Manufacturers
National Association of Psychiatric
Health Systems
National Community Pharmacists
Association
National Rural Health Association
Novartis
Pfizer
Quest Diagnostics
SAS
Siemens Corporation
Society for Human Resource
Management
State Farm
TeraDact Solutions Inc.
Trinity Health
U.S. Chamber of Commerce
Wal-Mart
Wolters Kluwer Health

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO MANEESHA MITHAL

Question 1. What is the risk that a data breach poses to consumers in today's economy?

Answer. Data breaches pose many risks to consumers, including the risk of stalking, identity theft, or other unlawful practices such as fraud.¹ For certain kinds of information, such as health information, data breaches may also cause reputational harm. For companies, data breaches can cause consumers to lose confidence in them.

Question 2. Are consumers concerned about identity theft these days?

Answer. Yes. Unfortunately, identity theft remains a major concern for consumers. The Commission estimates that as many as 9 million Americans have their identities stolen each year. Indeed, the Commission has received more consumer complaints about identity theft than any other category of complaints every year since 2002.

Identity theft has serious repercussions for victims. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for

¹There is limited data regarding the incidence of these harms. However, the FTC is aware that some identity theft is caused by data breaches. According to a survey conducted on behalf of the FTC in 2006, about 11 percent of identity theft victims reported that they knew their information was stolen from a company. See Federal Trade Commission, *2006 Identity Theft Survey Report* (Nov. 2007), available at <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.

education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

Question 3. What is the average cost per incident of a data breach in the United States?

Answer. According to an annual study conducted by the Ponemon Institute, the average cost of a data breach to companies was \$204 per compromised customer record in 2009. The study indicates that the average total cost to companies of a data breach incident rose from \$6.65 million in 2008 to \$6.75 million in 2009. These costs may include expenses for detection of the breach, engaging forensic experts, notification of consumers, free credit monitoring subscriptions, the economic impact of lost or diminished customer trust, and legal defense.²

Question 4. Do you believe that companies should be required to maintain appropriate safeguards protecting sensitive consumer data?

Answer. Yes. If companies do not maintain appropriate safeguards to protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace. Accordingly, the Commission has undertaken substantial efforts to promote data security in the private sector through law enforcement, education, and policy initiatives. For example, on the law enforcement front, the Commission has brought 29 enforcement actions since 2001 against businesses that fail to implement reasonable security measures to protect consumer data.

Question 5. What are the most necessary provisions of this legislation? Currently, how well are consumers protected against identity theft, fraud and other harm?

Answer. The Commission believes that several provisions of the legislation are important. First, the Commission supports the requirement that a broad array of entities implement reasonable security policies and procedures, including both commercial enterprises and nonprofits. Problems with data security and breaches affect businesses and nonprofit organizations alike. Thus, requiring that this broad array of entities have reasonable security policies and procedures is a goal that the Commission strongly supports.

Second, the Commission supports the breach notification provisions of the bill. Indeed, various states have already passed data breach notification laws which require entities to notify affected consumers in the event of a data breach. Notice to consumers may help them avoid or mitigate injury by allowing them to take appropriate protective actions, such as placing a fraud alert on their credit file or monitoring their accounts. In addition, breach notification laws have further increased public awareness of data security issues and related harms, as well as data security issues at specific companies.³ Breach notification at the Federal level would extend notification nationwide and accomplish similar goals.

²Ponemon Institute, *2009 Annual Study: Cost of a Data Breach* (Jan. 2010), available at http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf.

³See, e.g., Samuelson Law, Technology, & Public Policy Clinic, University of California-Berkeley School of Law, *Security Breach Notification Laws: Views from Chief Security Officers* (Dec. 2007), available at http://www.law.berkeley.edu/files/cso_study.pdf; Federal Trade Commission Report, *Security in Numbers: SSNs and ID Theft* (Dec. 2008), available at <http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf>.

Third, the Commission supports the legislation's robust enforcement provisions, which would: (1) give the FTC the authority to obtain civil penalties for violations⁴ and (2) give state attorneys general concurrent enforcement authority.⁵

With respect to current protections, the Commission enforces several laws and rules imposing data security requirements, including the Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB"), the Fair Credit Reporting Act, and the FTC Act. However, at present, in most of the cases the Commission brings, it cannot obtain civil penalties. I believe the provision allowing FTC to seek civil penalties for violations of S. 3742 would have a significant additional deterrent effect.

Question 6. Which provisions in my bill do you support most strongly?

