Calendar No. 563

111TH CONGRESS
2d Session

SENATE

REPORT
111–290

DATA BREACH NOTIFICATION ACT

SEPTEMBER 15, 2010.—Ordered to be printed

Mr. LEAHY, from the Committee on the Judiciary, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany S. 139]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to which was referred the bill (S. 139) to require Federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information, having considered the same, reports favorably thereon, without amendment, and recommends that the bill do pass.

CONTENTS

89–010

I. BACKGROUND AND PURPOSE OF THE DATA BREACH NOTIFICATION ACT

A. SUMMARY

In the first decade of the 21st century, American consumers have borne witness to an explosion in the commerce of digital information. From Government agencies to financial institutions, from doctors' offices to retail stores, entities are collecting and storing sensitive personal information by the gigabyte. Such widespread use of electronic data to identify individuals expedites everyday transactions, with great benefit to consumers: Systems access information faster; businesses conduct individually-tailored transactions more effectively; and Government agencies can now transfer data at lightning speed. Convenience, however, comes hand-in-hand with risks. Cyberspace has become a primary platform for domestic and international crime; data privacy, in turn, is now essential to our individual and collective security.

In February of 2009, Director of National Intelligence, Dennis C. Blair provided the following details on the threats, "spam—unsolicited email that can contain malicious software—now accounts for 81 percent of all email according to Message Labs (Symantec); the Georgia Tech Information Security Center projects a ten-fold increase in malicious software targeting data in the coming year; and botnets—networks of hijacked computers used to deliver spam or launch distributed denial of service attacks—are expected to compose 15 percent of all online computers in 2009." [1] The technology necessary to employ cyber attacks, in other words, is increasingly accessible. It can also be devastatingly dangerous.

Despite the acknowledged threats, however, United States privacy law has failed to keep pace with technological developments. The Data Breach Notification Act aims to enhance data security by ensuring that individuals and law enforcement are notified when sensitive personal information is put at risk and by creating incentives for entities to take steps to secure their data systems. Multiple Federal entities, including the Secret Service, the Federal Trade Commission,[2] and President George W. Bush's Identity Theft Task Force,[3] have urged Congress to pass such legislation. It is long past time for Congress to enact a single, national standard for notification in the event of a data breach.

B. INCREASING RISKS FROM DATA BREACHES

1. Identity theft

When asked about their daily concerns, consumers in the United States place identity theft at the top of the list. At the Federal Trade Commission, where consumer concerns flood in every day,

---

[1] Director of National Intelligence Dennis C. Blair, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence (Unclassified Version), at 39 (February 12, 2009), available at *http://intelligence.senate.gov/090212/blair.pdf*.

[2] See Protecting the Privacy of the Social Security Number from Identity Theft: Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways & Means, 110th Cong. 14 (2007) (statement of the Federal Trade Commission), available at *http://www.ftc.gov/os/testimony/P065409socsectest.pdf;* Data Breaches and Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation, 109th Cong. 7 (2005) (statement of the Federal Trade Commission), available at *http://www.ftc.gov/os/2005/06/050616databreaches.pdf*.

[3] President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, 34–37 (2007), available at *http://www.idtheft.gov/reports/StrategicPlan.pdf*.

complaints about identity theft rank above concerns about deceptive advertisements, harassing telemarketing, or unfair credit practices.[4] In April of 2007, Zogby Interactive Survey found that 91 percent of adult users of the Internet were concerned that their identities might be stolen;[5] and a September 2009 Unisys Security Index survey found that 65 percent of American respondents were "seriously concerned" about misuse of their personal information—more respondents than expressed worry over the H1N1 virus in the headlines at the time.[6]

Such widespread concerns are not surprising. Security breaches are rampant, and identity theft places a heavy toll on its victims. The Privacy Rights Clearinghouse reports that between 2005 and 2009 security breaches allowed unauthorized access to more than 340 million records containing individuals' sensitive personal information.[7]

These breaches make clear that vulnerabilities exist across industries, and in entities both public and private. For example, in February 2009, the Federal Aviation Administration announced a breach pursuant to which 45,000 records containing current and former employees' personal information were exposed;[8] in January 2009, Heartland Payment Systems provided public notice that hackers had installed malicious software on the company's payment processing network and accessed more than 130 million credit card accounts;[9] in December 2008, Royal Bank of Scotland Group PLC's processing unit, RBS Worldpay, disclosed that a breach of its payment systems had put more than 1.5 million consumers' financial records and more than 1.1 million social security numbers at risk;[10] earlier that year, State Department officials informed three leading Presidential candidates that contractors had accessed their passport files without authorization;[11] and in January 2007, TJX Companies, the parent company of retailers Marshalls and TJ Maxx, announced that hackers had accessed information from more than 45 million credit and debit cards.[12] These breaches present a grave and real threat for consumers, Government, and business entities.

Once information is obtained, the potential for harm is great. Financial account numbers are sold cheaply on the Internet black market, with a Russian website advertising stolen credit card numbers with limits above $10,000 at the price of $50 for a batch of

---

[4] Director of National Intelligence Dennis C. Blair, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence (Unclassified Version), at 39 (February 12, 2009), available at *http://intelligence.senate.gov/090212/blair.pdf*.

[5] Zogby International, Zogby Poll: Most Americans Worried About Identity Theft, Apr. 3, 2007, *www.zogby.com/search/ReadNews.dbm?ID=1275* (last visited Jan. 11, 2010).

