CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

May 29, 2007

S. 1178
Identity Theft Protection Act

As ordered reported by the Senate Committee on Commerce, Science, and Transportation on April 25, 2008

SUMMARY

S. 1178 would require private companies and federal agencies to develop and enforce a system to safeguard the personal information of consumers and to notify consumers whenever there has been a breach in the security system. Under the bill, consumers also would have the option to freeze their credit reports in the event of a threat to their personal information. The bill also would restrict the use, display, and sale of Social Security numbers (SSNs). The Federal Trade Commission (FTC) would enforce those restrictions and requirements. Assuming appropriation of amounts specifically authorized in the bill, CBO estimates that implementing S. 1178 would cost $2 million in 2008 and $8 million over the 2008-2012 period.

Enacting S. 1178 could increase federal revenues as a result of the collection of additional civil and criminal penalties assessed for violations of data security regulations. Collections of criminal penalties are recorded on the budget as revenues, deposited in the Crime Victims Fund, and later spent. CBO estimates, however, that any additional revenues that would result from enacting the bill would not be significant because of the relatively small number of cases likely to be involved.

S. 1178 contains a number of intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA): some would preempt state law and others would place new requirements on state, local, and tribal governments (particularly on educational organizations and schools). The preemptions of state law would not impose significant direct costs on states. The other requirements of the bill could result in additional spending for the affected public entities, but CBO estimates that the costs of those mandates would not exceed the threshold established in UMRA ($66 million in 2007, adjusted annually for inflation).

S. 1178 would impose private-sector mandates on consumer credit-reporting agencies and other entities that acquire, maintain, or utilize sensitive personal information, including

Social Security numbers. Because of uncertainty about the number of entities that are already in compliance with most of the mandates in the bill, CBO cannot estimate the incremental cost of complying with those mandates and cannot determine whether the aggregate direct cost of all the mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($131 million in 2007, adjusted annually for inflation).

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of S. 1178 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit).

	By Fiscal Year, in Millions of Dollars				
	2008	2009	2010	2011	2012
CHANGES IN SPENDING SUBJECT TO APPROPRIATION [a]					
Authorization Level	2	2	2	2	0
Estimated Outlays	2	2	2	2	0

a. Enacting S. 1178 also could affect revenues from the assessment of civil criminal penalties; and it could affect direct spending from the expenditure of any criminal penalties assessed. CBO estimates that any such effects would be less than $500,000 a year.

BASIS OF ESTIMATE

For this estimate, CBO assumes that the bill will be enacted in 2007 and that the specified amounts will be appropriated for each year. CBO estimates that implementing the bill would cost $2 million in 2008 and $8 million over the 2008-2012 period to issue regulations and enforce the bill's new provisions restricting the use of personal information.

Section 12 would require federal agencies to develop, implement, maintain, and enforce programs for the security of personal information an agency possesses. In the event of a security breach involving a reasonable risk of identity theft, S. 1178 would require government agencies to notify an individual whose information may have been compromised. Notification would be in the form of individual notice (written notice to a home mailing address or via e-mail) as well as through an Internet Web site and the mass media. 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 a toll-free telephone number and Web site that the individual can use to obtain information on identity theft.

This provision would codify the current practice of the federal government regarding data security and security breach notification. The Federal Information Security Management Act of 2002 provides requirements for securing the federal government's information systems, including the protection of personal privacy. The National Institute of Standards and Technology develops information security standards and guidelines for other federal agencies, and the Office of Management and Budget (OMB) oversees information technology security policies and practices. OMB estimates that federal agencies spend around $5.5 billion a year to secure the government's information systems.

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 security breaches. Therefore, CBO expects that implementing this provision 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 personnel information in the United States. Although CBO cannot anticipate the number of security breaches nor the extent of any such occurances, a significant breach of security involving a major collector of personnel 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.

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

S. 1178 contains a number of intergovernmental mandates, but CBO estimates that the costs of those mandates would not exceed the threshold established in UMRA ($66 million in 2007, adjusted annually for inflation).

Safeguarding Personal Information and Notifying Individuals of Security Breaches

The bill would establish new requirements for safeguarding personal information and put in place a new federal requirement for notifying individuals and the Federal Trade Commission in the event that personal information is compromised. Those new federal requirements would apply to educational organizations and schools, including public school systems and universities. (It would not apply to state, local, or tribal governments broadly.)

Under current law, educational institutions that receive federal funds already are required to safeguard certain personal information and must comply with standards required under the Family Educational Rights and Privacy Act and established by the Department of Education. Depending on the differences between the rules promulgated by the FTC and those already required by the department, educational institutions may have to make changes to their current systems. The bill also would require schools to notify affected individuals of any breach of security in which personal information of more than 1,000 individuals may have been compromised and to maintain a toll-free number for contacting the school. If schools are required to change procedures for handling information, implement new controls on computer systems, provide additional information to the FTC, or provide notifications, they could face added costs. However, existing regulations cover, at least in a broad manner, many of the issues that S. 1178 addresses; additional costs likely would not exceed the threshold.