Answer. As noted above, the Commission supports the legislation's effort to require a broad array of entities to implement reasonable security policies and procedures, the creation of a breach notification requirement at the Federal level, and the legislation's robust enforcement provisions. Of all the provisions, perhaps the most beneficial is the provision giving the FTC the authority to enforce civil penalties against entities that do not maintain reasonable security. Such penalties would provide a strong incentive for companies to maintain adequate data security.

Question 7. I understand that the Commission in the past has publicly supported and even recommended to Congress the enactment of Federal legislation enhancing data security across private industry. Do you also support applying data security requirements to other covered entities—such as nonprofits, as covered in my bill—that also maintain sensitive consumer data?

Answer. Yes. It is important that nonprofits that collect consumers' personal information are covered by the bill because problems with data security and breaches affect businesses and nonprofit organizations alike. Indeed, many of the breaches that have been reported in recent years have involved nonprofit universities, for example. From consumers' perspective, the harm from a breach is the same whether their information was disclosed by a nonprofit or a commercial entity. Requiring reasonable security policies and procedures of this broad array of entities is a goal that the Commission strongly supports.

Question 8. Have there been instances in which nonprofits leaked consumers' information making those consumers vulnerable to subsequent fraud or identity theft?

Answer. Yes. A number of sources publicly report data breaches that have occurred at nonprofits. For example, the Identity Theft Resource Center⁶ and Privacy Rights Clearinghouse⁷ both list incidents of recent data breaches that include numerous non-profit organizations.

⁴This recommendation is consistent with prior Commission recommendations. See Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Science, and Transportation, 109th Cong. (Jun. 16, 2005), available at <http://www.ftc.gov/os/2005/06/050616databreaches.pdf>; Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Trade, and Consumer Protection, 111th Cong. (May 5, 2009), available at <http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf>; Prepared Statement of the Federal Trade Commission Before the Subcomm. on Interstate Commerce, Trade, and Tourism of the S. Comm. on Commerce, Science, and Transportation Committee, 110th Cong. (Sep. 12, 2007), available at <http://www.ftc.gov/os/testimony/070912reauthorizationtestimony.pdf>; Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Science, and Transportation, 110th Cong. (Apr. 10, 2007), available at <http://www.ftc.gov/os/testimony/P040101FY2008BudgetandOngoingConsumerProtectionandCompetitionProgramsTestimonySenate04102007.pdf>. These recommendations also were made in an April 2007 report released by the President's Identity Theft Task Force, which was co-chaired by the Attorney General and the FTC Chairman, as well as in a report on Social Security numbers released in December 2008. See The President's Identity Theft Task Force Report, Sep. 2008, available at <http://idtheft.gov/reports/IDTRReport2008.pdf>; FTC Report, "Recommendations on Social Security Number Use in the Private Sector," (Dec. 2008), available at <http://www.ftc.gov/opa/2008/12/ssnreport.shtml>.

⁵This recommendation is consistent with prior Commission recommendations. See The President's Identity Theft Task Force, "Combating Identity Theft: A Strategic Plan," (Apr. 2007), available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

⁶See http://www.idtheftcenter.org/artman2/publish/lib_survey/IIRC_2008_Breach_List.shtml.

⁷See <http://www.privacyrights.org/data-breach#CP>.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO
IOANA RUSU

Question 1. What is the risk that a data breach poses to consumers in today's economy?

Answer. The most palpable risk posed by data breach to consumers is that of identity theft and fraud, either at the time of the breach or later, as the compromised information is sold and resold. When consumers' personal information is compromised in this way, a bad actor could appropriate that information and use it to obtain credit and government services, among other benefits.

Identity theft and fraud, however, are not the only harms posed by data breaches. Even though a consumer's personal information is not ultimately used to commit identity theft or fraud, the simple fact that his or her information is now freely floating in the marketplace and the consumer has no control over its use reduces consumer confidence in the marketplace. If consumers exchange their personal information for services provided by a certain company, and that company ultimately loses control of that information, consumers may be less willing to reveal personal information to vendors in future transactions. Consumers should be able to engage in the marketplace with confidence, knowing that their information is being safely and responsibly guarded by marketplace actors.

Question 2. What is the average cost per incident of a data breach in the United States?