[6] Unisys Corporation, Unisys Security Index: United States (2009), available at *http://www.unisyssecurityindex.com/resources/reports/US%20Security%20Index%20Oct%2009.pdf*.

[7] Privacy Rights Clearinghouse, Chronology of Data Breaches, *http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP* (last visited Jan. 11, 2010).

[8] Joe Davidson, FAA's Latest Security Challenge Is in Cyberspace, Not the Skies, Washington Post, D3 (February 11, 2009).

[9] Brian Krebs, Payment Processor Breach May Be Largest Ever, Washington Post Security Fix (January 20, 2009), *http://voices.washingtonpost.com/securityfix/2009/01/paymentlprocessorlbreachlmaylb.html*.

[10] Press Release, RBS WorldPay, RBS WorldPay Announces Compromise of Data Security and Outlines Steps to Mitigate Risks (Dec. 23, 2008), available at *http://www.rbsworldpay.us/RBSlWorldPaylPresslReleaselDecl23.pdf*.

[11] Amy Schatz, Congress Raises Call for Data Safeguards, Wall Street Journal, A4 (March 30, 2008).

[12] TJX Says Theft of Credit Data Involved 45.7 Million Cards, New York Times, C2 (March 30, 2007).

ten as early as 2004.[13] Debit card numbers may be used to siphon money globally from automatic teller machines. And sensitive personally identifiable information may be used for acts as various as opening fraudulent credit accounts, leasing property under false names, evading sanctions by providing false identities to law enforcement, and stalking.

These immediate harms are not the only concerns. Victims of identity theft who suffer no direct financial loss may find their credit ruined and their lives disrupted as they spend upwards of 80 hours to restore their records.[14]

Data breaches cost U.S. businesses as well. In 2008, the average cost to private companies was $6.65 million per data breach.[15] Adding to such direct costs is the revenue lost when consumers decrease purchases based on fear of identity theft. In 2006, 30 percent of consumers polled by the Wall Street Journal said that they limited their online purchases because of such fears, and 24 percent said they had cut back on online banking.[16]

2. Organized crime and cybersecurity

Today's larger, more carefully targeted, and more sophisticated data breaches are increasingly perpetrated by organized crime rings working across national boundaries. In the past year alone, Federal prosecutors indicted an American and two Russian co-conspirators for installing malicious software in grocers' payment systems to fraudulently obtain more than 4.2 million credit and debit card accounts,[17] and individuals from Russia, Estonia, and Moldova for using sophisticated hacking techniques to compromise RBS Worldpay's data encryption protection and gain access to over 1.5 million financial accounts and 1.1 million social security numbers.[18]

Intrusions by cybercriminals and foreign states have also placed sensitive military information, valuable intellectual property, and essential infrastructure at risk. As documented by the Office of the Director of National Intelligence, nations, including Russia and China, have the technological capability to collect intelligence information from U.S.-based networks and to use such networks to interfere with our national infrastructure, and "terrorist groups, including al-Qa'ida, HAMAS, and Hizballah, have expressed the desire to use cyber means to target the United States."[19] In 2009 alone, we have seen computer technology utilized to penetrate civil-

---

[13] Brian Krebs, Phishing Feeds Internet Black Markets, WashingtonPost.com (November 10, 2004), *http://www.washingtonpost.com/wp-dyn/articles/A59347–2004Nov18.html*.

[14] Jon Swartz, Survey: ID Theft Takes Time to Wipe Clean, USA Today, B1 (July 28, 2005).

[15] Ponemon Institute, Fourth Annual U.S. Cost of Data Breach Survey (2009), available at *http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008–2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf*.

[16] Jennifer Cummings, Substantial Numbers of U.S. Adults Taking Steps to Prevent Identity Theft, Harris Interactive & Wall Street Journal Online, May 18, 2006, *http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=1058*.

[17] Jerry Harkavy, Illicit Software Placed on Hannaford Servers Blamed for Breach of 4.2 Million Cards, Brattleboro Reformer (March 28, 2008).

[18] Press Release, Federal Bureau of Investigation, International Effort Defeats Major Hacking Ring (November 10, 2009), available at *http://atlanta.fbi.gov/dojpressrel/pressrel09/atl111009.htm*.

[19] Director of National Intelligence Dennis C. Blair, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence (Unclassified Version), at 39 (Feb. 12, 2009), available at *http://intelligence.senate.gov/090212/blair.pdf*.

ian air traffic control networks,[20] the U.S. electrical grid,[21] defense projects such as the Pentagon's Joint Strike Fighter project,[22] and live video feeds from operational U.S. Predator drones.[23] The United States as a Nation, like each individual American consumer, can no longer afford to take data security for granted.

To track the use of new technologies for disrupting computer networks, to trace profits obtained via technological theft, and to apprehend those responsible for breaches, Federal law enforcement needs information about cyber crimes to effectively safeguard individuals and the national security.

C. THE DATA BREACH NOTIFICATION ACT

Federal data breach notification legislation is an essential step toward protecting data security in the United States. The Data Breach Notification Act would serve the dual purpose of informing consumers when their personal information is at risk and informing Federal law enforcement when a breach has occurred.

The bill provides a single Federal standard—ensuring that U.S. consumers receive notice of a breach wherever they live, that businesses have clear notification standards to follow across State lines, and that Federal law enforcement receives the information it needs to protect public safety and national security. Supporters of the legislation include Consumers Union and the Business Software Alliance.

