



CONGRESSIONAL BUDGET OFFICE  
COST ESTIMATE

November 18, 2011

**S. 1535**  
**Personal Data Protection and Breach Accountability Act of 2011**

*As reported by the Senate Committee on the Judiciary on September 22, 2011*

**SUMMARY**

S. 1535 would establish new federal crimes relating to unauthorized access to sensitive personal information. The bill also would require most federal agencies and businesses that collect, transmit, store, or use personal information to notify any individuals whose information has been unlawfully accessed. The bill also would require businesses to develop a data privacy and security program to protect the privacy of certain personal information held by those businesses. In addition, S. 1535 would require data brokers (firms that collect and sell personal information on individuals) to provide individuals access to the information held by such firms and to establish procedures for individuals to respond to inaccuracies in that information. Finally, the legislation would require federal agencies to provide additional oversight of the information security systems used by federal contractors and vendors.

Assuming appropriation of the necessary amounts, CBO estimates that implementing S. 1535 would cost \$60 million over the 2012-2016 period. Enacting S. 1535 could increase civil and criminal penalties and thus could affect federal revenues and direct spending, but CBO estimates that such effects would not be significant in any year. Further, enacting S. 1535 could affect direct spending by agencies not funded through annual appropriations. CBO estimates, however, that any changes in net direct spending by those agencies would be insignificant. Because the bill could affect direct spending and revenues, pay-as-you-go procedures apply.

S. 1535 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the cost of complying with those mandates would be small and would not exceed the threshold established in UMRA (\$71 million in 2011, adjusted annually for inflation).

S. 1535 also would impose several private-sector mandates as defined in UMRA. Much of the private sector already complies with many of the bill's requirements. However, the bill would require a large number of entities in the private sector to implement new or

enhanced security standards and provide additional services for customers. Consequently, CBO estimates that the aggregate direct cost of the mandates in the bill would exceed the annual threshold established in UMRA for private-sector mandates (\$142 million in 2011, adjusted annually for inflation).

## ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of S. 1535 is shown in the following table. The costs of this legislation fall within budget functions 750 (administration of justice), 800 (general government), and all other budget functions that contain salaries and expenses.

	By Fiscal Year, in Millions of Dollars					
	2012	2013	2014	2015	2016	2012-2016
<b>CHANGES IN SPENDING SUBJECT TO APPROPRIATION</b>						
Estimated Authorization Level	10	15	15	15	15	70
Estimated Outlays	5	10	15	15	15	60

## BASIS OF ESTIMATE

For this estimate, CBO assumes that the bill will be enacted in early 2012, that the necessary amounts will be provided each year, and that spending will follow historical patterns for similar activities.

Most of the provisions of the bill would codify the current practices of federal agencies regarding the security of sensitive personal information and the procedures they use to notify individuals concerning a breach in the security of that information. S. 1535 would require businesses and government agencies to use more advanced security encryption techniques to safeguard sensitive personal information and to notify law enforcement agencies in the event of a security breach.

While existing laws generally do not require agencies to notify affected individuals of security breaches, agencies that have experienced this problem have generally provided notification. Therefore, CBO expects that codifying this practice would probably not lead to a significant increase in federal spending. Nonetheless, the federal government is one of the largest providers, collectors, consumers, and disseminators of personal information in the United States. Although CBO cannot anticipate the number or extent 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 result in significant costs to notify individuals.

S. 1535 also would require federal agencies to provide several reports to the Congress concerning data security issues. The legislation would require agencies to conduct additional privacy impact assessments on commercially purchased data that contains personally identifiable information, and the Government Accountability Office would be required to report on the desire for privacy and federal agencies' need to use personally identifiable information acquired by private-sector firms. In addition, the General Services Administration (GSA) would be required to provide additional security assessments for government contracts involving data brokers. Based on information from the Office of Management and Budget and GSA, CBO expects that the bill would expand on current regulations and guidance for federal agencies regarding the use and protection of sensitive personal information. In addition, the legislation would require more oversight by the Department of Homeland Security for public and private-sector data. Assuming appropriation of the necessary amounts, CBO estimates that hiring additional staff, conducting administrative oversight, and preparing reports would cost \$15 million annually when fully implemented. We expect that it would take about three years to fully implement the bill's requirements.