Answer. According to the Ponemon Institute *Annual Cost of a Data Breach* study conducted in 2009, the average cost of a data breach in 2008 cost companies an average of \$202 per compromised record—of which \$152 pertains to indirect cost including abnormal turnover or churn of existing and future customers.¹ Despite an overall rise in total data breach cost over the past 4 years, Ponemon Institute indicates that direct costs appear to be declining slightly from a high of \$54 in 2006 to a low of \$50 in 2008.²

Consumers Union believes that a robust notice of breach requirement supports business investment in improved data protection, saving consumers the time, effort and cost incurred in dealing with a data breach, and saving companies the cost of future breaches.

Question 3. Are consumers concerned about identity theft these days?

Answer. Yes, we believe that consumers are extremely concerned about identity theft and fraud today.

In December 2009, Mintel Comperemedia reported that nearly half of adults polled (46 percent) were worried about someone stealing money from their bank accounts or stealing their identities.³

In addition, in February 2010, the Federal Trade Commission published the Consumer Sentinel Network Data Book for 2009.⁴ In this report, the FTC aggregated and compiled all consumer complaints received during 2009 through a number of avenues, including FTC hotlines and complaints filed with the Better Business Bureau and the U.S. Postal Service. The number one consumer complaint category during calendar year 2009 was identity theft: a total of 278,078 consumers (or 21 percent of all reported claims) were affected.⁵

This data seems to indicate that consumers remain justifiably concerned about identity theft and identity fraud.

Question 4. Do you believe that companies should be required to maintain appropriate safeguards protecting sensitive consumer data?

Answer. Consumers Union strongly believes that companies should be required to maintain appropriate safeguards protecting sensitive consumer data. When entities require or induce consumers to provide personal information in exchange for receiving a good or service, those entities must also ensure that the personal information they store and use is handled in a secure and responsible manner. Consumer confidence in the marketplace will decrease if consumers believe their information can easily be lost or stolen.

¹“Fourth Annual U.S. Cost of Data Breach Study,” Ponemon Institute, January 2009 <<http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf>>.

²*Id.*

³“Recession increases people's fear of identity theft,” Mintel Comperemedia, December 29, 2010 <<http://www.comperemedia.com/pressreleases/743>>.

⁴“Consumer Sentinel Network Data Book for January–December 2009,” Federal Trade Commission, February 2010 <<http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf>>.

⁵*Id.*

Question 5. What are the most necessary provisions of this legislation? Currently, how well are consumers protected against identity theft, fraud and other harm?

Answer. A number of states already require notification of data breach. However, the requirements differ from state to state, and many of the laws take different approaches vis-a-vis the risk threshold.

The data broker provision, which requires defined entities to maximize the accuracy and accessibility of their records, as well as to provide consumers with a process to dispute information, is a particularly necessary provision of this legislation, as this issue has not been uniformly addressed at the state level.

In addition, we appreciate the balanced approach this bill takes toward risk, allowing entities to circumvent the notification requirements only when there is “no reasonable risk of identity theft, fraud, or other unlawful conduct.” While some state laws do go even further by completely eliminating the risk threshold altogether, we believe the approach of this bill is sufficiently balanced to protect consumers.

The provision granting enforcement authority to state attorneys general and other state officials is also particularly necessary and important. So far, state attorneys general have been at the forefront of the battle against identity theft. Giving state officials enforcement authority means placing more cops on the beat, thus increasing chances that bad behavior will be singled out and punished.

Question 6. Which provisions in my bill do you support most strongly?

Answer. Consumers Union strongly supports S. 3742. We believe this bill will allow consumers to better protect themselves and limit loss resulting from data breach, as well as provide incentives for compliance to put in place responsible information security practices. The provisions which we believe will best achieve these purposes are:

1. The requirement that both for-profit and non-profit entities put in place responsible information security policies;
2. The bill’s notification provisions, which require notification to consumers within 60 days of the breach;
3. The bill’s requirement that all entities provide 2 years of free credit reports or credit monitoring in case of breach;
4. The bill’s focus on information brokers, and its requirements that such brokers maximize accuracy and access to records, as well as providing a way for consumers to dispute information; and
5. The provision allowing state Attorneys General and other state officials or agencies to bring enforcement actions against any entity violating this bill.

Question 7. Does Consumers Union believe it is important to require both non-profit and private sector entities to protect the security of the personal consumer data they maintain and to provide breach notice? Is the scope of the bill appropriate in your view?

Answer. Consumers Union believes that it is important to require both non-profit and private sector entities to protect the security of the personal consumer data they maintain and to provide breach notice. Consumers face the same risks when personal data is compromised, regardless of whether the breach is associated with a for-profit or non-profit entity. While we are certainly cognizant of the fact that many non-profits may not have the resources to provide notification or credit monitoring, we believe that the bill’s provisions exempting such action due to excessive cost are sufficient.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO
STUART K. PRATT

Question 1. What is the risk that a data breach poses to consumers in today’s economy?