1. Providing notice to consumers

First, S. 139 requires that a business or Government entity that experiences a data breach promptly notify any consumer whose sensitive personally identifiable information has been exposed. In 2002, California led the nation by enacting S.B. 1386, the first State law to require that businesses notify consumers in the event of a breach.[24] Today, there is national consensus that such notice is necessary to allow consumers to take steps to prevent identity theft. Forty-five States, the District of Columbia, Puerto Rico, and the Virgin Islands currently have laws requiring that consumers receive notice of data breaches.

The bill strikes a careful balance between over-notification and underreporting of data breaches. Section 3(b) provides a safe harbor releasing an entity from the obligation to notify consumers if there is "no significant risk that a security breach has resulted in, or will result in, harm to the individual." This notification trigger recognizes that there are harms other than identity theft that can result from a data breach—harms such as financial crimes and stalking—while simultaneously acknowledging that consumers may not respond to notices if they arrive frequently when there is no risk of harm.

---

[20] Siobhan Gorman, FAA's Air-Traffic Networks Breached by Hackers, Wall Street Journal, A4 (May 7, 2009).
[21] Siobhan Gorman, Electricity Grid in U.S. Penetrated by Spies, Wall Street Journal, A1 (April 8, 2009).
[22] Siobhan Gorman, August Cole, & Yochi Dreazen, Computer Spies Breach Fighter-Jet Project, Wall Street Journal, A1 (April 11, 2009).
[23] Siobhan Gorman, August Cole, & Yochi Dreazen, Insurgents Hack U.S. Drones, Wall Street Journal, A4 (December 17, 2009).
[24] Cal. Civ. Code §§ 1798.29, .82, .84.

The bill provides additional exemptions to the notice requirement when a law enforcement or national security reason counsels against immediate notice and allows reasonable delay for an entity to conduct a risk assessment to determine the threat posed by a breach.

The requirements for notice are specific. Individuals must be notified in writing, by telephone, or by email if they have consented to such notice. When a breach places the sensitive personally identifiable information of more than 5,000 residents of a State at risk, notice must also be provided according to Section 4(2) through major media outlets in the State.

2. Increasing law enforcement capabilities to protect and enhance cybersecurity

Second, to enhance Federal law enforcement's capabilities in fighting cybercrime, S. 139 mandates that notice immediately be provided to the Secret Service in the event that a breach involves unauthorized access to more than 10,000 individuals' sensitive personally identifiable information or to a database containing the sensitive personally identifiable information of more than 1,000,000 individuals nationwide. The bill also empowers the Secret Service to obtain additional information about the data breach from business entities and requires that it provide further notice to Federal agencies such as the Federal Bureau of Investigation, the U.S. Postal Inspection Service, and State Attorneys General, who may be involved in preventing further harm from the breach or the perpetration of additional breaches.

In Congressional testimony, the Department of Justice has specifically urged Congress to require security breach reporting to Federal law enforcement, including both the U.S. Secret Service and the Federal Bureau of Investigation. This law is intended to ensure that law enforcement receives such notice of data breaches.[25] Additionally, as highlighted in the President's 2009 Cyberspace Policy Review, partnerships among Government agencies, law enforcement, and private industry are essential to addressing cybersecurity-related risks.[26] The bill is intended to facilitate interagency and public-private cooperation to solve and prevent data breaches.

3. Enforcement

Third, S. 139 contains strong civil enforcement provisions. The bill authorizes State Attorneys General, or the U.S. Attorney General, to bring a civil enforcement action against violators of the bill's notification requirements and to recover a civil penalty of not more than $1,000 per affected individual, per day, and a maximum penalty of $1,000,000 per violation, unless the violation is willful or intentional. It is not uncommon for Congress to authorize both Federal and State entities to enforce Federal consumer protection laws. In fact, Federal antitrust laws, the CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act

[25] Identify Theft: A Victims Bill of Rights: Hearing Before the Subcomm. on Information Policy, Census and National Archives of the H. Comm. on Oversight and Government Reform, 111th Cong. 9 (2009) (statement of Deputy Assistant Attorney General Jason M. Weinstein), available at *http://oversight.house.gov/images/stories/documents/20090617111143.pdf.*

[26] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, at iv (May 29, 2009), available at *http://www.whitehouse.gov/assets/documents/Cyberspace1Policy1Review1final.pdf.*

of 2003), and the Communications Act of 1934 also authorize State Attorneys General to seek damages or to enjoin further Federal law violations. The State enforcement provisions in S. 139 are modeled after those laws and require cooperation and communication between Federal and State entities to prevent duplication of efforts.

The bill authorizes the Secret Service to investigate data security breaches and to provide guidance to companies that have been the victim of a data security breach on their notice obligations under the bill. Since 1984, Congress has provided statutory authority for the Secret Service to investigate a wide range of financial crimes, including offenses under 18 U.S.C. § 1028 (false identification fraud), § 1029 (access device fraud), § 1030 (computer fraud). In the last two decades, the Secret Service has conducted more than 733,000 financial fraud and identity theft investigations involving these statutes, leading to the prosecution of more than 116,000 individuals.[27]

Section 316(b) of the bill expressly requires that the FBI must be notified of any data security breach that involves espionage, foreign counterintelligence, or national security matters. Under title 18, section 1030(d)(1), the Secret Service and FBI have concurrent jurisdiction to investigate violations of section 1030 relating to false identification fraud, access device fraud, and computer fraud. Section 1030 designates the FBI as the primary investigative agency for such offenses if they involve espionage, foreign counterintelligence, or other national security matters. Accordingly, the bill incorporates this requirement in the context of breach notice, so that the FBI is promptly notified of any data breach matters that involve espionage, foreign counterintelligence, or national security.