The legislation also would require the Secret Service and Federal Trade Commission to complete additional investigations. Based on information from those agencies, CBO estimates that those activities would cost less than \$500,000 annually per agency, subject to the availability of appropriated funds.

### **Direct Spending and Revenues**

S. 1535 would establish new federal crimes relating to the unauthorized access of sensitive personal information. Thus, enacting the bill could increase collections of civil and criminal fines. CBO estimates that any additional collections would not be significant because of the relatively small number of additional cases likely to result. Civil fines are recorded as revenues. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and subsequently spent without further appropriation.

Further, enacting S. 1535 could affect direct spending by agencies not funded through annual appropriations. CBO estimates, however, that any changes in net direct spending by those agencies would be insignificant.

### **PAY-AS-YOU-GO CONSIDERATIONS**

The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. Enacting S. 1535 could increase federal revenues and direct spending, but CBO estimates that such effects would not be significant in any year.

## **ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS**

S. 1535 contains intergovernmental mandates as defined in UMRA because it would explicitly preempt laws in at least 46 states that require businesses to notify individuals in the event of a security breach and would impose notification requirements and limitations on state Attorneys General. 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 that the costs of the mandates would be small and would not exceed the threshold established in UMRA for intergovernmental mandates (\$71 million in 2011, adjusted annually for inflation).

## **ESTIMATED IMPACT ON THE PRIVATE SECTOR**

S. 1535 would impose several private-sector mandates as defined in UMRA by:

- Requiring certain business entities that handle personally identifiable information for 10,000 or more individuals to establish and maintain a data privacy and security program;
- Requiring business entities that handle personally identifiable information to notify individuals if a security breach occurs in which such individuals' sensitive personally identifiable information is compromised; and
- Requiring business entities that have experienced a security breach to purchase various credit-monitoring services and provide compensation for damages to the individuals whose personal information was included in a data security breach.

The majority of businesses already comply with data security standards and breach notification procedures similar to many of the bill's requirements. However, if the bill is enacted, a large number of entities in the private sector would need to implement new or enhanced security standards and provide additional services and compensation for customers whose information was included in a data security breach. Consequently, CBO estimates that the aggregate direct cost of all the mandates in the bill would exceed the annual threshold established in UMRA for private-sector mandates (\$142 million in 2011, adjusted annually for inflation).

### **Data Privacy and Security Requirements**

Subtitle A of title II would require businesses engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more individuals to establish and maintain a program for data privacy and security. The program would be designed to protect against both unauthorized access and any anticipated vulnerabilities. Business entities would be required to conduct periodic risk

assessments to identify such vulnerabilities and assess possible security risks in establishing the program. Additionally, entities would have to train their employees in implementing the data security program.

The bill would direct the FTC to develop rules that identify privacy and security requirements for the business entities covered under subtitle A. Financial institutions that are subject to the data security requirements under the Gramm-Leach-Bliley Act and entities that are subject to the data security requirements of the Health Insurance Portability and Accountability Act would be exempt from the requirements of subtitle A.

The cost per entity of those requirements would depend in part on the rules to be established by the FTC, the size of the entity, and its current ability to secure, record, and monitor access to data, as well as on the amount of sensitive, personally identifiable information maintained by the entity. The majority of states already have laws requiring business entities to utilize data security programs, and it is the current practice of many businesses to use security measures to protect sensitive data. However, some of the new standards for data security in the bill could impose additional costs on a large number of private-sector entities.

For example, under the bill, business entities covered under subtitle A would be required to enhance their security standards to include the ability to trace access and transmission of all records containing sensitive, personally identifiable information. The current industry standard on data security has not reached that level. According to industry experts, information on a particular individual can be collected from several places and, for large companies, can be accessed by thousands of people from several different locations. The ability to trace each transaction of data containing personally identifiable information would require a significant enhancement of data management hardware and software for the majority of businesses. Further, the bill's definition of sensitive, personally identifiable information is broader than the current industry standard. This definition would significantly increase the number of entities that would be required to implement new or enhanced data security standards. The aggregate cost of implementing such changes would exceed the annual threshold for private-sector mandates.

### **Notification of Security Breaches**

Subtitle B of title II would require business entities engaged in interstate commerce that use, access, transmit, store, dispose of, or collect sensitive, personally identifiable information to notify individuals in the event of a security breach if the individuals' sensitive, personally identifiable information is compromised. Entities would be able to notify individuals using written letters, the telephone, or email.