Answer. CDIA believes that data breaches often do pose a risk to consumers, and that if there is a significant risk of harm, consumers should be notified of that risk. However, there are also many types of data breaches that do not pose specific risks to consumers, and in those cases, providing a notice to consumers could be counter-productive.

Specifically, CDIA agrees with the FTC, that:

“[t]he challenge is to require notices only when there is a likelihood of harm to consumers. There may be security breaches that pose little or no risk of harm, such as a stolen laptop that is quickly recovered before the thief has time to boot it up. Requiring a notice in this type of situation might create unneces-

sary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, notices may be more common than would be useful. As a result, consumers may become numb to them and fail to spot or act on those risks that truly are significant. In addition, notices can impose costs on consumers and on businesses, including businesses that were not responsible for the breach. For example, in response to a notice that the security of his or her information has been breached, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on his or her credit files, or obtain a new driver's license number. Each of these actions may be time-consuming for the consumer, and costly for the companies involved and ultimately for consumers generally.”¹

Question 2. Are consumers concerned about identity theft these days?

Answer. Although CDIA has not reviewed any recently conducted polling on this issue, we believe that anecdotal evidence and press accounts demonstrate that some consumers are concerned about identity theft.

Question 3. What is the average cost per incident of a data breach in the United States?

Answer. CDIA does not have any basis to draw an estimate.

Question 4. Do you believe that companies should be required to maintain appropriate safeguards protecting sensitive consumer data?

Answer. Yes, CDIA has testified in favor of such requirements, as long as they are a true national standard that focuses on safeguarding sensitive personal information, scaled appropriately for size and type of company and sensitivity of data.

However, as I stated in my testimony, “While CDIA’s members support the creation of a national standard for data security, we believe that it is also critical that such a standard not interfere with the operation of other Federal laws which already exist. To accomplish this, additional work must be done to fine-tune the exception in the current bill, intended to avoid duplicative and potentially confusing requirements.”

Question 5. What are the most necessary provisions of this legislation? Currently, how well are consumers protected against identity theft, fraud and other harm?

Answer. While CDIA supports the data security and breach notification provisions in this legislation, we believe that the most important provisions are the information broker provisions because if these provision are retained, their inclusion undermines the effectiveness of the bill, and could expose consumers and businesses to increased risk of identity theft, fraud and other harm.

CDIA is not in a position to comment on how well consumers are currently protected, but we strongly believe that if the “information broker” provisions of this legislation are not removed, the ability of companies to fight identity theft, fraud and other harm could be severely compromised, as the effectiveness of the tools that CDIA members provide to assist companies in these endeavors could be weakened.

Question 6. Which provisions in my bill do you support most strongly?

Answer. While CDIA supports the data security and breach notification provisions in this legislation, we believe that the inclusion of the information broker provisions undermines the effectiveness of the bill, because if these provision are retained, their inclusion undermines the effectiveness of the bill, and could expose consumers and businesses to increased risk of identity theft, fraud and other harm. Therefore, CDIA urges you to strike these provisions from the legislation.

Further, as I stated in my testimony: “While CDIA’s members support the creation of a national standard for data security, we believe that it is also critical that such a standard not interfere with the operation of other Federal laws which already exist. To accomplish this, additional work must be done to fine-tune the exception in the current bill. Allowing a company to be exempt from a data security standard only when it is ‘in compliance with’ a similar standard found in another law imposes two sets of duties, two sets of costs and two sets of liability on that company. For CDIA’s largest and smallest businesses this is an unnecessary burden. For our smallest businesses this duty likely increases the costs of the Errors and Omissions insurance policies which have to cover this dual liability risk. We urge the Committee to adjust the exception so that is not an ‘in compliance with’ test and to instead use a ‘subject to’ test.”

Question 7. To what extent should your members be required to protect sensitive personal information?

¹Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Science, and Transportation, 109 Cong. (Jun. 16, 2005), available at <http://www.ftc.gov/2005/06/050616databreaches.pdf>.

Answer. CDIA members take their responsibility to protect sensitive consumer information seriously, whether they are required to do so under law or not. They have developed sophisticated methodologies to ensure that the data that they hold is protected.

In terms of legal requirements, CDIA members that operate as financial institutions under GrammLeach-Bliley are required to protect sensitive information. Other legal requirements, such as Section 5 of the FTC Act, also bind our members, even where they may not fall into the GLB data protection requirements, and CDIA companies take their responsibility to protect data seriously.