4. Preemption

Fourth, the legislation balances the important role of States as leaders on privacy issues with the recognized need for Federal uniformity in breach notification law. As discussed in the President's Identity Theft Task Force Report of September 2008, "at present, there is no single data security or breach notification standard that applies in the United States. Rather, there is a patchwork of state laws and sector-specific Federal laws and regulations that are varied and have uneven application."[28] The bill preempts State laws on breach notification in order to provide a clear, national standard. The bill also, however, carves out an exception for State laws requiring that consumers be provided with additional information about victim protection assistance available in certain States. Finally, the bill's requirements do not apply to State or local government entities, and the Committee does not intend for the bill to preempt or displace State laws that address obligations of State and local government entities to provide notice of a security breach.

II. HISTORY OF THE BILL AND COMMITTEE CONSIDERATION

A. INTRODUCTION OF THE BILL

Senator Dianne Feinstein introduced the Data Breach Notification Act on January 6, 2009. This legislation is very similar to the

[27] United States Secret Service, White Paper: Data Broker Legislation—S.1490 (2007).

[28] President's Identity Theft Task Force Report, Combating Identity Theft: A Strategic Plan, 13 (2008), available at *http://www.idtheft.gov/reports/IDTReport2008.pdf*.

Notification of Risk to Personal Data Act of 2007, S. 239, which Senator Feinstein introduced on January 10, 2007, and to the Notification of Risk to Personal Data Act of 2005, S. 751, which Senator Feinstein introduced on April 11, 2005. The Judiciary Committee favorably reported S. 239 on May 3, 2007, by voice vote with an amendment in the nature of a substitute. The legislation is also very similar to Subtitle B of the Personal Data Privacy and Security Act of 2009, S. 1490. The Committee favorably reported S. 1490 on November 5, 2009 with amendments.

The Committee has held two hearings directly related to S. 139. On March 21, 2007, the Judiciary Committee's Subcommittee on Terrorism, Technology and Homeland Security held a hearing titled, "Identity Theft: Innovative Solutions for an Evolving Problem." This hearing examined the problem of identity theft and legislative solutions to this problem, and discussed the need for Federal legislation on data breach notification. The following witnesses testified at this hearing: Ronald Tenpas, Associate Deputy Attorney General, United States Department of Justice; Lydia Parnes, Director Bureau of Consumer Protection, Federal Trade Commission; James Davis, Chief Information Officer and Vice Chancellor for Information Technology, University of California, Los Angeles; Joanne McNabb, Chief California Office of Privacy Protection; and Chris Jay Hoofnagle, Senior Staff Attorney, Samuelson Law, Technology & Public Policy Clinic, School of Law (Boalt Hall), University of California, Berkeley.

On April 13, 2005, the Judiciary Committee held a hearing titled, "Securing Electronic Personal Data: Striking a Balance between Privacy and Commercial and Governmental Use." This hearing examined the growing problem of breaches of data security and the practices and weaknesses of the rapidly growing data broker industry. The hearing also explored legislative options for ensuring that consumers who were at risk of identity theft could protect their personal data and take steps to prevent the misuse of their private information. The following witnesses testified at this hearing: Deborah Platt Majoras, Chairman of the Federal Trade Commission; Chris Swecker, Assistant Director for the Criminal Investigative Division at the Federal Bureau of Investigation; Larry D. Johnson, Special Agent in Charge of the Criminal Investigative Division of the U.S. Secret Service; William H. Sorrell, President of the National Association of Attorneys General; Douglas C. Curling, President, Chief Operating Office, and Director of ChoicePoint, Inc.; Kurt P. Sanford, President & CEO of the U.S. Corporate & Federal Markets LexisNexis Group; Jennifer T. Barrett, Chief Privacy Officer of Acxiom Corp.; James X. Dempsey, Executive Director of the Center for Democracy & Technology; and Robert Douglas, CEO of PrivacyToday.com.

B. COMMITTEE CONSIDERATION

On October 23, 2009, S. 139 was placed on the Judiciary Committee's agenda. The Committee considered this legislation on November 5, 2009. No amendments were offered to the bill. The Committee voted to report the Data Breach Notification Act of 2009, without amendment, favorably to the Senate by roll call vote as follows:

Tally: 14 Yeas, 3 Nays, Pass 2
Yeas (14): Leahy (D–VT), Kohl (D–WI), Feinstein (D–CA), Feingold (D–WI), Schumer (D–NY), Durbin (D–IL), Cardin (D–MD), Whitehouse (D–RI), Klobuchar (D–MN), Kaufman (D–DE), Specter (D–PA), Franken (D–MN), Hatch (R–UT), Grassley (R–IA).
Nays (3): Sessions (R–AL), Graham (R–SC), Coburn (R–OK).
Pass (2): Kyl (R–AZ), Cornyn (R–TX).

III. SECTION-BY-SECTION SUMMARY OF THE BILL

Section 1. Short title

This section provides that the legislation may be cited as the "Data Breach Notification Act."