Preemptions of State and Local Laws

S. 1178 would preempt a number of state and local laws that establish rules for safeguarding personal information and that restrict the use of SSNs. The bill would preempt state laws that require schools or other entities that collect personal information to notify individuals in the event of a security breach, and it would preempt state laws that do not afford individuals greater protection regarding the release of private information by credit-reporting agencies. The bill also would establish a federal law that would place a number of restrictions on the display, collection, sale, and transfer of SSNs and would preempt similar state and local laws. Those preemptions would be intergovernmental mandates as defined in UMRA, but they would impose no duty on states that would result in additional spending.

The bill would place notification requirements on state attorneys general that prosecute cases involving breaches of security or violations of the new rules governing Social Security numbers. Since state laws would be preempted by the bill, the new federal law would be the primary avenue for prosecuting cases. Consequently, the notification requirements would be an intergovernmental mandate, but CBO estimates that the costs of such notifications would be small.

Social Security Numbers

In some cases, the bill's restrictions on the collection, sale, or use of SSNs would place requirements on state and local governments, including schools. The bill would prohibit states from displaying SSNs on driver's licenses, but this practice is already prohibited by federal law as part of the Intelligence Reform and Terrorism Prevention Act of 2004. The bill also would prohibit state and local governments from allowing prisoners access to SSNs of other individuals. While those prohibitions would be intergovernmental mandates, they would place no new requirement on states that would result in significant additional spending.

The bill would prohibit schools from displaying SSNs on identification cards or tags. Federal law currently places some restrictions on the use of SSNs by colleges, universities, and other schools that receive federal funding. While the specific prohibition on the use of SSNs on identification materials would be new, indications from organizations that represent public schools and universities are that few schools, if any, still use SSNs as identifiers. Consequently, CBO estimates any additional costs as a result of this requirement would be small.

ESTIMATED IMPACT ON THE PRIVATE SECTOR

S. 1178 would impose private-sector mandates on credit-reporting agencies and other entities that acquire, maintain, or utilize sensitive personal information, including SSNs. Because of uncertainty about the number of entities that are already in compliance with most of the mandates in the bill, CBO cannot estimate the incremental cost of complying with those mandates. Therefore, CBO cannot determine the total direct cost of the mandates contained in the bill or whether such costs would exceed the annual threshold established by UMRA for private-sector mandates ($131 million in 2007, adjusted annually for inflation).

Security Program

Section 2 of S. 1178 would require covered entities to implement and enforce a written program to secure sensitive personal information, which includes a person's name, address, or telephone number in combination with their social security number. Covered entities include businesses, employers, educational and nonprofit institutions that acquire, maintain, and utilize sensitive personal information. According to industry and government sources, many states already have laws requiring business entities to utilize data security programs. Moreover, it is the current practice of many businesses to use security measures to protect sensitive data. However, because of uncertainty about the number of entities that are already

in compliance with the data security mandates, CBO cannot estimate the incremental cost of complying with those mandates. Additionally, this section would require the FTC to promulgate regulations that would require procedures for authenticating the credentials of any third party to which a covered entity transfers or sells sensitive personal information. CBO cannot estimate the cost of complying with this mandate because the cost would depend on the rules to be established by the FTC.

Notification of Security Breach Risk

In the case of a security breach affecting 1,000 or more persons, section 3 would require covered entities to report the breach to the Federal Trade Commission and notify all consumer reporting agencies. If the required investigation of the breach finds that there is a reasonable risk of identity theft, the entity also would be required to notify all affected individuals. According to industry and government sources, millions of individuals' sensitive personally identifiable information is illegally accessed every year. However, according to those sources, a majority of states already have laws requiring notification in the event of a security breach. In addition, it is the current practice of many business entities to notify individuals in the event of a security breach. Because of uncertainty about the number of entities that are already in compliance with the notification mandates, CBO cannot estimate the incremental cost of complying with the notification requirement under the bill.

Security Freeze on Credit Reports

Section 4 would allow consumers to place a security freeze on their credit report by making a request to a consumer credit reporting agency. The credit reporting agency would be prevented from releasing the credit report to any third parties without prior authorization from the consumer. The agency also would be required to notify all other consumer reporting agencies of the security freeze at the consumer's request. According to industry sources, most states currently have credit freeze laws in place. Because of uncertainty about the number of entities that are already in compliance with the security freeze mandate, CBO cannot estimate the incremental cost of complying with the notification requirement under the bill.

Social Security Number Protection

Section 11 would prevent covered entities from soliciting a social security number from an individual unless no other identifier can be used reasonably. This section also would prevent covered entities from displaying SSNs, or any part of such a number, on any card or tag used for identification, such as student or employee identification cards. CBO estimates that the cost imposed on all covered entities would be small, since relatively few covered entities still use SSNs in this manner.

ESTIMATE PREPARED BY:

Federal Costs: Susan Willie and Matthew Pickford
Impact on State, Local, and Tribal Governments: Leo Lex
Impact on the Private Sector: Fatimot Ladipo

ESTIMATE APPROVED BY:

Peter H. Fontaine
Deputy Assistant Director for Budget Analysis