Question 8. Is a national standard for information security requirements necessary in your view? If so, why?

Answer. CDIA believes that a national information security standard would be helpful, but is not necessary. Specifically, there are already 46 states that have enacted some form of data security requirement, and we believe that an additional Federal requirement is necessary *only to the extent that it fully and completely establishes a real national standard and preempts these state laws.*

Question 9. How should businesses dispose of sensitive consumer information?

Answer. CDIA believes that the appropriate standards for disposal have been established through Section 628 of the Fair Credit Reporting Act (FCRA), and the accompanying regulations. We would urge the Committee to retain that language.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO
MELISSA BIANCHI

Question 1. What is the risk that a data breach poses to consumers in today's economy?

Answer. The AHA has not undertaken any independent and/or systematic research specifically about this issue. Rather, we typically rely on—and are very aware of—publically available information about data breaches, including the likely incidence and impact of breaches both generally and in the health care field. A recent study, 2010 Data Breach Investigations Report, conducted by the Verizon Business RISK team in cooperation with the United States Secret Service (available at http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf), for example, found that healthcare accounts for only about 3 percent of data breaches.

HHS is now collecting and displaying information on data breaches of unsecured PHI under new expanded HIPAA requirements mandated by HITECH. The new requirements obligate HIPAA covered entities to report such breaches to HHS in addition to providing notice to affected individuals and, for larger breaches, the media. Specifically, if the breach involves more than a total of 500 individuals, regardless of their residency, the covered entity must notify the Secretary of HHS concurrently with the required notification sent to the affected individuals as well as notify the media. For all other breaches, the covered entity must maintain a log documenting the breaches that occur during the year and submit that log to HHS no later than 60 days after the end of each calendar year. HHS' breach notification rule also requires the Secretary to post on the HHS Website a list of breaches involving more than 500 individuals. This list must identify each covered entity involved in the breach where the unsecured PHI of more than 500 individual is acquired or disclosed. Such information will be helpful in understanding the incidence and impact of data breaches and effective strategies for reducing their occurrence and mitigating their impact.

Question 2. Are consumers concerned about identity theft these days?

Answer. Again, the AHA has not undertaken any independent and/or systematic research specifically about the issue, and we typically rely on publicly available information that suggests consumers generally remain concerned about identity theft. The AHA and its member hospitals share patients' concerns about identity theft, especially about the unique impact of identity theft in the health care delivery context.

For hospitals and other health care providers, identity theft creates concerns for patient safety and quality of care; and, accordingly, hospitals and health care providers take the issue very seriously. In addition to the financial harm associated with other types of identity theft, identity theft in health care creates real risks of patients receiving improper medical care and may endanger patients' health because of inaccurate entries in their medical records. Patients who are victims of identity theft also may have their insurance depleted, become ineligible for health or life insurance, or risk becoming disqualified from some jobs.

Question 3. What is the average cost per incident of a data breach in the United States?

Answer. Again, the AHA has not undertaken any independent and/or systematic research specifically about the issue, and we typically rely on publicly available information.

Question 4. Do you believe that companies should be required to maintain appropriate safeguards protecting sensitive consumer data?

Answer. The AHA believes that it is important for companies to take appropriate measures to protect sensitive consumer information. Hospitals already do this as part of their HIPAA compliance obligations. HIPAA requires hospitals and other covered entities to implement detailed protocols for protecting the privacy and security of the patient information they maintain. HIPAA includes rules for notifying patients in the event of a security breach. Under the Security Rule, for example, a hospital must maintain the confidentiality, integrity, and availability of electronic protected health information that it creates, receives, maintains, or transmits. In practice these terms have the following meanings:

- confidentiality—preventing disclosure of EPHI to unauthorized persons or processes;
- integrity—preventing unauthorized alteration or destruction of EPHI; and
- availability—ensuring that EPHI is accessible and useable when needed by authorized persons.

The Security Rule also requires the performance of a entity-wide risk analysis of all information systems that handle electronic protected health information and the implementation of a risk management program that includes security measures to reduce the identified risks to a reasonable and appropriate level. Hospitals also must periodically update security measures as necessary and appropriate to enhance the security of patient information and address new and emerging security threats. These are only a few of the HIPAA Security Rule's comprehensive requirements.

Question 5. What are the most necessary provisions of this legislation? Currently, how well are consumers protected against identity theft, fraud and other harm?