Section 2. Notice to individuals

Section 2 requires that a business entity or Federal agency give notice to an individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, compromised, following the discovery of a data security breach. The notice required under section 2 must be made without unreasonable delay. Section 2 requires that a business entity or Federal agency that does not own or license the information compromised as a result of a data security breach notify the owner or licensee of the data. The owner or licensee of the data would then provide the notice to individuals as required under this section. However, agreements between owners, licensees and third parties regarding the obligation to provide notice under section 2 are preserved.

Section 3. Exemptions

Section 3 allows a business entity or Federal agency to delay notification by providing a written certification to the U.S. Secret Service that providing such notice would impede a criminal investigation, or damage national security. This provision further requires that the Secret Service must review all certifications from business entities (and may review certifications from agencies) seeking an exemption from the notice requirements based upon national security or law enforcement, to determine if the exemption sought has merit. The Secret Service has 10 business days to conduct this review, which can be extended by the Secret Service if additional information is needed. Upon completion of the review, the Secret Service must provide written notice of its determination to the agency or business entity that provided the certification. If the Secret Service determines that the exemption is without merit, the exemption will not apply. Section 312 also prohibits Federal agencies from providing a written certification to delay notice, to conceal violations of law, prevent embarrassment or restrain competition.

Section 3(b) exempts a business entity or agency that conducts a risk assessment after a data breach occurs, and finds no significant risk of harm to the individuals whose sensitive personally identifiable information has been compromised, from the notice requirements of section 2, provided that: (1) the business entity or Federal agency notifies the Secret Service of the results of the risk assessment within 45 days of the security breach; and (2) the Secret Service does not determine within 10 business days of receipt the notification that a significant risk of harm does in fact exist

and that notice of the breach should be given. Under section 3(b) a rebuttable presumption exists that the use of encryption technology, or other technologies that render the sensitive personally identifiable information indecipherable, and thus, that there is no significant risk of harm.

Section 3(c) also provides a financial fraud prevention exemption from the notice requirement, if a business entity has a program to block the fraudulent use of information—such as credit card numbers—to avoid fraudulent transactions. Debit cards and other financial instruments are not covered by this exemption.

Section 4. Methods of notice

Section 4 provides that notice to individuals may be given in writing to the individuals last known address, by telephone or via email notice, if the individual has consented to email notice. Media notice is also required if the number of residents in a particular State whose information was, or is reasonably believed to have been, compromised exceeds 5,000 individuals.

Section 5. Content of notification

Section 5 requires that the notice detail the nature of the personally identifiable information that has been compromised by the data security beach, a toll free number to contact the business entity or Federal agency that suffered the breach, and the toll free numbers and addresses of major credit reporting agencies. Section 5 also preserves the right of States to require that additional information about victim protection assistance be included in the notice.

Section 6. Coordination of notification with credit reporting agencies

Section 6 requires that, for situations where notice of a data security breach is required for 5,000 or more individuals, a business entity or Federal agency must also provide advance notice of the breach to consumer reporting agencies.

Section 7. Notice to law enforcement

Section 7 requires that business entities and Federal agencies notify the Secret Service of the fact that a security breach occurred within 14 days of the breach, if the data security breach involves: (1) more than 10,000 individuals; (2) a database that contains information about more than one million individuals; (3) a Federal Government database; or (4) individuals known to be Government employees or contractors involved in national security or law enforcement. The Secret Service is responsible for notifying other Federal law enforcement agencies, including the FBI and the relevant State Attorneys General, within 14 days of receiving notice of a data security breach.

Section 8. Enforcement

Section 8 allows the Attorney General to bring a civil action to recover penalties for violations of the notification requirements in subtitle B. Violators are subject to a civil penalty of up to $1,000 per day, per individual and a maximum penalty of $1 million per violation, unless the violation is willful or intentional.

Section 9. Enforcement by State attorneys general

Section 9 allows State attorneys general to bring a civil action in U.S. district court to enforce subtitle B. The attorney general may stay, or intervene in, any State action brought under this subtitle.

Section 10. Effect on Federal and State law

Section 10 preempts State laws on breach notification, with the exception of State laws regarding providing consumers with information about victim protection assistance that is available to consumers in a particular State. Because the breach notification requirements in the bill do not apply to State and local government entities, this provision does not preempt State or local laws regarding the obligations of State and local government entities to provide notice of a data security breach.

Section 11. Authorization of appropriations

Section 11 authorizes funds for the Secret Service as may be necessary to carry out investigations and risk assessments of security breaches under the requirements of subtitle B.

Section 12. Reporting on risk assessment exemptions

Section 12 requires that the Secret Service report to Congress on the number and nature of data security breach notices invoking the risk assessment exemption and the number and nature of data security breaches subject to the national security and law enforcement exemptions.

Section 13. Definitions

Section 13 defines ''sensitive personally identifiable information'' in a limited manner. Information will qualify if it combines a person's last name and first name or first initial with one of these four categories of personal information: (1) a non-truncated social security number, driver's license number, passport number, or alien registration number; (2) two of: the individual's home address and telephone number, mother's maiden name, or complete birth date; (3) unique biometric data; or (4) a unique account number or electronic identification number in combination with an associated security code. Additionally, a financial account number will qualify as ''sensitive personally identifiable information'' if it is accessed or acquired without the account holder's name but in combination with an associated security code or password.

Section 14. Effective date

This Act takes effect 90 days after the date of enactment of this Act.