If a business does not own or license the information, it would have to notify the owner or licensee of the information following a breach. A notice in major media outlets serving a state or jurisdiction also would have to be provided 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. They would have to notify 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, the sensitive, personally identifiable information of millions of individuals is illegally accessed or otherwise breached every year. However, according to those sources, 46 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. Therefore, CBO estimates that the notification requirements would not impose significant additional costs on businesses.

The subtitle also contains a provision that would require providers of electronic communication services (such as Internet service providers) to inform the entity that began a transmission of information using their systems if they become aware that a breach of sensitive, personally identifiable information has occurred. This would constitute a mandate on those service providers. The cost to inform business entities of a breach would probably be small.

### **Remedies for Security Breaches**

Subtitle B of title II would impose requirements on businesses to mitigate the cost of data breaches to consumers. In particular, the subtitle would require businesses that have experienced a breach to provide upon request:

- Two years of credit-monitoring services and two years of quarterly consumer credit reports,
- Reimbursement of any costs or damages to the individual, and
- Up to two years of credit-freezing services for the individual.

The costs associated with providing remedies for security breaches could exceed the annual threshold for private-sector mandates.

Most states that have laws in place to address security breaches do require businesses to provide credit-monitoring and reporting services or to compensate for damages resulting from a breach. However, some businesses currently offer those services, depending upon the severity of the breach. The cost of bulk purchases of the credit-monitoring or reporting services is about \$60 per person according to credit industry professionals. Historically, 6 percent to 8 percent of individuals whose data was included in a breach accept such services when offered.

According to an industry report, in 2010, more than 16 million records containing personally identifiable information (a person's name, combined with any of the following: Social Security number, driver's license number, medical record, or financial record, for example) were breached, and the number of breaches has been increasing each year. Because this legislation would expand the definition of what is considered a data breach of sensitive, personally identifiable information, the number of incidents considered to be breaches and the number of records in each breach could increase under the bill. If the large number of security breaches continues, in spite of the requirements for information security programs and encryption, the cost of providing credit-monitoring or reporting services in the event of a data breach could be substantial.

Business entities that experience a breach would have to pay, upon request, the costs incurred by individuals as a result of the security breach of their sensitive identifiable information, including costs associated with identity theft. Business entities could choose either to provide insurance for consumers to be paid in the event of a breach or to pay consumers the actual cost associated with damages incurred. According to industry data, the average out-of-pocket cost to the consumer in the event of identity theft is about \$600. Not all breaches lead to identity theft, however, even if a small percentage of individuals affected by data breaches experience identity theft, the cost of this mandate could be large.

The legislation would require businesses that have experienced a breach to provide credit-freezing services to consumers upon their request and would require credit agencies to adhere to certain standards when providing those services. The credit agencies would be permitted to charge a moderate fee for those services to be paid for by the business entity for up to two years. Most state laws allow consumers to freeze their credit accounts free of charge for a short time if their personally identifying information is included in a breach. However, according to industry experts, the service is rarely requested. Also, according to those sources, the fee to establish a freeze on a credit account is about \$10. Therefore, CBO estimates that the cost of this mandate would be small.

## **PREVIOUS CBO ESTIMATES**

On October 31, 2011, CBO transmitted a cost estimate for S. 1408, the Data Breach Notification Act of 2011, as ordered reported by the Senate Committee on the Judiciary on September 27, 2011. On October 27, 2011, CBO transmitted a cost estimate for S. 1151, the Personal Data Privacy and Security Act of 2011, as ordered reported by the Senate Committee on the Judiciary on September 27, 2011. The three pieces of legislation each address unauthorized access to personal information but have different provisions. S. 1408 and S. 1151 would have similar implementation costs, while the costs to implement S. 1535 would be higher because it includes provisions that would require federal agencies to conduct privacy assessments, increased auditing of programs and contracts, as well as new reporting requirements.

**ESTIMATE PREPARED BY:**

Federal Costs: Law Enforcement Agencies–Mark Grabowicz  
Department of Homeland Security–Jason Wheelock  
Federal Trade Commission–Susan Willie  
Other Federal Agencies–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