Answer. The legislation would provide consumers with better protection of their personal information held by a wide range of entities, similar to the protection already afforded personal information held by HIPAA covered entities. In the hospital setting, patient information—including demographic information, Social Security Numbers and financial information—already is well protected. HIPAA has mandated comprehensive protection of patient information for nearly a decade. Under the HITECH Act, Congress recently strengthened the HIPAA privacy and security requirements as well as HHS' ability to enforce HIPAA. The HITECH Act also increased penalties for noncompliance and gave state attorneys general the ability to enforce HIPAA directly as well as establish a Federal framework for data breach notification for HIPAA covered entities. As a result of the HITECH Act, business associates of HIPAA covered entities also are directly subject to HIPAA's provisions. This means that protected health information held by business associates also is protected under HIPAA's comprehensive framework.

Question 6. Which provisions in my bill do you support most strongly?

Answer. The AHA and its members support robust privacy protections for personal information. As applies to hospitals, however, we believe that the protections proposed under the Data Security and Breach Notification Act duplicate those already in place under HIPAA. We believe that the provisions of this Act are wholly duplicative of compliance requirements imposed by HIPAA and, therefore, that any provisions in the bill are unnecessary as applied to the protected health information held by HIPAA covered entities and their business associates.

Question 7. Can you think of any instances in which it might be important for hospitals to follow the security safeguards and requirements outlined in S. 3742?

Answer. Protected health information held by hospitals and other HIPAA covered entities, as well as by their business associates, already is protected by HIPAA. The protections proposed in S. 3742 mirror the HIPAA protections. Subjecting HIPAA covered entities to S. 3742 would require hospitals to establish two separate compliance programs—one for HIPAA, and one to comply with the FTC rules established under S. 3742. This will increase compliance costs for HIPAA covered entities—costs likely to ultimately be borne by patients in the form of higher health care costs. These additional compliance requirements, however, will not increase the protection of consumer information. The requirements proposed under S. 3742 are not more robust than HIPAA and will not afford consumers any greater protection.

In some cases, hospitals do not maintain certain employee information as part of their HIPAA covered functions. These hospitals may instead maintain this information separate from their health care component. In these cases, the personal information of hospital employees (other than information held by a hospital's self-funded health plan, which is protected by HIPAA) would not be considered protected health information and would not be protected by HIPAA. Where this employee information resides outside of the sphere of HIPAA protection, we believe it would be appropriate to apply the protections of S. 3742 that apply to personal information held by employers generally.

CONSUMER DATA INDUSTRY ASSOCIATION
Washington, DC, December 7, 2010

Senator ROGER WICKER,
Washington, DC.

Dear Senator Wicker,

I again appreciate the opportunity to testify before the Senate Commerce Committee regarding S. 3742, The Data Security and Breach Notification Act of 2010, and I am writing today to follow up on the questions you asked about the breach notification trigger.

CDIA has polled our members and some of the law firms which often advise companies which have been the victim of a crime resulting in the breach of sensitive personal information, and the one constant that they report is that there is no means of determining how individual state triggers operate due to the fact that breaches are multi-state and so decisions don't pivot off of an individual state's notice trigger. One very experienced outside counsel makes the following point:

"The best way to prevent extraneous notices from being sent would be a robust and uniform trigger appropriately tailored to areas where there is a significant risk of identity theft."

CDIA agrees with this.

The question of the trigger is one way of measuring the likelihood of notices being sent, but not the only one. If the definition of sensitive personal information is very broad, for instance, then this too affects the frequency with which notices are sent. CDIA continues to disagree with giving the FTC regulatory powers which allow it to add to the statutory definition of sensitive personal information which, when breached, would lead to a breach notice. The definition of "harm" could also have an impact on the number and usefulness of breach notification notices. For instance, as indicated by the Consumers' Union witness at the hearing, they are moving toward a theory that most types of data losses, including the loss of de-identified data, should give rise to a notice. They also testified that most breaches of data should result in notices.

I hope the above is of some help to you as you consider both the question of the threshold for a trigger and also the scope of the definition of the data associated with breaches. CDIA also remains very concerned about the data broker provisions and continues to believe that this section must be dropped from the bill in its entirety in order to even consider moving a uniform standard for data breach notification and data security.

CDIA continues to support passage of an appropriately structured breach notification duty and a duty to secure sensitive personal information, but only if there is a true national standard and not just a 51st standard that layers into the various state laws.

Thank you for your consideration.
Sincerely,

STUART K. PRATT,
President and CEO.

○