IV. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

The Committee sets forth, with respect to the bill, S. 139, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

DECEMBER 11, 2009.

Hon. PATRICK J. LEAHY,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 139, the Data Breach Notification Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Grabowicz and Matthew Pickford (for federal costs) and Marin Randall (for the impact on the private sector).

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

S. 139—Data Breach Notification Act

Summary: S. 139 would require most government and business entities that collect, transmit, store, or use sensitive personal information to notify any individuals whose information has been unlawfully accessed through a breach in the security systems designed to protect such information from unauthorized access. The legislation defines sensitive personal information as combinations of an individual's name, address or phone number, and Social Security number, driver's license number, financial account information, or biometric data (that is, finger print, voice print, or retina scan). Under certain circumstances, entities could apply to the Secret Service for exemptions from the notification requirements. In addition, S. 139 would create civil penalties for entities that fail to provide notice to affected individuals.

CBO expects that agencies would incur negligible costs to implement the legislation because they already comply with the notification requirements in the bill. Implementing S. 139 could increase collections of civil penalties that would affect revenues, but CBO estimates that any such effect would not be significant in any year. In addition, enacting S. 139 could affect direct spending for notification requirements by agencies not funded through annual appropriations. CBO estimates, however, that any changes in net spending by those agencies would be negligible. Complying with the bill's provisions could increase the expenses of the Secret Service, but CBO estimates that such costs would be less than $500,000 annually and subject to the availability of appropriated funds.

S. 139 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the cost of complying with the requirements would be small and would not exceed the threshold established in UMRA ($69 million in 2009, adjusted annually for inflation).

The notification requirements in S. 139 would impose private-sector mandates as defined in UMRA. Because most businesses already comply with similar state requirements, CBO estimates that the incremental cost to comply with the mandates would fall below the annual threshold established in UMRA for private-sector mandate ($139 million in 2009, adjusted annually for inflation).

Estimated cost to the Federal Government: Enacting S. 139 could affect both direct spending and revenues, but CBO estimates that any such effects would be negligible.

In the event of a security breach, S. 139 would require most government agencies to notify individuals whose personal information has been unlawfully accessed. Notification would be in the form of an individual notice (a written notice to a home mailing address, a telephone call, or an e-mail) as well as through the mass media for breaches involving the sensitive information of 5,000 or more individuals. The legislation also would require the agency to provide affected individuals with a description of the accessed information, a toll-free number to contact the agency, the names and toll-free telephone numbers of the major credit-reporting agencies, and in some instances, information on an individual state's victim protection assistance.

This provision would codify the current practice of the federal government regarding notifications of security breaches. While existing laws generally do not require agencies to notify affected individuals of data breaches, this has been the practice of agencies that have experienced such breaches. Therefore, CBO expects that implementing those notification provisions would probably not lead to a significant increase in spending. Nonetheless, the federal government is also one of the largest providers, collectors, consumers, and disseminators of personal information in the United States. Although CBO cannot anticipate the number of security breaches, a significant breach of security involving a major collector of personal information, such as the Internal Revenue Service or the Social Security Administration, could involve millions of individuals, and there would be significant costs to notify individuals of such a security breach.

The legislation also would require a business entity or federal agency (under certain circumstances) to notify the Secret Service that a security breach has occurred, but would permit entities or agencies to apply to the Secret Service for exemption from notice under certain circumstances. Based on information from the Secret Service, CBO estimates any additional investigative or administrative costs to that agency would likely total less than $500,000 annually and would be subject to the availability of appropriated funds.

Impact on state, local, and tribal governments: S. 139 contains intergovernmental mandates as defined in UMRA. The bill would explicitly preempt laws in at least 45 states regarding the treatment of personal information and would impose notification requirements and limitations on State Attorneys General and state insurance authorities. Because the limits on state authority would impose no duties with costs and because the notification requirements would result in minimal additional spending, CBO estimates the costs of the mandates would be small and would not exceed the threshold established in UMRA ($69 million in 2009, adjusted annually for inflation).

Estimated impact on private sector: S. 139 would impose private-sector mandates as defined in UMRA. The bill would require business entities engaged in interstate commerce that use, access, transmit, store, dispose of, or collect sensitive personally identifiable information to notify individuals if a security breach occurs

that affects the individuals' sensitive, personally identifiable information. Entities would be able to notify individuals using written letter, the telephone, or email under certain circumstances. The bill also would require those entities to notify the owner or licensee of any such information that the entity does not own or license and would require notice in major media outlets serving a state or jurisdiction for any breach of more than 5,000 residents' records within a particular state. In addition, business entities would be required to notify other entities and agencies in the event of a large security breach. Entities that experience the breach of such data would have to notify the affected victims and consumer reporting agencies if the breach involves more than 5,000 individuals, and the U.S. Secret Service if the breach involves more than 10,000 individuals. The bill, however, would exempt business entities from the notification requirements under certain circumstances.

According to industry sources, millions of individuals' sensitive personally identifiable information is breached every year. However, according to those sources, 45 states already have laws requiring notification in the event of a security breach. In addition, it is the standard practice of most businesses to notify individuals if a security breach occurs. CBO therefore estimates that the incremental costs incurred by businesses to comply with the requirements in the bill would fall below the annual threshold established in UMRA for private-sector mandate ($139 million in 2009, adjusted annually for inflation).

Previous CBO estimates: On December 2, 2009, CBO transmitted a cost estimate for S. 1490, the Personal Data Privacy and Security Act of 2009, as ordered reported by the Senate Committee on the Judiciary on November 5, 2009. On December 7, 2009, CBO transmitted a cost estimate for H.R. 2221, the Data Accountability and Trust Act, as ordered reported by the House Committee on Energy and Commerce on September 30, 2009. Those bills address security breaches of sensitive personal information and notification requirements for the federal government and private industry. S. 1490 would require agencies to prepare additional reports for the Congress on the security of sensitive personal information held by the federal government. CBO estimates that preparing those reports and other security assessments would cost $25 million over the 2010–2014 period. H.R. 2221 would require the Federal Trade Commission to develop regulations to enforce new notification requirements. CBO estimates that it would cost that agency $5 million over the 2010–2014 period to carry out those activities.

CBO determined that S. 1490 and H.R. 2221 also contained intergovernmental mandates, but any costs would be small and would not exceed the threshold established in UMRA ($69 million in 2009, adjusted for inflation). In addition, CBO determined that S. 1490 and H.R. 2221 would impose private-sector mandates that would exceed the annual threshold established in UMRA ($139 million in 2009, adjusted annually for inflation) in at least one of the first five years the mandate are in effect.

Estimate prepared by: Federal costs: Mark Grabowicz and Matthew Pickford; Impact on state, local, and tribal governments: Elizabeth Cove Delisle; Impact on the private sector: Marin Randall.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

V. REGULATORY IMPACT EVALUATION

In compliance with rule XXVI of the Standing Rules of the Senate, the Committee finds that no significant regulatory impact will result from the enactment of S. 139.

VI. CONCLUSION

By providing a Federal standard for notification in the event of a data breach, the Data Breach Notification Act, S. 139, will create a powerful incentive for government and private industry to improve the security of their data systems, will ensure that consumers are notified when their sensitive personally identifiable information is at risk, and will provide Federal law enforcement with critical information in the fight against cyber crime.

VII. ADDITIONAL VIEWS

ADDITIONAL VIEWS FROM SENATORS SESSIONS, KYL AND GRAHAM

There is bipartisan agreement on the need for congressional action to confront the growing threat posed by criminals who steal Americans' personal information. There is also a bipartisan consensus on a need for a national standard for notifying consumers and law enforcement in the event of a data breach that compromises individuals' sensitive personal information. Such notice provides law enforcement with valuable leads on how to fight cybercrime, including data and identity theft crimes, which has exploded in recent years, and which is increasingly committed by sophisticated criminal enterprises with global reach. Timely notice of genuine threats to individuals' identity information also gives consumers the opportunity to protect themselves. In order for such consumer protections to be effective, however, it is important that notices be sent after a conscientious assessment of the risk that a breach poses to consumers. If notices are sent for trivial security breaches, consumers may be overwhelmed by inconsequential notices and become more likely to ignore warnings that matter—when their identity information is genuinely at risk. If we are to succeed in our shared goal of protecting consumers, it is critical that Congress strike a careful balance. We are concerned that this bill could lead to excessive (and thus counterproductive) notice to consumers, and so we hope that the right balance can be achieved when this bill comes before the full Senate.

To date, 45 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have adopted laws governing notice to individuals whose personal identity information has been compromised. Such protection is important, but the proliferation of state laws has produced a patchwork in which the protections for consumers—and the rules for business—are uneven and at times confusing. We firmly believe that Congress should provide a uniform national standard in this area, and we commend Senator Feinstein's efforts to do so in this bill. We remain committed to the goals underlying this legislation, and we hope to work with our colleagues to craft a bill that best serves our shared interests in assisting law enforcement and protecting consumers.

BACKGROUND

Identity theft is a major concern for consumers and for businesses, and the threat posed by the increasingly sophisticated criminal enterprises that perpetrate these acts is both serious and growing. Both business and government have spent a great deal of

time and effort to understand and combat this crime. Law enforcement agencies at the federal, state and local levels have increased their cooperation, and businesses and governments at all levels have adopted more rigorous internal controls to protect individuals' information. Nevertheless, periodic breaches that compromise sensitive personal information continue to occur, because of inadequate defenses against criminals, or because of negligence in securing sensitive information. Reports this week that the National Archives may have compromised sensitive information, including Social Security numbers, for 250,000 individuals because of a single lost computer hard drive are a sober reminder of the need for better security.

Our first priority must be to ensure that consumers have the tools to protect themselves in the event of a data breach. Americans need to be notified when information pertaining to them is compromised in a way that may jeopardize their identities. For such notices to be effective, however, they must be issued only when there are reasonable grounds to do so. We know from the experience of the Gramm-Leach-Bliley Act (GLBA) that over-notification leads to consumer apathy, with the result that consumers are exposed to greater risks.

SPECIFIC CONCERNS WITH S.139, THE DATA BREACH NOTIFICATION ACT

Although we support the goals of this legislation, we have some specific concerns with S.139 as reported by the Committee, and believe that the bill could be improved in several areas.

1. The scope of protected personal information includes widely publicly-available information

The bill defines the protected class of information—"sensitive personally identifiable information"—to include widely-available information such as home address, phone number, and date of birth. Such information is frequently available in public records, and release or compromise of such information alone is not sufficient to pose a risk of identity theft. Nor is the release of such information alone sufficiently grave to justify notice to the FBI and the Secret Service.

2. The definition of Security Breach is too broad

The bill defines a breach as including unauthorized "access" or "acquisition" of sensitive personally identifiable information. While "access" to such information is a common term used in the criminal code, its use alongside "acquisition" implies that "access" refers only to instances where the personal data is not "acquired"—i.e. where the data is not in some way recorded, collected, or taken for future, potentially harmful, use. Thus, the current definition of a "breach" would appear to cover instances where information is viewed in passing, or possibly where a person obtains unauthorized access to a computer system that contains personal information, even if the invader never views or downloads the information. Such activity, however, does not threaten individuals whose data was "accessed" with any harm.

Although the definition of a Security Breach excludes "the release of a public record" that is not otherwise protected by con-

fidentiality or nondisclosure rules, the S.139 does not define a "public record" and thus the bill could be read to treat release of specific information available in a public record as a Breach while permitting release of a full public record.

3. The "harm" standard for notice to consumers is vague

One of the most valuable aspects of S. 139 is the requirement that companies who suffer data breaches report those incidents to law enforcement. That reporting requirement will assist our law enforcement agencies to better analyze and defend against the methods of increasingly sophisticated and global criminal enterprises that commonly engage in data theft. In order to avoid desensitizing the public through over-notification of such breaches, however, Congress should provide a clear risk-based standard for requiring companies to take the additional step of notifying individual consumers who might have been affected by the breach.

The standard currently in S.139, requires consumer notice unless there is "no significant risk" of "harm to the individual." "Harm" is undefined, and although the Majority suggests that the "harm" in question should cover not only identity theft but also financial crime or threats to a person's safety such as from stalking, judicial interpretations of similar state laws suggest that the current language could encompass not only such serious matters but also less concrete "harms," such as the time a person must spend to expunge negative credit information or even purely reputational "harms" that might be suffered from some types of disclosures. A more disciplined approach would be to require notice when there is a risk of "misuse of the individual's personal information for identity theft, fraud, or other illegal purposes, or financial harm to the individual."

4. Consumer notice methods and timing

S. 139 requires entities victimized by a Security Breach to send any notice to consumers "without unreasonable delay." While "reasonable delay" is defined to include the time necessary to determine the scope of the breach and secure the database from further exploitation, the bill does not currently make clear that notice may be delayed to allow the holder of the data to assess the possible risks to consumers and evaluate the need for a breach notice.

More significantly, S. 139 currently requires consumers receive both actual notice of a breach (through mail, telephone, or email) and constructive notice through announcements in major media outlets. Where actual notice is feasible, however, any constructive notice through mass media outlets is duplicative and unnecessary. Congress should follow the example of those states, including California, that call for notice through mass media only as a fall-back alternative when actual notice is impossible or impracticable. In addition, S.139 should allow consumers to be notified through whatever channels they customarily use to communicate with the business or entity whose systems were breached. As currently drafted, the bill would not permit notice via email unless a consumer has specifically consented to such email notice in advance.

5. Other Issues

We agree with the sponsors of S. 139 on the need for Congress to set a uniform national standard for breach notification, and we hope that the preemption language in the bill will be reinforced when S. 139 is considered by the full Senate. We also believe that the civil penalty provisions in the bill should be clarified to ensure that the civil penalty cap applies to each incident or breach, so that the damages ceiling for mishandling a breach would not be multiplied by the number of consumers—possibly in the millions—that could be affected in a single incident. In addition, we would suggest that the bill's reference to encryption technology adopted by an "established standards setting body" might be strengthened by making clear that the standard-setting body must be widely-accepted or certified by the FTC.

CONCLUSION

For these reasons, although we share the general goals S. 139 attempts to serve, we urge our colleagues to revisit these policy and drafting issues that remain in this bill.

JEFF SESSIONS.
JON KYL.
LINDSEY GRAHAM.

VIII. CHANGES TO EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by S. 139, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

TITLE 15—COMMERCE AND TRADE

* * * * * * *

CHAPTER 41—CONSUMER CREDIT PROTECTION

* * * * * * *

Subchapter III—Credit Reporting Agencies

* * * * * * *

§ 1681c–1. Identity theft prevention; fraud alerts and active duty alerts

* * * * * * *

(b) EXTENDED ALERTS.—

(1) IN GENERAL.—Upon the direct request of a consumer, or an individual acting on behalf of or as a personal representative of a consumer, who submits an identity theft report, *or evidence that the consumer has received notice that the consumer's financial information has or may have been compromised*, to a consumer reporting agency described in section 1681a(p) of this title that maintains a file on the consumer, if the agency has received appropriate proof of the identity of the requester, the agency shall—

(A) include a fraud alert in the file of that consumer, and also provide that alert along with any credit score generated in using that file, during the 7-year period beginning on the date of such request, unless the consumer or such representative requests that such fraud alert be removed before the end of such period and the agency has received appropriate proof of the identity of the requester for such purpose;

(B) during the 5-year period beginning on the date of such request, exclude the consumer from any list of consumers prepared by the consumer reporting agency and provided to any third party to offer credit or insurance to the consumer as part of a transaction that was not initi-

ated by the consumer, unless the consumer or such representative requests that such exclusion be rescinded before the end of such period; and

(C) refer the information regarding the extended fraud alert under this paragraph to each of the other consumer reporting agencies described in section 1681a(p) of this title, in accordance with procedures developed under section 1681s(f) of this title.

fi